Table of Contents

Chapter 1: Welcome

System requirements
Windows® operating system
Macintosh®

Chapter 2: Getting started with Intralinks

What are exchanges?
A quick tour of your Intralinks exchange
Security within Intralinks
Your role within your exchange
Logging into Intralinks
Logging in the first time
Returning to Intralinks
Changing your password
Resetting a lost password
Personalizing your Intralinks experience
Registering a mobile phone to receive security codes
Logging out
Removing yourself from an exchange
Recommending other users
Troubleshooting

Chapter 3: Setting up exchanges

The exchange life cycle
Working with your Intralinks representative
Tasks that must be performed by an Intralinks employee
Tasks you can perform
Working with your business group
Business group membership levels
Defining an exchange template
Creating an exchange
Creating an exchange splash screen and footer
Making changes to email alerts
Moving an exchange from one phase to another
Viewing and changing exchange settings
Enabling Intralinks Viewer
Using Intralinks Viewer to track users’ viewing time
Setting up document tags
Setting up custom fields
Setting default values and access levels for custom fields
Setting custom field values for exchanges
Ordering archive copies of your exchanges
Creating working sets
Using public working sets
Viewing exchange details
Ensuring that members of your organization can download content from Intralinks exchanges
Chapter 4: Managing users and groups ..............................................................41
Getting started with user groups......................................................................41
Creating and managing groups ..........................................................................42
Using the Add Group Wizard ...........................................................................42
Modifying group properties ................................................................................44
Viewing the members of a group .......................................................................44
Viewing the history for a user group .................................................................45
Removing user groups ....................................................................................45
Users’ roles within an exchange ........................................................................46
Group member roles ........................................................................................46
Adding users ......................................................................................................48
Using the Add Users Wizard ............................................................................48
Adding users from the Hub ...............................................................................50
Importing user information using Intralinks Designer ........................................51
Requesting another manager to add users .......................................................52
Responding to requests that users be added to your exchange .........................53
Assigning users to another group .....................................................................53
Changing a user’s exchange role ......................................................................54
Making a user a key contact for the exchange ...................................................54
Removing users from the exchange .................................................................55
Managing an individual user’s access to multiple exchanges .........................55
Copying groups from one exchange to another .............................................56
Finding users and groups ...............................................................................58
Finding users using smart filters ......................................................................58
Resending welcome alerts to exchange members ............................................59
When users leave your organization .................................................................59
Users’ roles within an exchange ........................................................................66
Group member roles ........................................................................................66
Adding users ......................................................................................................68
Using the Add Users Wizard ............................................................................68
Adding users from the Hub ...............................................................................70
Importing user information using Intralinks Designer ........................................71
Requesting another manager to add users .......................................................72
Responding to requests that users be added to your exchange .........................73
Assigning users to another group .....................................................................73
Changing a user’s exchange role ......................................................................74
Making a user a key contact for the exchange ...................................................74
Removing users from the exchange .................................................................75
Managing an individual user’s access to multiple exchanges .........................75
Copying groups from one exchange to another .............................................76
Finding users and groups ...............................................................................78
Finding users using smart filters ......................................................................78
Resending welcome alerts to exchange members ............................................79
When users leave your organization .................................................................79

Chapter 5: Publishing documents ....................................................................60
Managing folders ..............................................................................................60
Creating folders ...............................................................................................60
Organizing folders ............................................................................................64
Moving folders ..................................................................................................65
Renaming folders and changing custom field values .......................................65
Deleting folders ...............................................................................................66
Adding documents ............................................................................................66
Using the New Document Wizard ....................................................................66
Replacing a placeholder with a document .......................................................71
Adding multiple documents at the same time ..................................................72
Replacing or updating documents ....................................................................75
Reviewing and modifying permissions .............................................................75
Setting permissions for all the documents in one or more folders ...................76
If you use document-level permissioning .........................................................77
If you use folder-level permissioning (permissions are inherited) .....................79
Overriding folder-level permissions ................................................................81
Making a document available to all exchange users .........................................83
Moving documents ...........................................................................................83
Sending alerts ..................................................................................................84
Deleting documents ..........................................................................................85
Copying and pasting documents ......................................................................85
Using working sets to copy documents from one exchange to another ........86
Checking out documents ..................................................................................86
Importing information using Intralinks Designer .............................................87
Using naming conventions to standardize document names .......................87
Enabling reviewers and previewers to publish documents, add folders and edit folder custom fields .................................................................91
Chapter 6: Protecting documents ...............................................................93
  What is document locking and protection? ..................................................93
  Document protection capabilities ...............................................................93
    Requirements for end users ........................................................................94
  Applying protections ....................................................................................94
  Changing protection settings ......................................................................95
  Tracking user activity ..................................................................................96

Chapter 7: Managing document permissions ............................................97
  Reviewing and modifying permissions .......................................................97
  Setting permissions for all the documents in one or more folders ..............98
    If you use document-level permissioning ..................................................99
    If you use folder-level permissioning (permissions are inherited) ..........100
  Overriding folder-level permissions .........................................................102
  Making a document available to all exchange users ..................................103

Chapter 8: Reviewing documents .............................................................104
  Viewing documents ....................................................................................104
  Finding documents ....................................................................................105
    Tips for using Intralinks’ search tools .......................................................108
    Finding documents using smart filters ...................................................109
  Downloading documents .........................................................................110
    Bulk downloading documents from a single exchange ..........................110
    Bulk downloading documents from multiple exchanges .....................111
  Printing documents ..................................................................................112
  Working with protected documents .........................................................113
    What is document locking and protection? ..............................................113
    Performing ad hoc analysis using IRM-protected Excel documents ........114
    Viewing PDF and Microsoft Office documents using Intralinks Viewer ..114

Chapter 9: Managing standard and rules-based business processes ............117
  What are business processes? ...................................................................117
    Standard processes ................................................................................118
    Rules-based processes ..........................................................................119
  Setting up standard business processes ....................................................120
    About submitters, reviewers and approvers ...........................................121
    Creating and configuring standard business processes ..........................121
    Setting up a document date trigger process ..........................................124
  Setting up rules-based business processes ..............................................127
    Creating and configuring a rules-based submission business process ....127
    Creating and configuring a rules-base document distribution business process .....133
    Creating and configuring a group-triggered document distribution business process ........................................138
  Activating business processes ..................................................................138
  Inactivating, reactivating and deleting business processes ......................143
  Renaming a business process ....................................................................144
  Copying a business process ......................................................................145
Chapter 10: Managing multi-task processes ...........................................146
  What are multi-task processes? .............................................................146
  Setting up multi-task business processes ............................................146
  Creating tasks for a multi-task process ...............................................150
  Activating multi-task processes ..........................................................156
  Inactivating, reactivating and deleting multi-task processes .................156
  Renaming a multi-task process ............................................................158
  Making changes to a multi-task process ..............................................158
  Using multi-task business processes to apply electronic signatures to documents .....158
    Electronic signatures are Title 21 CFR Part 11 compliant ......................160

Chapter 11: Completing tasks that are assigned to you .....................161
  Using standard and rules-based business processes .............................162
    Viewing tasks that are assigned to you ..............................................162
    Submitting documents ........................................................................162
    Reviewing and approving documents that have been submitted to you ....165
    Requesting a document .......................................................................166
    Responding to document requests .....................................................167
    Acknowledging receipt of documents ...............................................168
    Resubmitting acknowledgment responses .......................................170
    Adding co-monitors ...........................................................................171
    Renaming a business process instance ..............................................171
    Cancelling a task ................................................................................171
  Using multi-task processes .................................................................172
    Viewing processes and tasks ...............................................................172
    Completing tasks ................................................................................173
    Adding comments to processes and tasks ...........................................176
    Changing the status of processes .......................................................178

Chapter 12: Using Intralinks eForms .................................................179
  Requirements and prerequisites .............................................................179
    If you are using eForms with business processes ...............................179
  Creating and modifying eForms ............................................................179

Chapter 13: Viewing, exporting and printing reports .......................181
  Viewing document reports ...................................................................181
    Viewing a list of folders and documents on the exchange ....................182
    Viewing history information for documents ......................................182
    Viewing a list of deleted documents ...............................................183
    Viewing reports for users and groups ...............................................183
      Viewing users’ and groups’ overall exchange activity ....................184
    Viewing advanced access reports .....................................................190
    Viewing Process Access Reports ......................................................192
  Other reports .......................................................................................193

Appendix A: Exchange settings .............................................................194

Appendix B: Data limits ........................................................................213

Index ....................................................................................................217
Chapter 1: Welcome

Welcome to Intralinks® Platform, the premier tool for secure online collaboration between organizations.

Intralinks Platform is designed to be easy to use, and we’ve included a number of tools to make your Intralinks experience even more productive.

This user guide provides step-by-step instructions for completing tasks using your Intralinks exchanges. Other tools also are available to help you make the most of your time while working in Intralinks exchanges:

The Answer Library is your online resource for troubleshooting issues that arise as you work in Intralinks exchanges. It also provides training videos to get you started with tasks that are new to you. To open the Answer Library, click the Help button in the upper right area of the Intralinks Platform window.

Of course, Intralinks also provides award-winning support. If the User Guide and Answer Library don’t answer your question, give us a call! Local telephone numbers for Intralinks Client Services can be found at:

http://www.intralinks.com/contact/client-services
System requirements

In order for you to use Intralinks Platform, your computer must meet the following minimum standard:

Windows® operating system

- Operating system: (No specific requirement, but must be able to support a supported Web browser)¹
- Screen resolution: 1024 by 768 dpi or greater
- Web browser²: Microsoft® Internet Explorer 7 or a newer version; Firefox® 42 and later; Google Chrome 46 and later³
- (If using Bulk Download or Bulk Print functions) Microsoft .NET Framework 2.0⁴
- Adobe® Flash® Player 9, 10.3 or 11⁵
- Adobe Reader® 10 or greater

¹. Your computer also must have a 32-bit processor and a minimum of 512 MB of RAM, 10 MB of available disk space and a 1 GHz CPU (central processing unit).
². Browsers must support the TLS encryption protocol. The SSLv3 protocol is not supported.
³. On Windows, Chrome requires Microsoft .NET Framework 2.0 or later.
⁴. Microsoft® .NET Framework 2.0 is a minimum requirement; .NET Framework 3.5 is recommended. If you are using a Firefox® browser, you also must install a third-party plugin, such as FFClickOnce, to enable .NET Framework and Firefox to work together. FFClickOnce and similar tools are available from the Mozilla® website: www.mozilla.org
⁵. If Adobe Flash Player is not installed, an alternative version of Intralinks Platform containing limited functionality is used. This alternative version is suitable only for reviewers. Manager and publisher functions require Adobe Flash Player to be installed. Flash Player is required to view Intralinks Platform in languages other than English.
Macintosh®

- Operating system: (No specific requirement, but must be able to support a supported Web browser)
- Screen resolution: 1024 by 768 dpi or greater
- Web browser: Safari 9 and later; Firefox 42 and later; Google Chrome 46 and later¹
- Adobe® Flash® Player 9, 10.3 or 11²
- Adobe® Reader® 10 or greater

Copyright © 2015 Intralinks, Inc. All rights reserved. Adobe, Flash and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. Macintosh and Safari are registered trademarks of Apple Inc. All other service, product and/or brand names are the property of their respective owners.

¹. On Macintosh, Chrome does not allow bulk downloading or bulk printing; use Safari to perform these functions.
². If Adobe Flash Player is not installed, an alternative version of Intralinks Platform containing limited functionality is used. This alternative version is suitable only for reviewers. Manager and publisher functions require Adobe Flash Player to be installed. Flash Player is required to view Intralinks Platform in languages other than English.
Chapter 2: Getting started with Intralinks

Overview

Read this chapter for overviews of:

- The features in Intralinks exchanges
- Intralinks’ security features
- Users’ exchange roles and responsibilities
- Logging into and out of Intralinks
- Managing your password
- Updating your profile and preferences
- Logging out of Intralinks Platform
- Removing yourself from an exchange
- Recommend that other people be given access to your exchanges
- Finding help if problems arise

What are exchanges?

Each Intralinks exchange provides a secure Web-based space for sharing critical information, performing workflow tasks, and collaborating with people both inside and outside your organization.

Exchanges can be used as document repositories, either enterprise wide or for corporate boards, but they can be used to meet a variety of organizational needs.

Depending upon the purpose of the exchange that you are using, you may use the exchange for sharing or consuming documents and other content; you may use it for collaboration or completing tasks that are part of a larger workflow, or a combination of these activities.

A quick tour of your Intralinks exchange

Whenever you use an Intralinks exchange, you must begin by logging in. This gives you access to the exchanges to which you have been assigned. To learn more about logging in, see the next section, “Logging into Intralinks.”

After you log into Intralinks, you will see a list of the exchanges in which you participate.

Security within Intralinks

Organizations use Intralinks exchanges to share highly sensitive or confidential information with one another. Intralinks recognizes that the need for security is paramount, and a variety of measures have been put into place to ensure that only the people intended to view each document actually see it.
For example, users see only the documents they are given permission to see, and exchange hosts can prevent users from printing, downloading or making images of the documents. Watermarking and other features can be used to discourage users from sharing the documents that they are allowed to print. Exchange managers also have a complete view of each user’s activities — which documents have been read or downloaded, when and how often.

For more information about Intralinks’ security features, see Chapter 3, Setting up exchanges, on page 19.

Your role within your exchange

Every person invited into an Intralinks exchange has been assigned an exchange role, or set of rights and responsibilities while working within the exchange. If you have been invited to a number of exchanges, you may discover that you have a slightly different role in each exchange.

(Note that exchange roles are different from group member roles, which are described on page 43.)

There are three basic exchange roles within Intralinks:

Reviewer – Reviewers generally can see and work with the people who were responsible for setting up the exchange, but they may not be able to see or work with one another. Most reviewers generally are not from the organization hosting the exchange.

Publisher – Publishers assist managers by adding documents to the exchange. They may be responsible for setting permissions for the documents — that is, identifying the exchange users who are allowed to view, print and download each document. Publishers can see reviewers and other publishers, as well as exchange managers. Publishers generally are from the organization that is hosting the exchange.

Manager – Managers are responsible for setting up and maintaining the exchange, with assistance from Intralinks Client Services. With a few exceptions, managers can perform all tasks within the exchange. They can publish documents, and they determine who has access to the exchange.

For a detailed discussion of exchange roles and the rights and responsibilities associated with each of them, see Chapter 4, Managing users and groups, on page 41.

Logging into Intralinks

Each time you visit Intralinks, you will be asked to log in by entering your email address and password. This is to ensure that you see only the documents that are relevant to you. You have a single password for Intralinks, no matter how many exchanges you participate in.

If your organization uses Single Sign-On (SSO) or Exclusive Single Sign-On (e-SSO) If your organization uses Intralinks’ Single Sign-On (SSO) or Exclusive Single Sign-On (e-SSO) functionality, you will be asked to log into your corporate network, rather than Intralinks, when you display the Intralinks login page. If you are already logged into the corporate network, Intralinks will be displayed automatically. While you are logged into the corporate network, you will not have
to enter your Intralinks credentials to view exchanges or protected documents that you have downloaded, unless you access an exchange that uses enhanced security, and the security rules require you to enter your credentials. (If your organization uses e-SSO, you will not be given Intralinks login credentials; you must log into the corporate network to access your exchanges and documents.)

For security purposes, it is important that you do not share your password with others. If a colleague needs to have access to an exchange, you can recommend that he or she be added as a member of the exchange. To learn more, see “Requesting another manager to add users” on page 52.

Logging in the first time

When you are invited to join an exchange, you will receive two email messages from Intralinks. (The message may indicate that it has come from the company that is hosting the exchange.) The first message includes a link to the exchange. The second message contains your temporary password to Intralinks; if you have participated in Intralinks exchanges in the past, you will be asked to use the password you use for other exchanges.

If your organization uses Single Sign-On (SSO) or Exclusive Single Sign-On (e-SSO) If your organization uses Intralinks’ Single Sign-On (SSO) or Exclusive Single Sign-On (e-SSO) functionality, you will not receive an email message with a temporary password.

About your email address
Your email address serves as your Intralinks user ID. If you have more than one email address, use the address for the account where you received the invitation message to the exchange. If your email address changes, contact Intralinks Customer Service for assistance in updating your Intralinks ID. Local telephone numbers for Intralinks Client Services can be found at:

http://www.intralinks.com/contact/client-services/

To log in the first time

1. Locate the email messages containing your invitation to the exchange and your password.
2. Click the link to the exchange that appears in the invitation message. A web browser opens and Intralinks’ license agreement is displayed.
3. Read the license agreement and click Accept to continue logging in. Your profile screen appears. Continue with step 4.

   If you do not agree to the terms of the license agreement, click Do Not Accept. The login screen reappears, and you can close your browser to exit.
4. Review the fields on the screen and make entries in the fields marked in red to create a user profile for yourself, to change your password and enter a challenge question, and to set preferences.

   The challenge question is particularly important. Be sure that you choose a question whose answer you are sure to remember, as you may be asked this question when you log in if your exchange uses Intralinks’ enhanced security, if you forget your password or if you contact Intralinks Client Services with other requests.
Mark the **Share additional info with users I work with** option if you want to make your entries in the **Title**, **Industry** and **Functional Area** fields available when colleagues view information about you in the **People** list on the **Hub**. If you do not want to share this information with others, unmark the **Share additional info with users I work with** option.

5. When you have finished making profile entries, click **Save**. Your exchange appears.

## Returning to Intralinks

**To log in after your first visit to Intralinks**

1. Using your Web browser, go to [www.intralinks.com](http://www.intralinks.com) and click the **Login** button that appears there. The Intralinks login page appears. (You can use your browser to create a bookmark for this page, making it easy for you to return to Intralinks in the future.)

   **If your organization uses Single Sign-On (SSO)** If your organization uses Intralinks’ Single Sign-On (SSO) functionality and you are logged into the corporate network, Intralinks will be displayed automatically. (If you are not logged into the corporate network, you will be asked to log into it.) Skip to step 5.

2. In the **Email Address** field, enter the email address for the account where you received your invitation to the exchange.

3. In the **Password** field, enter the password you created after you logged into Intralinks the first time.

   If you have forgotten your password, click the **Forgot your Password?** link and follow the instructions that appear on your screen. (For step-by-step instructions, refer to “Resetting a lost password” on page 13.)

4. Click **Log In**.

   If a message appears asking you to answer your challenge question or a security code, type the answer and click **Submit**.

   The Intralinks **Hub** appears, displaying a list of the exchanges in which you are a participant. (If you have been invited to only one exchange, that exchange is displayed immediately.)

   The **Hub** also includes a dashboard. The dashboard gives you quick access to new documents, unread documents, new and updated documents, open tasks assigned to you, tasks that you can initiate, and links to maintenance tasks and help tools. If you have access to more than 50 exchanges, information only for the five exchanges you use most are displayed.

5. Select either an item in the dashboard or an exchange. To select an exchange, double-click the exchange name.

   If the managers of the exchange have opted to use Intralinks’ enhanced security function, you may be asked to enter the answer to your challenge question (which you selected the first time you logged into Intralinks). You also may be asked to enter a one-time password or security code; if this is the case, follow the steps on the screen to complete the login process.

   Depending upon how your exchange is set up, you can receive security codes by email or as a text message (SMS) on a mobile device. Some exchanges may require you to use one method or the other; other exchanges may allow
you to choose the option you prefer. To learn more, see “Registering a mobile phone to receive security codes” on page 15.

A variety of enhanced security settings are available to exchange managers, and your login experience may vary from one exchange to another, and from one time to the next. Intralinks’ enhanced security is risk based, so you might be asked to answer your challenge question if you log into Intralinks from a different location than you usually do, for example.

6. If you selected an exchange, a list of documents available to you in the exchange is displayed. If you selected a dashboard item, that item is displayed.

Changing your password

Your Intralinks password expires periodically to ensure the security of the exchanges that you access. For most users, passwords expire every 90 days, but exchange managers may set another frequency for their exchanges.

If your password has expired, a message appears when you attempt to log into Intralinks, instructing you to create a new password.

You can change your password more frequently if you like. Follow the instructions below to do so.

If your organization uses Single Sign-On (SSO) If your organization uses Intralinks’ Single Sign-On (SSO) functionality, you do not have a separate Intralinks password, and you will not receive password expiration alerts.

► To change your password

1. Log into Intralinks using your old password. The Intralinks Hub appears.

2. Locate the My Profile link at the top of the window and click it. Your profile screen appears.

3. In the Current Password field, enter the password you have been using.

4. In the New Password and Re-type New Password fields, enter the new password.

   A tip will appear onscreen to outline the rules for creating your password. (Depending upon the selections that exchange managers made when setting them up, the rules may vary.)

5. Click OK.

Resetting a lost password

If you have forgotten your password, you can reset it. If you have registered a mobile device with Intralinks, you can receive a security code by text message (SMS); this code will allow you to reset your password. If you have not registered a mobile device, the code can be sent to the email address that you use to log into Intralinks. To learn more, see “Registering a mobile phone to receive security codes” on page 15.

If your organization uses Single Sign-On (SSO) If your organization uses Intralinks’ Single Sign-On (SSO) functionality and you have forgotten your
password, contact your organization’s IT department for assistance. Do not use the procedure below.

**To reset your password**

1. On the login page, click Forgot your password? The Forgot Password screen appears.
2. Enter the email address that you use to log into Intralinks, then click Next. The Answer security question screen appears.
3. Answer the question that appears on the screen. This is the challenge question you chose when you created your Intralinks user profile. Click Submit. (Note: You may not be asked to answer your challenge question under some circumstances. If this is the case, go on to step 4.)
4. The Choose Delivery Method screen appears. If you have registered one or more mobile devices with Intralinks, you can choose to have a security code sent by text (SMS) to one of these devices. You also can opt to receive an email message with a link that will allow you to reset your password. Choose the method you prefer.
5. Click Next. A text or email message will be sent to you.
6. **If you chose email as your delivery option:** Check your email for a message from Intralinks. The message contains a link that will allow you to reset your password. Click the link to display a screen where you can enter your new password. You also may be asked to answer your challenge question on this screen.

   **If you chose SMS as your delivery option:** Check your mobile device for a message from Intralinks. The message contains a security code that will allow you to reset your password. The Enter code screen is displayed in Intralinks; enter the code here and click Next. The Create new password screen appears; enter and confirm your new password, then click Finish.

After you reset your password, the Intralinks Hub appears.

**Personalizing your Intralinks experience**

You can update your contact details (except for your email address) and preferences for using Intralinks at any time.

**To update your profile and preferences**

1. Log into Intralinks Platform. The Intralinks Platform Hub appears.
2. Locate the My Profile link at the top of the screen and click it. The Details view of your profile screen appears.
3. Review the information on the screen and make any needed changes.

   Mark the Share additional info with users I work with option if you want to make your entries in the Title, Industry and Functional Area fields available when they view information about you in the People list on the Hub. If you do not want to share this information with others, unmark the Share additional info with users I work with option.
4. Click the Alerts tab to display the Alerts view of your profile screen. Review the selection and make any changes that you like.
You can indicate whether email alert messages will be in HTML or plain-text format; whether these alert messages will be sent to additional addresses; and the frequency with which these alert message will be sent to you.

(Note that an exchange manager may wish to send you a message immediately; in some circumstances, you may receive an alert immediately, regardless of the preference you select here.)

5. Click **OK**.

### Registering a mobile phone to receive security codes

If you register a mobile phone or another device that is capable of receiving text (SMS) messages, you can have security codes texted to you. These codes can be used to reset your password or to gain access to exchanges with enhanced security requiring a one-time password before entry. Some exchanges may require you to use one method or the other; other exchanges may allow you to choose the option you prefer. When resetting your password, you always have the option to use either SMS or email as the delivery method.

In most cases, receiving security codes by text is a faster, easier alternative to having a temporary password sent by email, but you can continue to have security codes sent to you by email if you like.

Intralinks will not use registered phone numbers for any purpose other than to send verification codes and will not share registered numbers with other parties.

If your password expires and you have not yet registered a mobile device, you will have the opportunity to do so when you reset your password. You also can register a device if you attempt to access an exchange that requires a security code, if the exchange manager allows the code to be sent by SMS. If you wish to register a device now, you can complete the steps below.

#### To register a mobile phone

1. Log into Intralinks Platform. The Intralinks Platform **Hub** appears.
2. Locate the **My Profile** link at the top of the screen and click it. The **Details** view of your profile screen appears.
3. In the **Security Settings** section of the screen, click the **Register and Review Mobile Numbers** link. The **Security Settings** screen appears in a new browser instance.
4. Review the country code and enter the phone number for your mobile device.
5. Click **Send Code**. A text message containing a security code will be sent to your mobile device.
6. Enter the security code on the **Verify Mobile Numbers** screen, then click **Verify**. The **Security Settings** screen will be redisplayed, showing the number as verified.
7. If you wish to register another mobile device, click **Add Mobile Number** and repeat steps step 4 through step 6. You can register up to three numbers. If you register multiple numbers, you will be able to choose which number will receive the text when a security code is requested.

If you do not wish to register any more numbers, close the **Security Settings** screen.
Logging out

Whenever you have finished working with your exchanges, we suggest that you log out of Intralinks to ensure that others will not be able to view information that is not meant for them. If your Intralinks session is idle for a set period of time, you will be logged out automatically. (A message will appear five minutes before this occurs, giving you the opportunity to continue working in your exchanges if you like.)

The amount of time before you log out typically is 60 minutes, but exchange managers may request a shorter idle time limit. The minimum session time allowed is 20 minutes. If you have access to multiple exchanges, the shortest timeout periods used by any of those exchanges will be the one used.

To log out of Intralinks Platform

◊ Click the Logout option in the upper right corner of the Intralinks Platform screen. The Intralinks login screen appears.

If your organization uses Single Sign-On (SSO), the login screen may not appear. In this case, a screen appears to inform you that you have logged out and can close the browser or click the Login button to return to Intralinks Platform.

Removing yourself from an exchange

Use the following procedure to remove yourself from an exchange that you no longer need to use.

If no Remove Me command appears in the Actions menu in step 3, the owner of your exchange does not allow you to remove yourself from the exchange. Contact an exchange manager for assistance.

To remove yourself from an exchange

1. Display the list of your exchanges in the Hub.
2. Highlight the exchange that you no longer need to use.
3. From the Actions menu, select Remove Me. A dialog box appears.
4. Select your reason for removing yourself, then click Remove Me.

 Recommending other users

Intralinks users can recommend that colleagues be added to the exchanges that they use. These recommendations are forwarded by email to the exchanges’ key contacts, who choose whether to add the individuals as exchange users.

To recommend that users be added to a single exchange

You can use the procedure below to recommend that users be added to the exchange that you currently are using.

The Users & Groups tab should be displayed.

1. Click the Recommend User to this Exchange button near the top of the screen. The first step of a two-step wizard appears.
2. Using the Select User(s) tab on the left side of the screen, enter the email address, name or organization associated with the person you are recommending. As you type, the list of contacts is narrowed to show only those that match your entry. When you see the name that you want, highlight it and click the arrow button  to move it to the Selected Users list.

   If you enter an email address that does not exist in Intralinks’ Global User Directory, the Recommend New User tab is displayed, and you can enter the information needed to add the individual to the Global User Directory. When you have entered the required information, click Add to add the person to the Selected Users list.

3. If you wish to add multiple people, repeat step 2. When you have finished adding users, click Next. The Review and Complete step of the wizard is displayed.

4. Enter a note explaining your request to the exchange manager.

5. Review the selected users to be sure they are correct. If any changes need to be made, click the Back button to do so.

6. When you are satisfied with your selections, click the Save button. A request will be emailed to the key contacts for the exchange.

   To recommend that users be added to multiple exchanges

   If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

   1. Click the People button on the left side of the screen to display a list of all the people you have worked with in Intralinks.

       These include people with public profiles, people you have added to your exchanges (if you are a manager on any exchanges), and people with whom you work on at least one exchange already, regardless of whether their profiles are public or private.

   2. Use the search and filtering tools to the right of the Hub button to find the person or people you want to recommend.

   3. Highlight the names of the person or people you want to recommend. To select multiple people, press the SHIFT or CTRL key while clicking the users’ names.

   4. From the Actions menu, select Recommend User to an Exchange. The first step of a two-step wizard appears, displaying a list of your exchanges.

   5. Mark the boxes next to the exchanges you want the selected users to be added to, and click Next. The second step of the wizard appears.

   6. Enter a note explaining your request to the exchange manager.

   7. Review the selected users and exchanges to be sure they are correct. If any changes need to be made, click the Back button to do so.

   8. When you are satisfied with your selections, click the Save button. A request will be emailed to the key contacts for the exchanges you selected.
Troubleshooting

Although Intralinks exchanges are designed to be easy to use and highly reliable, tools are available to help you if you encounter problems as you complete your tasks. In addition to Intralinks’ award-winning customer support, we provide an extensive knowledgebase, the Intralinks Answer Library, to help answer your questions and get you back to work as quickly as possible. The Answer Library also provides training videos to get you started with tasks that are new to you.

You can browse through the Answer Library — the most popular topics appear first in the list — or you can search for a specific word or phrase.

To view the Answer Library

◊ Click the Help option in the upper right corner of the Intralinks window. The Intralinks Answer Library appears in a new browser window.

If the Answer Library does not provide the information you want, contact Intralinks Client Services. Contact options can be found in the box on the right side of the Answer Library screen.
Chapter 3: Setting up exchanges

Overview

Read this chapter for overviews of:

- The exchange life cycle
- Working with your Intralinks representative
- Creating exchange templates
- Creating exchanges
- Creating exchange splash screens
- Moving exchanges from one phase to another
- Viewing and changing exchange settings
- Enabling Intralinks Viewer
- Setting up document tags
- Setting up and managing custom fields
- Requesting archive copies of your exchanges
- Intralinks’ enhanced security options
- Creating and managing working sets
- Viewing exchange details
- Ensuring that members of your organization can download content from Intralinks exchanges

The exchange life cycle

Once your organization signs a contract (also known as an Enterprise Service Agreement, or ESA) with Intralinks, you or a colleague is contacted by an Intralinks Client Services representative to create a business group. The business group includes all the people within your organization who will be responsible for creating and managing the exchanges associated with your contract.

After the business group is established, your Intralinks representative creates a template for you tailored for your industry segment. Once the template is in place, you can begin creating exchanges.

When you create an exchange, it is in the hold phase. During this time, you select the people — exchange users — who will have access to the exchange and assign exchange roles to each of them. During the preparation phase, your team members add documents and folders to the Intralinks exchange and prepare it for use by reviewers. When you are ready for reviewers to begin reading the documents on the exchange, you move it to the open phase.

For more information about phases, see “Moving an exchange from one phase to another” on page 24.
Working with your Intralinks representative

The exchange creation process is a collaborative effort between the people who will manage the exchanges and Intralinks employees, generally referred to as Intralinks administrators.

Tasks that must be performed by an Intralinks employee

An Intralinks employee, generally referred to as an Intralinks administrator, must perform a few key steps in the exchange setup process. These steps include:

- Creating a business group for your organization
- Creating one or more templates that will be used as the starting point for creating exchanges
- Changing certain options, such as those for enhanced security, document protections, full-text document search, and the ability to log in more than once at the same time

Tasks you can perform

Depending upon the specific rights assigned to you, as an exchange manager you can perform most of the tasks needed to create and maintain your exchanges. These include:

- Updating templates
- Creating exchanges
- Adding and removing contacts (exchange users)
- Adding members to your business group

The specific rights available to business group members are described in the next section, “Working with your business group.”

Working with your business group

Although an Intralinks administrator must create a business group for you, you must decide who among your coworkers are to be members of the group, along with the positions they will hold. These positions are referred to as business group membership levels.

Business group membership levels

There are six levels of membership in an Intralinks business group:

**Coordinator** — Members at this level can update templates and contact records. They can view all templates associated with the business group, update them and use them to create new exchanges. Coordinators can view the records for all contacts and add and remove contact records. Coordinators can give business group membership to people on the contact list.

**Member 50** — Members at this level can update templates, but have more limited control over contact records than coordinators do. They can view all templates
associated with the business group, update them and use them to create new exchanges. Member 50 members can view the records for all contacts and add and remove contact records.

**Member 40** — Members at this level can view all templates associated with the business group and use them to create new exchanges. Member 40 members can view the records for all contacts and add and remove contact records.

**Member 30** — Members at this level can view the records for all contacts and add and remove contact records. Member 30 members cannot view or modify templates, nor can they create exchanges.

**Member 20** — Members at this level can view all templates associated with the business group, update them and use them to create new exchanges. Member 20 members cannot view or change contact records.

**Member 10** — Members at this level can view all templates associated with the business group and use them to create new exchanges. Member 10 members cannot view or change contact records.

**Contacts** — Contacts are not business group members, but they can be made group members by a coordinator. The people who appear in the contact list either were added directly to the list or have been given access to an exchange created by this business group. Contacts are not able to view templates or the contact list or create exchanges.

**Defining an exchange template**

Your Intralinks representative works with you and your business group colleagues to define the settings that will be used to create the templates that you will use to create exchanges. These templates speed the exchange creation process, since they provide default settings that are based on your organization’s industry segment and the organization’s particular needs.

Every business group needs to define at least one template, but your business group may have several templates depending upon the needs of your organization. As noted earlier, templates must be created by an Intralinks employee.

For information about individual settings used on templates and exchanges, see Appendix A, *Exchange settings*, on page 194.

**Creating an exchange**

If you have a business group membership that is anything other than Member 30, you can create new exchanges using the steps in the following procedure.

**Note:** If the exchange that you want to create is similar to an existing exchange, you can make a copy of (“clone”) the existing exchange using Intralinks Designer, and then modify the copy as needed. For more information, consult the *Intralinks Designer User Guide* or the help system that accompanies Intralinks Designer.

**To create an exchange**

1. **If you are viewing the Hub:** Click the **IL5 Hub** button on the left side of the screen. The **IL5 Hub** is displayed.
If you are viewing an exchange: Roll your mouse over the exchange name in upper left corner of the screen and select IL5 Hub from the list that appears. The IL5 Hub is displayed.

2. Select new exchange from the list of commands on the left side of the screen. The new exchange settings screen is displayed.

3. From the template list, select the template you want to use for the new exchange. The names of your organization and business group are displayed, along with your Intralinks contract number. The settings selected on the template appear, as well.

4. In the exchange name field, enter a descriptive title for the new exchange.

   To ensure that the exchange name will be displayed correctly in Intralinks Drive and other Intralinks applications, we recommend that you do not use the following characters: ?*:/<>|n

5. Review the settings. When you are satisfied with the selections, select save from the list of commands at the left side of the screen.

For information about individual settings, see Appendix A, Exchange settings, on page 194.

After you have created an exchange, you must add users and documents to it before making it available. For more information, see Chapter 4, Managing users and groups, on page 41 and Chapter 5, Publishing documents, on page 60.

Creating an exchange splash screen and footer

You can create a splash screen that appears when users enter your exchange. Depending upon your selections, the splash screen will appear every time a user enters the exchange, only the first time the user enters the exchange, or never.

Splash screens can be used to welcome new users to the exchange and to reinforce your corporate brand. Splash screens often include non-disclosure agreements or similar legal statements that are meant to discourage exchange users from sharing information on the exchange improperly.

Unlike a splash screen, the footer always appears at the bottom of your exchange, regardless of the screen that is displayed. Footers typically are used to provide branding and links to information elsewhere on the Internet that is relevant to your exchange users. Bear in mind that all users, regardless of their exchange role, can see the footer, so avoid including links that are inappropriate for some groups within the exchange. In addition, the footer provides contact information for Intralinks customer support; this information cannot be removed or changed.

To create or modify an exchange’s splash screen and footer

The Hub should be displayed.

1. Locate the exchange that you want to update, and right-click on it. A menu appears.

2. Select View Exchange Properties.

3. If a splash screen appears, review the information that appears on the screen, then select continue or accept. The settings screen for the selected exchange appears.
4. Select **footer/splash** from the list of commands on the left side of the screen. The existing splash screen, if one exists, is displayed.

5. Select **update** from the list of commands on the left side of the screen.

6. Make the required changes.

7. Click **save**. The updated splash screen is displayed.

8. Click **close**. The settings screen reappears.

To return to Intralinks Platform, click **close** in the menu on the left side of the screen.

### Making changes to email alerts

When new or existing Intralinks users are invited to your exchange, an alert message is emailed to them. Likewise, when a document is added or updated, users can be alerted by email. Intralinks provides standard text for these messages, but you can add notes of your own to these messages.

In addition, you can select what will be displayed in the From: line on these messages. You can display Intralinks’ name, the name of organization that is hosting the exchange (that is, your organization), the name of the person sending the message, or the business group.

This task is optional.

#### To add notes to email alerts

**Note:** If enhanced security has been applied to the exchange, you must open the exchange before beginning this procedure. If you do not, you will not be able to access the exchange’s **settings** screen.

The **Hub** should be displayed.

1. Locate the exchange whose alerts you want to change, and right-click on it. A menu appears.

2. Select **View Exchange Properties**.

3. If a splash screen appears, review the information that appears on the screen, then select **continue** or **accept**. The **settings** screen for the selected exchange appears.

4. Select **alerts** from the list of commands on the left side of the screen. The standard alerts text and any existing notes are displayed.

5. Select **update** from the list of commands on the left side of the screen.

6. From the **from** list for each type of message, select the person or group that should appear in the From: line on email alerts.

7. Review the standard text that appears for each of the alerts and add notes if needed.

8. Click **save**. The **alerts** screen reappears.

9. Click **close**. The **settings** screen reappears.

To return to Intralinks Platform, click **close** in the menu on the left side of the screen.
Moving an exchange from one phase to another

Exchange phases determine which exchange users have access to the exchange. Phases are used to ensure that no one has access to the exchange until you’re ready for them to use it.

There are three exchange phases:

**Hold phase** – This is the initial phase that is used while the exchange is being set up by exchange managers. Use this phase to add the users who will take part in the preparation and open phases. You also can add folders and documents. Publishers and reviewers do not have access to the exchange while it is in the hold phase, so this phase also can be used to temporarily close the exchange to these users, if necessary.

**Preparation phase** – In this phase, publishers are given access to the exchange. During the preparation phase, publishers and managers add the folders and documents that will be viewed by reviewers in the open phase. Reviewers do not have access to the exchange during the preparation phase.

**Open phase** – All exchange users are free to use the exchange.

Although exchanges typically begin their life cycle in the hold phase and end it in the open phase, you are free to move the exchange among these phases as your business needs dictate.

**To move your exchange from one phase to another**

Only individuals with one of the manager exchange roles or the Publisher Plus exchange role can change an exchange’s phase.

The **Hub** should be displayed.

1. Locate the exchange whose phase you want to change, and right-click on it. A menu appears.
2. Select **View Exchange Details**. The **Details** screen for the exchange appears.
3. From the **Phase** list, select the exchange phase you want.
4. Click **Save**.

An email alert message is sent to all exchange users who become active. For example, when you move an exchange from the hold phase to the preparation phase, users with the exchange roles of Publisher Plus, Publisher, Reviewer Plus and Previewer are alerted. When you move the exchange from the hold phase or preparation phase to the open phase, reviewers are alerted.

**Viewing and changing exchange settings**

For information about individual settings, see Appendix A, *Exchange settings*, on page 194.
To view settings for your exchange

1. In the Hub, locate the exchange whose settings you want to view, and right-click on it. A menu appears.
2. Select View Exchange Properties.
3. If a splash screen appears, review the information that appears on the screen, then select continue or accept. The settings screen for the selected exchange appears.

To return to Intralinks Platform, click close in the menu on the left side of the screen.

To change settings for your exchange

1. In the Hub, locate the exchange whose settings you want to change, and right-click on it. A menu appears.
2. Select View Exchange Properties.
3. If a splash screen appears, review the information that appears on the screen, then select Continue or Accept. The settings screen for the selected exchange appears.
4. Select update settings from the list of commands on the left side of the screen.
5. Make the required changes.
6. Click save.

To return to Intralinks Platform, click close in the menu on the left side of the screen.

Note that you are unable to change some of the settings that appear on the settings screen. Some settings are determined by the template that was used to create the exchange. Other settings can be changed only by an Intralinks administrator.

Enabling Intralinks Viewer

Intralinks Viewer is a secure document viewer that can be used to view protected and unprotected PDF and Microsoft Office documents. Intralinks Viewer is an alternative to Adobe Reader and similar tools.

Intralinks Viewer can be enabled for each of the following file types:

- Portable Document Format (PDF)
- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint

Each of these file types can be enabled separately; you could choose to enable Intralinks Viewer only for Microsoft Word, for example. You can choose to make Intralinks Viewer available only for protected files, or for all PDFs and Microsoft Excel, Word and PowerPoint files on the exchange. You can choose to require that Intralinks Viewer be used by all viewers, or you can give exchange managers the option to view documents in their native application. For Microsoft Office
documents, you can give users the option to view the documents in either Intralinks Viewer or Acrobat Reader.

Users can print protected documents displayed in Intralinks Viewer, if Protect/No Print was not selected when the documents were protected.

If Intralinks Viewer is not used for unprotected files, they are displayed in a browser, Microsoft Excel, Word or PowerPoint, or Adobe Acrobat or Adobe Reader, depending upon how your exchange and each user's Adobe software are set up.

If you choose to use Intralinks Viewer only for protected files, other files will be displayed in a browser, Excel, Word, or Adobe Acrobat or Adobe Reader, depending upon how each user's browser and Adobe software are set up.

Intralinks Viewer must be enabled by an Intralinks administrator. If you want to use Intralinks Viewer with your exchange, contact your Intralinks sales representative for assistance.

For more information about Intralinks Viewer and its capabilities, see “Viewing PDF and Microsoft Office documents using Intralinks Viewer” on page 114.

Using Intralinks Viewer to track users’ viewing time

Intralinks Viewer’s time tracking capability makes it possible for exchange managers to determine how much time each exchange member and group have viewed each document on their exchanges. This information appears on a number of reports.

Time tracking is available automatically on exchanges for which Intralinks Viewer is enabled. Time tracking is most effective in exchanges that do not allow users to view documents in applications other than Intralinks Viewer.

Time tracking information is available only for documents opened after the December 2013 release of Intralinks Platform was introduced. No information is available before that date. Time is tracked for PDF, Microsoft Word, Excel and PowerPoint formats. Other document types cannot be displayed in Intralinks Viewer, and as a result no viewing information is not available for them.

How time tracking works

When a user opens a document in Intralinks Viewer, a message appears asking the user to click on it. When the user clicks on the message, the document is displayed and time tracking for the document begins.

Time will continue to be tracked if network connectivity is temporarily lost; if connectivity is lost for an extended period of time, time tracking will stop at the point at which network connectivity was lost and the connection to Intralinks Platform ended. Tracking also will be halted if the user minimizes the Intralinks Viewer window, logs out of Intralinks Platform or allows his or her session to expire. Tracking for the document will resume when the document is reopened. If a user logs into Intralinks Platform multiple times using different computers and opens the same document twice at the same time, the amount of time each document instance is displayed will be counted.

The time required to open and display documents is not tracked. Only the time that users actually view documents is included in viewing counts.
Times is tracked in hours, minutes and seconds. If a user experiences a system crash while viewing a document, the time tracked may be up to a minute less than the actual viewing time because of the frequency with which viewing time is recorded.

**Viewing time tracking information**

The following reports display information about users’ document viewing time:

- Document Access Report
- Group Coverage Report and Multi-group Coverage Report
- User Coverage Report and Multi-user Coverage Report

On the Document Access Report, the **Total View Time** column provides information about users’ viewing activities.

On the Coverage reports, the Show list includes a **Total View Time** option for exchanges on which Intralinks Viewer has been enabled. The documents that have been viewed most appear at the top of these reports. 00:00:00 is displayed for documents that have not been viewed at all in Intralinks Viewer.

**Setting up document tags**

You have the option of using tags to organize the documents on your exchange. If you take advantage of this functionality, exchange managers and publishers can assign tags — words or phrases that describe the contents of your documents — to documents using the New Document Wizard. These tags offer great flexibility in classifying and organizing information in ways that are meaningful to your organization. For example, using tags you can classify and locate documents dealing with Canadian commodity contracts no matter where they are located in the exchange. Tags can be added, changed or removed at any time for one or multiple documents. The tags that are assigned to documents appear in the documents list, and users can use them when searching for documents. Up to 25 tags can be assigned to each document.

Intralinks provides predefined sets of tags that are tailored for your market segment. You can edit the tags in these sets, as well as edit or remove existing tags to create a collection of tags that makes the most sense and provides the greatest value to your organization and the users of your exchange.

Tags are organized into *sets*. These are simply related groups of tags that are organized to make it easier for you to find the tags you want when applying them to documents. All the tags for your exchange collectively are known as a *tags collection*. As a best practice, we recommend that you create sets for languages other than English before adding tags in those languages.

In order for you to use tags, the **Tags** exchange setting must be marked. You also must review and publish the tags collection for the exchange.

**To view the tags on your exchange**

1. Roll your mouse over the **Maintenance** tab at the top of the screen. A menu appears.
2. Select **Exchange Tags**. The tags currently set up for your exchange are displayed.
To add a set
1. Display the tags for your exchange. Highlight the Tags folder or, if you want for the new set to appear within another set, highlight that set.
2. Click the Add Set button at the top of the screen. The Add Set screen appears.
3. Enter a descriptive title for the set.
4. Click Add.
The set appears in the tags list.

To change the name of a set
1. Highlight the set that you want to change.
2. Click the Edit Set button at the top of the screen. The Edit Set screen appears.
3. Enter the new title for the set.
4. Click Save.
The set's new name is displayed in the tags list.

To add a tag
1. Display the tags for your exchange.
2. Highlight the set to which the tag will belong. The tag will appear inside this set.
3. Click the Add Tag button at the top of the screen. The Add Tag screen appears.
4. Enter a descriptive title for the tag.
5. Click Add.
The tag appears within the selected set in the tags list.

To change the name of a tag
1. Highlight the tag that you want to change.
2. Click the Edit Tag button at the top of the screen. The Edit Tag screen appears.
3. Enter the new title for the tag.
4. Click Save.
The tag's new name is displayed in the tags list.

To delete a tag or set
Note that if you delete a set, all the tags within the set are removed, as well.
1. Highlight the tag or set that you want to remove.
2. Click the Delete Selection button at the top of the screen. A message appears asking you to confirm your selection.
3. Click Delete.
**To activate the tags collection**

Note that once tags are activated, or *published*, they cannot be inactivated.

1. Display the tags for your exchange.
2. Click the **Publish** button at the top of the screen. (If this button is dimmed, the tags have been published already.)

Tags now can be assigned to documents.

**Setting up custom fields**

Custom fields provide you with a structured way to describe your documents, exchange groups and exchanges in greater detail. Custom fields enable you to enter specific pieces of information, such as expiration dates, locations, and the like. These fields can be used to print reports. They also can be used in some business processes to select documents, users and other items that share common attributes. In the past you may have used the **Notes** field to keep track of this information; with custom fields you can more easily manage the information and ensure that it is entered consistently.

You can assign values to custom fields for documents, folders and groups as you add them to your exchange. To assign values to the custom fields for the exchange itself, see “Setting custom field values for exchanges” on page 34.

Intralinks provides you with a set of preconfigured custom fields. Some fields are marked “Read Only” and cannot be changed. You can change the labels (names) that appear onscreen for custom fields if you like; your changes will affect all the members of the exchange. You can disable the fields that you do not wish to use (if they are not read only), and you can add new custom fields if the existing fields do not meet your needs.

Custom fields are based on the following field types:

- **String**: Fields of this type enable you to enter any text you like (alphabetic and numeric characters and symbols)
- **Date**: For date fields you can enter a date or select it from a pop-up calendar.
- **Numeric**: Only numbers can be entered into numeric fields.
- **Options**: With this type of field (also known as a multi-selection list), you can select one or more pre-defined items from a list. (To select multiple items, press the **SHIFT** key while clicking them.)

In order for you to use custom fields, the **Custom fields** exchange setting must be marked and the custom fields collection must be *published* (activated) on the exchange. If you manage multiple exchanges, you may have a different set of custom fields for each exchange.

Users with the following roles automatically are allowed to set an exchange’s custom field values: Manager Plus, Hidden Manager Plus, Manager, Publisher Plus. Users with the Manager Limited and Publisher role can be given permission to set documents’ custom fields’ values, as well, depending upon these users’ permissions for the documents themselves.
To view and define custom fields

Use this procedure to view the custom fields for your exchange and to change their attributes.

1. Roll your mouse over the Maintenance tab at the top of the screen. A menu appears.
2. Click Field Definitions. The custom fields for your exchange are displayed.
3. Use the panel on the left side of the screen to display the particular fields that you wish to view or modify.

Using this screen, you can enable custom fields and mark them as required or read only. You also can change the order in which they appear by dragging each field to the location that you want.

You also have the ability to hide read-only fields on screens used to configure naming conventions and business processes, and well as those that apply to documents, groups and exchanges. Read-only custom fields that have been hidden are no longer required. Hidden fields do not appear for users with exchange roles other than Manager Plus. For users with the Manager Plus exchange role, the following rules apply:

- Fields that are hidden will not appear in new naming conventions, business process configurations, documents, groups or exchanges.
- In existing standard, rules-based and multi-task business process configurations in Draft status, hidden fields are visible and their values can be removed. If the values are removed, the fields will no longer be available onscreen once the configuration is saved.
- Hidden fields will not appear for documents, groups or exchanges for any new business process configurations.

Note: You can make some modifications to existing custom fields only if there are no naming conventions or process configurations on the exchange. These modifications include making a Read Only field editable, making a field required (or not required), and disabling the field.

To rename custom fields

Users with the Manager Plus exchange role can rename required and read-only fields including those already being used by business processes. The changes are applied after you log out of Intralinks Platform and log back in. The changes are not visible on the Owner and Target views of process configurations.

1. Roll your mouse over the Maintenance tab at the top of the screen. A menu appears.
2. Click Field Definitions. The custom fields for your exchange are displayed.
3. Use the panel on the left side of the screen to display the particular field that you want to rename. Click on the field to highlight it.
4. From the More Actions menu, select Properties. The Properties screen for the field appears.
5. In the Label field, enter the new name for the field.
6. Click Save.
To change the options that appear in custom fields’ option lists

You can change the list of values that appears for fields with the type of Options.

Note that custom fields identified as Read Only cannot be changed.

1. Roll your mouse over the Maintenance tab at the top of the screen. A menu appears.
2. Click Field Definitions. The custom fields for your exchange are displayed.
3. Use the panel on the left side of the screen to display the particular field that you want to edit. Click on the field to highlight it.
4. From the More Actions menu, select Values. The Values dialog box appears.
5. To add an option, click Add Option. To edit an existing option, highlight it and then click Edit Option. A dialog box appears, allowing you to add or edit an option.
6. To delete an option, highlight it and click Remove Option. A message will appear asking you to confirm your selection; click Remove.
7. When you have finished making changes, click OK to close the Values screen.

To add a new custom field

Be sure that the exchange that you want to change is displayed.

1. Roll your mouse over the Maintenance tab at the top of the screen. A menu appears.
2. Click Field Definitions. The custom fields for your exchange are displayed.
3. If you want the new custom field to be a child field of an existing field, highlight the field that will be its parent field.

Child fields are secondary fields; that is, they appear only if the parent field has been selected, and they typically provide more detail about the parent field.

If you do not want the field to be a child field, do not highlight any custom fields.
4. Click the Add New Field button at the top of the screen. The Properties view of the Add Custom Field wizard appears.
5. Name the field.
6. Select the type of field that you wish to create:

   - Options — Select this option if you want to provide users with a pre-defined list of choices. Users will be able to choose one or more of the options in the list, but they will not be able to add new options.
   - String — This field type also is known as a text field. It is the most flexible of all the field types. Select this field if you want users to type their answer. They will be able to make entries using alphabetic and numeric characters and symbols.
• **Date** — Select this field type if you want users to provide a date. Users will be able to enter a date or select it from a pop-up calendar.

• **Numeric** — Select this option if you want users’ entries to include only numbers.

7. Click **Next**. The **Values** view of the Add Custom Field wizard appears.
   
   If you selected **Options** in step 6, continue on to step 8. If you selected any other field type in step 6, click **Next** and skip to step 9 below.

8. To add an option, click **Add Option**. A dialog box appears, allowing you to add an option. Enter the name of the option and click **Save**. Add all the options that are needed for this field.
   
   If you make a mistake while adding a field, you can edit or delete it. To do this, highlight it and click either **Edit Option** or **Remove Option**. A message will appear asking you to confirm your selection; click **Remove**.
   
   Mark the **Enable** option for each option and then click **Next**. The **Permissions** view of the Add Custom Field wizard appears.

9. Enter a default value for the custom field.
   
   In most instances, default values are optional; however, you must set default entries for required fields if they will be set to **See** or **No Permission** for any exchange roles or individuals. Required fields are indicated by an asterisk (*) next to their names.
   
10. Review each exchange role displayed (Manager, Reviewer, etc.) and change the access level as needed. Access levels include:
    
    **Control** — Users given this permission can view the custom field and change the value selected for it.
    
    **See** — Users given this permission can view the custom field, but they cannot make any changes to the value that is displayed.
    
    **No Permission** — Users who are not given any custom field permission can neither view the field nor make changes to the value selected for it.
    
    Users with the Manager Plus role automatically have the ability to control custom fields.
   
11. When you have finished making changes, click **Save**. The new field appears in the custom fields list.
   
   The new field is not enabled. Be sure to enable it, and mark it as Read Only or Required if necessary.

▶ **To disable and enable individual custom fields**

Note that custom fields identified as Read Only cannot be disabled.

By default, all custom fields are enabled and will be available when the custom fields are published. You can disable fields that you will not use. If you change your mind later, you can enable the fields again.

1. Roll your mouse over the **Maintenance** tab at the top of the screen. A menu appears.
2. Click **Field Definitions**. The custom fields for your exchange are displayed.
3. Highlight the custom field you want to disable (or enable).
4. Click the **Disable** (or **Enable**) button at the top of the screen.

**To activate (publish) all custom fields**

Note that once custom fields are activated, or *published*, they cannot be inactivated.

1. Display the custom fields for your exchange.
2. Click the **Publish** button at the top of the screen.

Custom fields now can be applied to documents.

**Note:** If the custom fields cannot be published (both the **Draft** and **Publish** buttons are dimmed), check to be sure that the fields that you want to use have been enabled. If none of the fields have been enabled, the collection cannot be activated.

### Setting default values and access levels for custom fields

You can prevent users with specific exchange roles (such as publisher or reviewer) from changing the values for custom fields, or from viewing the custom fields altogether. (You cannot restrict users who have been assigned the Manager Plus role.) This can be especially useful for custom fields that are used to trigger business processes; by limiting who can change custom field values, you can ensure that the process workflow is not altered and prevent errors from occurring.

You also can set default (suggested) values for custom fields. These default selections will appear as suggestions to users whose custom field permission allows them to control the custom field, and as automatic entries for users whose role allows them to see but not change the custom field.

**Important!** If you choose to prevent any exchange roles from seeing or changing custom fields values for any fields, you **must** set default values for those fields.

**To set the default value and access rights for a custom field**

1. Roll your mouse over the **Maintenance** tab at the top of the screen. A menu appears.
2. Click **Field Definitions**. The custom fields for your exchange are displayed.
3. Highlight the custom field that you want to edit.
4. From the **More Actions** menu, select **Permissions**. The **Permissions** screen for the selected field appears.
5. Enter a default value for the custom field.

In most instances, default values are optional; however, you **must** set default entries for required fields if they will be set to **No Permission** for any exchange roles or individuals. Required fields are indicated by an asterisk (*) next to their names.

6. Review each exchange role displayed (Manager, Reviewer, etc.) and change the access level as needed. Access levels include:

   **Control** — Users given this permission can view the custom field and change the value selected for it.
See — Users given this permission can view the custom field, but they cannot make any changes to the value that is displayed.

No Permission — Users who are not given any custom field permission can neither view the field nor make changes to the value selected for it.

Users with the Manager Plus role automatically have the ability to control custom fields.

7. When you have finished making changes, click Save.
Repeat steps 3 through 7 for every custom field you wish to update.

Setting custom field values for exchanges

Exchange custom fields can be used to define a variety of attributes for exchanges, including the geographical regions in which they are used, their purpose, and so on. If you plan to use naming conventions to automatically rename documents as they are added to your exchange, you can incorporate the exchange custom fields’ values into the document names. For more information about naming conventions, see “Using naming conventions to standardize document names” on page 87.

To set custom field values for an exchange

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Place the mouse pointer over the exchange whose details you want to view. A menu of options appears.
2. Select View Exchange Details. A screen appears displaying information about the exchange.
3. One or more custom fields appear below the Name, Host, ID and Phase fields. Make an entry for every field that applies to this exchange. As you make entries, additional fields may appear.
4. When you have finished making your entries, click Save.

Ordering archive copies of your exchanges

From time to time, you may want to have a copy of your exchange for reference or regulatory compliance purposes. You can order copies that will be sent to you on DVD or transferred to a secure FTP server on the Internet where you can download it. Archive copies provide a snapshot of your exchange at a particular point in time from a selected user’s viewpoint. Any documents that are unavailable to the selected user will not appear in the archive copy.

If all work involving the exchange has been concluded, you can request that the exchange be deleted.

Note: If your exchange is hosted in the United Kingdom (the Geo specific mount point exchange setting is set to UK), your archive copies will be created in the United Kingdom, as well. If the exchange setting is set to USA, the archive copies will be created in the United States.
To request an archive copy of your exchange

The Hub should be displayed.

1. Locate the exchange you want to be archived and highlight it.
2. From the Actions menu select Order Archive Copy. The Terms and Conditions for Intralinks Archive screen appears.
3. Review the terms and conditions, and click Agree to continue. A wizard appears.
4. In the first step of the wizard, indicate whether you want a compliance archive or a data archive. Compliance archives are replicas of the exchange from a particular user’s viewpoint; they contain nearly all the same information that can be found on the exchange. Data archive versions contain only folders and files in a Windows Explorer-style format, along with Q&A threads if Q&A is being used on your exchange.
5. Select the viewpoint that will be used for the archive copy. Click the Browse button to display a list of viewpoints that are available for this exchange. Highlight the viewpoint you want and click Add.
6. Select the number of copies you want.
7. Indicate whether you want the exchange to be deleted. If you select Yes, the exchange will be deleted in 30 days, and billing for it will end.
8. Select the delivery mode, DVD or FTP.
9. Click Next. The Delivery Details step of the wizard appears.
10. Review the information at the top of the screen and then enter your delivery and billing addresses. If the delivery and billing addresses are the same, mark the Same as Deliver To option to copy your delivery address details to the billing address fields. If you want billing information to be taken from your organization’s contract with Intralinks, mark the Bill as Per Contract option. (If you are unsure about the billing address, use this option.)
11. Click Next. The Order Details step of the wizard appears.
12. Carefully review the information on the screen. If you are satisfied with the order details, click Submit. Your request will be sent to Intralinks for fulfillment.
   
   If changes are required, click the Back button to make them, then return to this screen to submit your order.

After you have submitted your order, a confirmation message appears, and a confirmation email message is sent to the address you entered in the delivery details step.

To view a list of archive copy orders that you have submitted

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the Maintenance button. Additional options appear.
2. Click on Archive Requests. A list of the orders you have submitted for archive copies is displayed.
Creating working sets

A working set is a collection of exchanges, users, groups or documents that you can use for performing tasks and printing reports. The working sets that you create are visible only to you.

All working sets can be used to print Access Reports showing information for all the objects (exchanges, users, groups or documents) in the working set. In addition, you can use exchange working sets to request documents for submission or review. You can use group working sets to copy groups into selected exchanges. You can use document working sets to copy documents into selected exchanges.

To create a working set

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Using the tabs on the left side of the screen, display the list of items (exchanges, groups, users or documents) that you want to include in this working set.
2. Highlight the items that you want to include in the working set. To select multiple exchanges, press and hold the SHIFT or CTRL key while you click each item.
3. From the Actions menu, select Add to Working Set. The Working Set screen appears.
4. Click Create new Working Set. A window appears.
5. Enter a name and description for the working set.
6. Click Save.
7. Click Save to close the Working Set screen. The new working set appears in the Hub.

To add items to an existing working set

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Using the tabs on the left side of the screen, display the list of items (exchanges, groups, users or documents) that you want to include in this working set.
2. Highlight the items that you want to include in the working set. To select multiple exchanges, press and hold the SHIFT or CTRL key while you click each item.
3. From the Actions menu, select Add to working set. The Working Set screen appears.
4. Select the working set to which the items should be added.
5. Click Save.
To remove a working set

You can locate working sets using Saved Searches on the Hub. For example, to view your document working sets, click the Documents tab on the Hub, and then click the Document working sets link in the Saved Searches box.

1. Locate the working set that you want to remove, and highlight it.
2. From the Actions menu, select Remove.

Using public working sets

Public working sets can be used by multiple users who perform the same tasks across a shared group of exchanges. Each public working set can be used by up to 50 predefined users. This ensures that tasks based on the working sets are performed consistently and accurately. Public working sets also can be used for reporting purposes.

Public working sets must be created by an Intralinks employee, but once they have been created, you can add and remove both users and exchanges to them.

The users who are added to a public working set must have access to the exchanges included in the working set in order to perform tasks using the set.

You can add exchanges to a public working set using the same steps that you use for updating a personal working set. For more information, see “To add items to an existing working set” on page 36. To add users to a public working set, follow the steps in the procedure below.

To add users to a public working set

Note: You can make changes to a public working set only if you have been given control privileges for the set. Also, the people that you add to the set must be Intralinks users already. To add new users, follow the steps in “Adding users” on page 48, then add them to your working set.

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. If the Exchanges tab is not selected, click it to display a list of exchanges and working sets that are available to you.

   To view only your working sets, click the Exchange working sets link in the Saved Searches box.

2. Highlight the public working set that you want to update.

3. From the Actions menu, select Properties. The Properties tab for the public working set appears.

4. Click the Users tab. A list of users who have been assigned to the working set is displayed.

5. Click Add Users. The Add Users to Working Set screen appears.

6. Enter the email address for a user who will be given access to the working set, and click Add. The user’s name appears in the Selected Users list.

7. Repeat step 6 for each user that you wish to add to the set. A maximum of 50 users can be assigned to any given working set.
8. When you have finished adding users, click **Done**. The **Users** tab reappears.

9. Using the **Permissions** column, indicate whether each user will be able to see the working set or control it.
   - **See** — The user can use the working set to perform tasks, but cannot make any changes to it.
   - **Control** — The user can use the working set to perform tasks. In addition, he or she can add and remove users and exchanges and view history information for the working set.

10. Review the information displayed in the **Exchange List Error** column. It lists any exchanges for which each user does not have access privileges. In order for users to be able to use this working set, they must be given access to all the exchanges in the list.

    You can quickly update users' access to exchanges using the **Manage Exchanges** screen. For more information, see "Managing an individual user’s access to multiple exchanges" on page 55. Once a user has been given access to all the exchanges in the working set, the set will become available to the user.

11. When you have finished setting permissions and reviewing exchange access issues, click **Save**.

▶ **To remove users from a public working set**

   **Note:** You can make changes to a public working set only if you have been given control privileges for the set.

   If the **Hub** is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select **Hub** from the list that appears.

   1. If the **Exchanges** tab is not selected, click it to display a list of exchanges and working sets that are available to you.

      To view only your working sets, click the **Exchange working sets** link in the **Saved Searches** box.

   2. Highlight the public working set that you want to update.

   3. From the **Actions** menu, select **Properties**. The **Properties** tab for the public working set appears.

   4. Click the **Users** tab. A list of users who have been assigned to the working set is displayed.

   5. For each user you wish to remove, click the red X icon that appears in the **Remove** column. The user’s name is removed from the list.

   6. Click **Save**.

**Viewing exchange details**

You can display a screen that shows a variety of details about your exchange, including the name of the host organization, the exchange’s ID and its current phase setting (hold, preparation or open), as well as the custom field selections, if any, that have been made for the exchange.
The **Mobile Settings** tab allows you to control whether this exchange will be available in Intralinks mobile apps. If you allow mobile users to access the exchange, you can choose to prevent them from opening protected documents.

Intralinks offers mobile apps for iPad and iPhone and for Android devices. These apps can be downloaded from Apple’s App Store and from Google Play.

### To view details for an exchange

If the **Hub** is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select **Hub** from the list that appears.

1. Place the mouse pointer over the exchange whose details you want to view. A menu of options appears.
2. Select **View Exchange Details**. A screen appears displaying information about the exchange.
3. When you have finished viewing the information, click **OK** to close the screen.

### To manage access on mobile devices

If the **Hub** is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select **Hub** from the list that appears.

1. Place the mouse pointer over the exchange whose details you want to view. A menu of options appears.
2. Select **View Exchange Details**. A screen appears displaying information about the exchange.
3. Click the **Mobile Settings** tab.
4. To give users the ability to view the exchange in Intralinks’ mobile apps, mark the **Access exchange on mobile devices** option. If you mark the selection, additional options become available.
   - If you do not want for the exchange to be accessible on mobile devices, be sure this option is unmarked
5. If you want to allow users to open unprotected document in third-party mobile apps like GoodReader, mark the **Allow other applications to open non-protected documents on mobile devices** option.
6. If you want to allow users to view protected documents on mobile devices, mark the **Allow protected documents to be viewed on the mobile device** option. If you mark this option, protected documents can be viewed only within the Intralinks mobile apps.
7. When you have finished making your selections, click **OK**.

### Ensuring that members of your organization can download content from Intralinks exchanges

To ensure that users will be able to download files from Intralinks exchanges and other Intralinks services, be sure that `download.intralinkscontent.com` has been added to the exception list for any web filtering solutions that your organization has in place. Downloads are available only from this URL. If users are unable to access this URL, their ability to download data from Intralinks services will be impacted.
Use this link to test access from any web browser:
https://download.intralinkscontent.com/ui/domainCheck.html
Chapter 4: Managing users and groups

Overview

Read this chapter for information about:

• The types of groups provided in Intralinks, and how they can be used
• The workflow for adding users and groups
• Creating, modifying and removing groups
• Users’ exchange roles, and how to change them
• Group member roles
• Adding and removing exchange users
• Recommending that users be added to exchanges
• Using groups to organize users
• Moving users from one group to another
• Removing users from an exchange
• Removing groups
• Managing users’ access to multiple exchanges
• Copying groups from one exchange to another
• Finding users
• Resending welcome alerts to exchange members

Before you begin

In order to perform the tasks in this chapter, Adobe Flash Player 9 must be installed on your computer.

When you select an Intralinks Platform exchange in the Intralinks Hub, a message will appear if Flash Player 9 is not installed. This message includes links to information about the Flash Player software and to a location on the Adobe website where you can download this free software utility. Your organization’s IT department may be required to install this software for you.

If Flash Player 9 is not installed, you can open the exchange, but you will be able to perform only basic reviewer-related tasks like reading and printing documents.

Getting started with user groups

User groups provide an easy way for managers and publishers to assign permissions for documents to users who share some common characteristics. Most often the members of a group all belong to a single organization. In the case of exchange groups and collaboration groups, it is possible for people from different organizations to be included in the same group. Permission to view and work with documents is assigned by group, speeding the permissioning process and reducing the opportunity for errors.
In Intralinks, the following types of user groups may be available:

- **Exchange groups** — Exchange groups are perhaps the most flexible type of user group for exchange management purposes; these groups are used solely to speed permissioning for documents and comments. Users can be added and removed from these groups at any time, can have any exchange role and can belong to more than one organization. Users can be included in any number of exchange groups. These groups are purely a management tool; members don’t gain any rights or responsibilities simply by being a member of the group.

- **Collaboration groups** — This type of group is available only if the collaboration group exchange setting is marked (on). Collaboration groups can include members with any kind of exchange role; all the members of the group can see one another regardless of their exchange roles.

  **Important!** All members of collaboration groups, including those with the exchange role of Hidden Manager Plus, are visible to one another, regardless of their exchange roles. If a user with the role of Hidden Manager Plus is added to a collaboration group, that person is visible to all the other members of the group.

Users can belong to multiple exchange or collaboration groups.

**Creating and managing groups**

Use the procedures in this section to create, update and modify groups.

**Using the Add Group Wizard**

▶ **To add a group to the exchange**

The **Users & Groups** tab should be displayed.

**Set properties for the group**

1. Click the **Add Group** button at the top of the screen. The **Set Properties** view of the Add Group Wizard appears.

2. Enter a name for the group.

3. Select the type of group you are creating.

   - **Exchange Group** — Select this group type if you simply want to give the group’s members access to documents and the members do not need to be visible to one another. Users with any exchange role can belong to an exchange group.

   - **Collaboration Group** — All members of collaboration groups can see one another, regardless of their exchange role.

4. (Optional.) You can add notes about the group if you like. These notes are for reference purposes only; they do not appear on reports.

5. Click **Next**. The **Details** view appears.
Enter details for the group

Use this screen to determine where the group’s documents will be stored and whether the group can perform detailed document searches. Using custom fields, you also can further describe the group.

1. Using the **Group Folder** field, you can specify a folder that will be used to store documents that are submitted by members of the group using a document submission business process, or that are identified as being owned by the group. If no group folder is specified, documents will be published to the folder specified in the business process configuration. Click **Browse** to select the folder that will be used for this group.

   This field is optional; if you do not plan to use document submission business processes or allow groups to own documents, you can skip this field.

2. (Optional.) If document content searching (full-text searching) is enabled for this exchange, you can give the group the ability to perform searches on documents’ contents, notes entered for documents and folders, and the titles of documents and folders. To do so, mark the **Allow group members to search document content** option.

   If this option is unmarked or if it does not appear, group members will be able to search only the titles of documents and folders.

3. Click **Next**. If custom fields have been enabled for this exchange, the **Custom Fields** view of the Add Group Wizard appears; continue to the next step. If custom fields are not being used, the **Choose Members** view of the wizard appears; in this case, skip to “Assign users to the group” on page 43.

   Custom fields can be used to print reports. They also can be used in some business processes to select documents, users and other items that share common attributes. For more information about custom fields, see “Setting up custom fields” on page 29.

4. The fields that appear on this screen vary depending upon the industry type that was selected for the template that was used to create your exchange. Make an entry for every field that applies to groups on this exchange. We recommend that you enter information consistently for every group to ensure accuracy when you print reports for your groups.

5. Click **Next**. The **Choose Members** view appears.

Assign users to the group

If you have not yet added users to the exchange, skip to step 2.

1. Highlight each user’s name in the list on the left side of the screen and click the arrow button to move the name to the group members list on the right.

   To include all members of a particular organization, highlight the folder for the organization and click the arrow button. All members of the organization appear in the group members list on the right side of the screen.

   You also can highlight one or more users’ names and drag them from one list to the other.

   If most or all of the users assigned to the exchange belong in this group, click the **Add All Users** button. All users’ names will appear in the list on the right.
Then highlight the names of any users who do not belong in the group and click the arrow button . These individuals are removed from the group.

2. Click Next. The Choose Members view appears.

Review member details

1. Review details about the group members that you have selected. If group member roles are being used with this exchange, select a group member role for the users who will perform particular functions within the group. These roles describe each member’s position within their organization or the function they perform as a member of your exchange.

   For more information about group member roles, see “Group member roles” on page 48.

2. Click Save. The Users & Groups list appears displaying the new group you created.

If you did not add users to the group in step 1, see “Adding users” on page 48 for information on adding users to the exchange and assigning them to the group.

Modifying group properties

After you have created a group, you can change the group’s name and add or edit a note about the group. If your exchange allows document content searching (full-text searching), you can add or remove this capability for the group.

To modify a group's properties

The Users & Groups tab should be displayed.

1. Locate the group you want to modify and highlight it.
2. From the Actions menu, select Properties. The Properties view of the group’s information screen appears.
3. Make whatever changes are required.
4. Click Save.

Viewing the members of a group

To view the members of a group

The Users & Groups tab should be displayed.

1. Locate the group you want to modify and highlight it.
2. From the More Actions menu, select Members. The Members view of the group’s information screen appears.
3. If you want to add members to the group, click the Add Members button. A list of all the users who have been added to the exchange appears; drag the members you want to add to the group list on the right.
4. Click Save.
Viewing the history for a user group

Use the following procedure to display a list of all the actions that have been made for a selected user group. The list includes information about the group’s creation, members who have been added and removed, and actions taken by members, such as accessing and exiting the exchange, viewing and printing documents and the like.

To view the history for a user group

The Users & Groups tab should be displayed.

1. Locate the group you want to modify and highlight it.
2. From the More Actions menu, select History. The History view of the group’s information screen appears.
3. To view a limited range of history, click in the Since field. A calendar appears; select the earliest date for which you want to see information.
4. To create a Microsoft Excel spreadsheet containing the currently displayed information, click the Export button. You can print the spreadsheet using Excel if you like.
5. Click Save.

Removing user groups

When you remove a user group from an exchange, you must decide whether the members of the group will be removed from the exchange, as well. Note that users will be removed from the exchange only if they do not belong to any other groups on the exchange. If you want to remove these users from the exchange, see “Removing users from the exchange” on page 55.

If you remove users from the exchange, there is no effect on other exchanges to which these users belong.

Alternatively, you can choose to remove the group, but not the group’s members. You may choose to do this if the group has become obsolete, but its members still have an interest in using the exchange. If the users are reviewers, assign them to other user groups to ensure that they can continue to work in the exchange. For more information, see “Assigning users to another group” on page 53.

To remove a user group

The Users & Groups tab should be displayed.

1. Locate the group you want to remove and highlight it.
   To select multiple groups, press the SHIFT or CTRL key while clicking the users’ names to highlight them.
2. Click the Remove Group button at the top of the screen.
3. A message appears asking you whether members of the group should be removed from the exchange, as well. Make your selection, then click Remove.
Users’ roles within an exchange

As mentioned in Chapter 2, *Getting started with Intralinks*, on page 9, *exchange roles* determine each user’s rights and responsibilities within an exchange. Users who are active in a number of exchanges may have a different role within each exchange.

(Note that exchange roles are different from *group member roles*, which are described on page 43.)

Exchange roles give great flexibility in enabling users to work efficiently. Exchange roles keep users focused on the tasks that are assigned to them. Each organization chooses the exchange roles that will be available in their exchange. Intralinks offers a total of nine exchange roles, though in practice few exchanges will contain all nine of those roles; a successful exchange could function with only two or three exchange roles.

Exchange roles can be divided into three broad types: *managers*, *publishers* and *reviewers*.

**Managers** — Managers are responsible for setting up and maintaining the exchange, with assistance from Intralinks Client Services. With a few exceptions, managers can perform all tasks within the exchange. They can publish documents, and they determine who has access to the exchange.

**Publishers** — Publishers assist managers by adding documents to the exchange. They may be responsible for setting permissions for the documents — that is, identifying the exchange users who are allowed to view, print and download each document. Publishers can see reviewers and other publishers. Publishers generally are from the organization that is hosting the exchange.

**Reviewers** — Reviewers are responsible for reading the documents that appear in the exchange. Reviewers generally can see and work with the people who were responsible for setting up the exchange, but they may not be able to see or work with one another. Most reviewers generally are not from the organization hosting the exchange.

**Manager exchange roles**

Exchanges can have as many as four types of managers, though most exchanges use only one or two manager exchange roles. Managers can participate in all phases of the exchange’s life cycle.

Manager roles include:

**Manager Plus** — This is the most powerful of all the exchange roles available in exchanges; users who are assigned this role are allowed to perform every task and to view all users on the exchange. This role is sometimes abbreviated as “manager +.” Most exchanges include users with this role.

**Hidden Manager Plus** — This exchange role is nearly identical to that of manager plus, but these managers will be hidden from users with publishing and reviewing exchange roles. That is, these managers’ names will not appear in lists of users viewed by publishers and reviewers. (They will be visible to other managers, however.) Hidden managers should be careful about posting documents or comments because these items *will* reveal their names to publishers and reviewers. This role sometimes is abbreviated as “(manager+).”
Manager – This exchange role is similar to that of manager plus, with one exception: users with this role may be given permission to delete and modify documents and comments. This role is seldom used.

Manager Limited – This exchange role is similar to that of manager plus, with one exception: users with this role must be given permission to add, delete and modify comments and documents. In addition, users with this role cannot create or update user groups. This role sometimes is abbreviated as “manager ltd.” This role is seldom used.

Publisher exchange roles
Exchanges can have up to two types of publishing exchange roles — though it is possible for an exchange not to have any members with publishing roles at all, since managers are able to perform all the tasks that are available to publishers. Publishers participate in the preparation and open phases of the exchange’s life cycle.

Publisher exchange roles include:

Publisher Plus – This exchange role is able to perform all tasks related to publishing and managing documents and comments. People with this role also can update user groups and exchanges settings for the footer and splash screen, and can change the exchange’s phase. People with this role can see all other users (except those with the hidden manager plus exchange role) and can be seen by all other users.

Publisher – People with this exchange role can post new documents and comments and can respond to the comments they have been given permission to see. These users may be given permission to modify or delete documents and comments. People with this role can see all other users (except those with the hidden manager plus role) and can be seen by all other users. This role is seldom used.

Reviewer exchange roles
Exchanges can have up to three types of reviewer exchange roles. These roles include:

Reviewer Plus – In addition to reviewing documents, users with this exchange role are able to add and remove reviewers from the exchange and create user groups. This role is rarely used.

Reviewer – People with this exchange role can view, print and download documents (subject to the restrictions set for each document). Previewers are active in the preparation and open stages of the exchange’s life cycle; they often are members of the organization hosting the exchange. Unless they are assigned to a collaboration group or a buyers group, previewers will not be able to see other reviewers or previewers taking part in the exchange.

Reviewer – People assigned this exchange role have the same rights as previewers, but are active only during the open phase of the exchange’s life cycle. Reviewers generally are members of organizations other than the organization hosting the exchange. In a typical exchange, most users will be reviewers. Unless they are assigned to a collaboration group or a buyers group, reviewers cannot see other reviewers or previewers taking part in the exchange.
Group member roles

*Group member roles* describe each member's position within their organization or the function they perform as a member of your exchange.

Group member roles are in addition to users' exchange roles (reviewer, manager, etc.). Group member roles can be used to define and drive business processes, as well as to organize and control access to your exchange's contents. These roles are optional and need not be assigned to all exchange members or to all members of a group. The group member roles available in your exchange have been preset and cannot be changed.

It is important to note that a user may belong to multiple groups and may be assigned a different group member role within each of those groups. If this is the case, the user will be assigned tasks only if the group member role assigned to him or her matches your selection here. Similarly, if the user has the same group member role within multiple groups, he or she will be assigned a separate task for each of those groups.

Adding users

If you have been assigned a manager exchange role of any type (Manager Plus, Hidden Manager Plus, Manager or Manager Limited) or the Reviewer Plus role, you can add users to your exchange.

Using the Add Users Wizard

You can add users using a five-step wizard.

▸ *To add users to the exchange*

The *Users & Groups* tab should be displayed.

*Select the users who will be added to the exchange*

1. Click the *Add Users* button at the top of the screen. The *Identify Users* view of the Add Users Wizard appears, and the *Select User(s)* tab is selected.

   You can use any combination of the techniques described in the next three steps to add users to the *Selected User(s)* list on the right side of the screen.

2. Select the user whom you want to add by entering the person's email address, name or organization. As you type, the names of users who match your entry are displayed. Highlight the name you want and click the arrow button to move the name to the list at the right. You can add as many names to the list at the right as you like.

   If you enter an email address that does not appear in Intralinks' Global User Directory (GUD), the *Add New User* tab appears, displaying the fields needed to add the user to the Global User Directory and your exchange. Enter the requested information, then click *Add*. The record is added to the directory and the new user's name is added to the list of users being added to the exchange.

3. If you want to import users from another Intralinks exchange, click the *Import Users* tab, then click *Choose* to display the *Select Source Exchange* screen. Highlight the exchange containing the users you want and click *Done.*
The names of all users on the selected exchange will appear on the Import Users tab. Highlight the users you want to add to this exchange and click the arrow button to move them to the Selected User(s) list.

4. If you want to track activities for a person who does not need to use your exchange, you can create a record that does not include the user’s email address. To do this, click the Add New User tab, then click the Add a user without an email address link below your list of contacts. A number of fields appear, enabling you to enter the information needed to add this user. Enter the requested information, then click Add. The new user’s name is added to the Selected User(s) list.

Exchange members without an email address cannot log into Intralinks, but you can assign them to groups, print reports for them and perform other tasks using their records. These users also can be assigned to business processes.

5. When you have selected all the users you wish to add, click Next. The Assign Roles view of the Add Users Wizard appears.

Select an exchange role for each new user

The users you selected on the previous screen appear in a list.

1. For each user, select an exchange role from the Role list.

   The exchange roles that appear in the list vary, depending upon how your exchange was set up. There may be as few as two or three roles in the list, or as many as nine. For more information about exchange roles, see “Users’ roles within an exchange” on page 46.

   If you want to apply the same role to multiple users, highlight the users’ names, then choose the role you want from the Apply to selected users list.

2. Click Next. The Assign to Groups view of the Add Users Wizard appears.

Assign each user to a group

The users you have selected in the previous steps appear in a list on the left side of the screen. The groups that have been created for this exchange appear on the right.

1. Drag each user’s name from the list on the left to the group to which he or she is being assigned.

   Group assignments are important because they determine which documents each user will be able to access, along with the level of security being applied to each group. All reviewers must be included in a group in order to work in the exchange.

   If the group you want has not been created yet If you discover that the group you want has not been created, click the Create Group button. The Add Group Wizard will open, allowing you to create the group. The Add Users Wizard will remain open, allowing you to continue adding this user once the group has been created. See “To add a group to the exchange” on page 42 for instructions for using the Add Group Wizard.

2. Click Next.
Send a welcome message to the users (optional)

You can send an email message welcoming the new users to the exchange if you like. A standard note is provided for you, but you can customize the note. Users will not receive the welcome message until the exchange is available to them. (For example, if the exchange is in the hold phase, reviewers cannot access it; they will receive a message when you change the exchange to the open phase.)

1. Review the list of users being added to the exchange. If you do not want for a particular user to receive a welcome message, unmark the checkbox that appears to the left of the person’s name. By default, all new users receive the message, and you receive a copy of it, as well.

2. If you want to change the subject of the welcome message or add a note of your own to it, click the Show Custom Note button. Subject and Note fields appear, enabling you to make the changes that you want.

3. Click Next.

Review and save your changes

1. Review the list of users you are adding, along with their exchange roles, alert settings and group assignments. If you need to make changes, click the Back button.

2. When you are satisfied with your entries, click Save. The users are added to the exchange, and a note is sent to each user who was selected to receive a welcome message and who can view the exchange.

Adding users from the Hub

You can use Intralinks’ powerful search tools to locate people whom you work with currently or have worked with in the past and then add them to your exchange. Using the following procedure, you can add either a single person or many people to the exchange.

To add users to exchanges from the Hub

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the People button on the left side of the screen to display a list of all the people you have worked with in Intralinks.

   These include people with public profiles, people you have added to your exchanges, and people with whom you work on at least one exchange already, regardless of whether their profiles are public or private.

2. Use the search and filtering tools to the right of the Hub button to find the person or people you want to add.

   If you plan to add many people to your exchanges, you can filter the list using the Advanced Search link below the Search box.

3. Highlight the names of the person or people you want to add. To select multiple people, press the SHIFT or CTRL key while clicking the users’ names.

4. From the Actions menu, select Add Users to an Exchange. A list of the exchanges to which you can add users appears.
5. Highlight the exchange you want to add the selected users to, and click Continue. The first step of the Add User to an Exchange wizard appears.

6. Select an exchange role for each user. Then click Next.

To learn more about exchange roles, see “Users’ roles within an exchange” on page 46.

7. Assign the users to groups. Drag each user’s name from the list on the left to the group to which he or she is being assigned.

Group assignments are important because they determine which documents each user will be able to access, along with the level of security being applied to each group. All reviewers must be included in a group in order to work in the exchange.

If the group you want has not been created yet If you discover that the group you want has not been created, click the Create Group button. The Add Group Wizard will open, allowing you to create the group. The Add Users Wizard will remain open, allowing you to continue adding this user once the group has been created. See “To add a group to the exchange” on page 42 for instructions for using the Add Group Wizard.

8. Click Next. The Send Alerts step of the wizard appears.

9. (Optional.) Revise the subject of the Welcome to Exchange email alerts that the users will receive and add a note to the alerts if you like. Then mark the Alert option for each new user whom you want to receive an alert.

10. Click Next. The Review and Complete step of the wizard appears.

11. Review the information that appears on the screen. If any changes are needed, click the Back button to display the screen where the changes can be made.

12. When you are satisfied with your entries, click Save.

13. A confirmation screen appears to tell you that the users were added to the exchange, or, if they could not be added, the reason they were not added. Email alerts will be sent to the users who were successfully added, welcoming them to your exchange.

If the exchange is not visible to one or more users (for example the exchange is in the hold phase and the users have been assigned the Reviewer role, which can view only open exchanges), the alerts will not be sent to them until the exchange becomes visible for them. (In the previous example, reviewers would receive the alert when the exchange was moved to the open phase.)

Importing user information using Intralinks Designer

If you have been assigned the Manager Plus exchange role, you can use Intralinks Designer to import information from another application using a Microsoft Excel spreadsheet or a Comma Separated Value (CSV) file. In the import process, you can choose to add users to your exchange, remove them, or synchronize your user information with another “system of record.” In addition, you can use Intralinks Designer to organize and manage documents and files on the exchange.

Information about using Intralinks Designer to manage user information can be found in the Intralinks Designer User Guide or the Intralinks Designer help system.
To start Intralinks Designer

◊ **From the Hub:** Highlight the exchange that you want to update, then select *Intralinks Designer* from the *Actions* menu.

◊ **From within an exchange:** First, click the *Documents* or *Users & Groups* button at the top of the screen. Then select *Intralinks Designer* from the *More Actions* menu.

If Intralinks Designer is installed on your computer, it is launched. If you have not installed Intralinks Designer yet, a screen appears, providing you with information about installing the application and a link to the Intralinks Designer installer.

**Note:** If you launch Intralinks Designer from Intralinks Platform and then close either Intralinks Designer or Intralinks Platform, the other application will be closed, as well.

**Requesting another manager to add users**

There may be times when you would like for other exchange managers to add people to exchanges to which you belong. You may have any type of role on these exchanges.

**To request that users be added to your exchange**

If the *Hub* is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select *Hub* from the list that appears.

1. Click the *People* button on the left side of the screen to display a list of all the people you have worked with in Intralinks.
   These include people with public profiles, people you have added to your exchanges, and people with whom you work on at least one exchange already, regardless of whether their profiles are public or private.

2. Use the search and filtering tools to the right of the *Hub* button to find the person or people you want to add.
   If you plan to add many people to your exchanges, you can filter the list by clicking options in the *Show only* section below the Search box. As you click each option, people who do not meet all the criteria you have selected are removed from view.

3. Highlight the names of the person or people you want to add. To select multiple people, press the **SHIFT** or **CTRL** key while clicking the users’ names.

4. From the *Actions* menu, select *Recommend User to an Exchange*. The first step of a two-step wizard appears, displaying a list of your exchanges.

5. Mark the boxes next to the exchanges you want the selected users to be added to, and click **Next**. The second step of the wizard appears.

6. Enter a note explaining your request to the exchange manager.

7. Review the selected users and exchanges to be sure they are correct. If any changes need to be made, click the *Back* button to do so.

8. When you are satisfied with your selections, click the *Save* button.

A request will be emailed to the key contacts for the exchanges you selected. Requests also will appear in the exchange managers’ *Assigned to Me* lists.
Responding to requests that users be added to your exchange

As an exchange manager, you may receive requests to add users to your exchanges. Use the following procedure to do so.

► To accept or reject requests that users be added to your exchanges

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the Approvals button on the left side of the screen. Additional options appear.
2. Click on Assigned to Me. A list of tasks awaiting a response from you is displayed.
3. Highlight the name of a potential exchange member.
4. From the Actions menu, select either Add User to Exchange or Reject request.
   If you reject the request, no further steps are needed. If you accept it, a wizard appears and you can select an exchange role and group for the new member.
5. Select an exchange role for each user. If a user will be a key contact for the exchange, mark the Key Contact option. Then click Next.
6. Assign the users to groups. Drag each user’s name from the list on the left to the group to which he or she is being assigned.
7. Click Save.
   A confirmation window appears to tell you that the user was added to the exchange, or, if he or she could not be added, the reason he or she was not added. If the user was successfully added, an email alert will be sent, welcoming the user to your exchange.

Assigning users to another group

You can move a user from one group to another quickly if the need arises. Using this procedure, you also can assign exchange users to a group if they were not assigned to one when they were added to the exchange.

► To assign a user to another user group

The Users & Groups tab should be displayed.

1. Using the Users & Groups smart filters, locate the user whose group assignment you want to change. Click the user’s name to highlight it.
2. From the More Actions menu, select Groups. The Groups view of the user’s information screen appears.
3. Click Assign to Groups. A list of groups appears in a list on the left side of the screen. A list of groups the user currently is assigned to (if any) appears on the right.
4. In the list on the left, highlight the group to which the user be assigned and click the arrow button ▶ to move the group’s name to the list on the right.
5. If you want to remove the user from a group, highlight the group’s name and click **Remove**.

6. Click **Save**.

### Changing a user’s exchange role

From time to time, you may find that you need to change a particular user’s exchange role. You also may find that the user should be a key contact for the exchange, or perhaps should no longer be a key contact anymore. Use the steps below to make these changes.

Note that exchange roles are different from **group membership roles**, which define the type of work that an individual performs within the group to which he or she belongs.

► **To change an individual user’s exchange role**

The **Users & Groups** tab should be displayed.

1. Locate the user whose exchange role you want to change using the Users & Groups smart filters. Click the user’s name to highlight it.

2. Click the **Properties** button at the top of the screen. The **Properties** view of the user’s information screen appears.

3. From the **Exchange Role** list, select the new role that the user will have.

4. Click **Save**.

► **To change several users’ exchange roles at the same time**

The **Users & Groups** tab should be displayed.

1. Locate the users whose exchange role you want to change using the Users & Groups smart filters. Press the **SHIFT** or **CTRL** key while clicking the users’ names to highlight them.

2. Click the **Properties** button at the top of the screen. A window appears, displaying the names of the users you selected, along with other information about them.

3. From the **Role** list next to each user’s name, select the new exchange role that the user will have.

4. Click **Save**.

### Making a user a key contact for the exchange

Key contacts are managers who have the ability to address issues other users may have with the exchange. Contact information for key contacts is included on email alerts that are sent out to users when they are invited to join the exchange, whenever new documents that affect them are added to the exchange, and the like.

► **To make a user a key contact**

The **Users & Groups** tab should be displayed.
1. Locate the user whose exchange role you want to change using the Users & Groups smart filters. Click the user’s name to highlight it.

2. Click the **Properties** button at the top of the screen. The **Properties** view of the user’s information screen appears.

3. Mark the **Key Contact** option. (If the user no longer will be a key contact, unmark the option.)

4. Click **Save**.

Removing users from the exchange

Occasionally you may need to remove a user from your exchange. The following steps explain how to do so.

Note that when users leave their organizations, they should be deregistered. Deregistered users can no longer access Intralinks and they are removed from all Intralinks exchanges automatically. In this case, it is not necessary for you to remove them from your exchange. For more information about deregistering users, see “When users leave your organization” on page 59.

**To remove a user from your exchange**

The **Users & Groups** tab should be displayed.

1. Using the Users & Groups smart filters, locate the user whom you want to remove. Click the user’s name to highlight it.
   
   To select multiple users, press the **SHIFT** or **CTRL** key while clicking the users’ names to highlight them.

2. Click the **Remove User** button at the top of the screen. A message appears asking you to confirm your decision.

   Note that if you remove a user from the exchange, the action cannot be undone; you will have to add the person to the exchange as though he or she were a new user.

3. Click **Remove from Exchange**.

**To view a list of users who have been removed from your exchange**

The **Users & Groups** tab should be displayed.

1. Click the **Removed Users** link at the bottom of the Groups list on the left side of the screen. A list of users who have been removed is displayed, along with contact information, their statuses and exchange roles, and the dates on which they last accessed the exchange and were removed from it.

2. To create a Microsoft Excel spreadsheet containing the currently displayed information, select **Export This View** from the **Export** menu. You can print the spreadsheet using Excel if you like.

Managing an individual user’s access to multiple exchanges

You can use the Manage Exchanges wizard to efficiently manage users’ access to all the exchanges that you manage. Using this wizard, you can:

- Add and remove users from multiple exchanges
• Assign or update users’ exchange roles

• Make users key contacts if they have been assigned the appropriate exchange roles

The Manage Exchanges wizard allows you to manage access for one user at a time.

▶ To manage a single user’s access to multiple exchanges

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the People tab on the left side of the screen. The Contacts sub-tab should be selected; if it is not, click it to select it.

2. Locate the user who access you wish to manage, and right-click on the user’s name. A menu appears.


4. Select an exchange role for each of the exchanges that you want the user to be able to access. To remove the user from an exchange, select No Access.

5. (Optional.) For exchanges in which the user has the appropriate roles, you also can make the user a key contact by marking the Key Contact option.

6. When you have made all your selections, click Next. Step 2 of the wizard appears, displaying the changes that you made.

7. Review the changes that you made on step 1 of the Manage Exchanges wizard. You can use this screen to make corrections before making your changes final.

   Only the exchanges that you modified are displayed. If you wish to make changes to other exchanges, click the Back button to redisplay step 1 of the wizard.

8. When you have made and reviewed all your changes, click Submit.

   When you click Submit, a confirmation message will appear. If you click Continue, your changes will be made, and the user will receive a welcome to exchange alert for the exchanges that are available to them. (Depending upon their exchange role and the exchange phase, the user may not have access to some exchanges. For example, reviewers do not have access to exchanges in the hold and preparation phases.)

Copying groups from one exchange to another

You can copy one or more groups from one exchange to another; if you have created group working sets, you can use them, as well to copy groups from one exchange to another.

You have to option to copy only the groups — without any group members — or both the groups and the users who are members of the groups. You also have the option to copy custom field settings if most or all of the values used in the original exchange will apply to the new exchange, as well.
To copy individual groups to another exchange

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Select the People tab on the left side of the screen.
2. Select the Groups subtab. The groups that you have created are displayed. If necessary, filter the groups to locate those that you wish to copy.
3. Highlight the group or groups that you want to copy.
4. From the Actions menu, select Copy Group.
5. An informational message appears. Read the message, then click Close.
6. Click the Exchanges tab.
7. Highlight the exchange where you want the copied group to appear.
8. From the Actions menu, select Paste Group. The Paste Options screen appears.
9. Mark the Copy group members from source group to existing target group option if you want to add the members of the group to the selected exchange. If you do not mark this option, only the group itself, without any members, will be copied.
10. Mark the Copy custom fields option if you want the custom fields set up for the group in the original exchange to be copied to the new exchange.
11. Click Save.
12. An informational message appears, alerting you that the groups are being copied; you will receive an email message when the files have been copied. Click Close.

To copy the groups in a working set to another exchange

To learn how to create and manage working sets, see “Creating working sets” on page 36.

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Select the People tab on the left side of the screen.
2. Select the Groups subtab. The working sets that you have created appear in the lower left area of the screen.
3. From the Actions menu, select Copy Working Set.
4. An informational message appears. Read the message, then click Close.
5. Click the Exchanges tab.
6. Highlight the exchange where you want the copied groups to appear.
7. From the Actions menu, select Paste Groups. The Paste Options screen appears.
8. Mark the Copy group members from source group to existing target group option if you want to add the members of the group to the selected exchange. If you do not mark this option, only the group itself, without any members, will be copied.
9. Mark the **Copy custom fields** option if you want the custom fields set up for the group in the original exchange to be copied to the new exchange.

10. Click **Save**.

11. An informational message appears, alerting you that the groups are being copied; you will receive an email message when the files have been copied. Click **Close**.

Finding users and groups

If your exchange has many users and groups, you can use Intralinks Platform’s search and smart filter tools to quickly locate the user or group you want to work with.

▶ To search for a particular user

The **Users & Groups** tab should be displayed.

1. Enter the name (first, last or both) of the person you wish to find in the **Search** box in the upper right corner of the Intralinks Platform window, then click **Go**. A list of users with the name you entered is displayed.

   **Note:** If you enter more than one word, your search results will include all users whose names include one word or the other. Your entry can be uppercase or lowercase; the **Search** field is not case sensitive.

2. To make changes to the user’s information, choose the appropriate command from the **Actions** menu.

▶ To filter the members of a group

The **Users & Groups** tab should be displayed.

1. Select the group you want to filter using the Group List on the left side of the screen. All the members of the group appear in the main area of the screen.

2. Click on **Unfiltered** or the Filter icon [in the upper right corner of the User List. Filters for users’ last names, organization and email address appear.

3. Type the information you want to find in the appropriate field. As you type, users who do not match your entry disappear from the User List.

   To redisplay the list of all users in the group, click the **Clear** button, which appears beneath the Filter icon.

Finding users using smart filters

Smart filters provide you with powerful tools for locating users based on a variety of attributes. For example, you can see all users associated with a particular organization, even if they have been assigned to multiple groups. You can view lists of users by active or inactive status. You can see users with a particular exchange role (Manager Plus or Publisher, say), and those who are designated as key contacts for the exchange. You also can view a list of users who have not been assigned to a user group yet, and therefore may not have access to any of the documents and folders on the exchange.

The contents of the smart filters folders are updated automatically as users are added to the exchange and their information is changed.
To view the contents of a smart filter

The Users & Groups tab should be displayed.

Smart filters appear on the upper left side of the screen.

◊ Click on the smart filter folder whose contents you want to view. The contents in the folder appear in the User List on the right side of the window.

Resending welcome alerts to exchange members

Occasionally you may be asked to resend the email message that welcomes a new user to your exchange. These welcome alerts can be resent to active exchange members.

To resend the welcome alert

1. Locate the exchange member to whom the alert will be sent.
2. From the More Actions menu, select Resend Welcome Alert. The Resend Welcome Alert screen appears.
3. (Optional.) If you want to make changes to the subject line of the alert or add a note to it, click Show Custom Note. Subject and Note fields appear, allowing you to make the changes that you want.
4. When you’re ready to send the alert, click Send.

When users leave your organization

When users leave your organization, they should be deregistered to prevent them from accessing information that should no longer be available to them. When users are deregistered, they can no longer access Intralinks Platform or any other Intralinks service with the email address and password they used previously. They are automatically removed from all exchanges.

Individuals who have been deregistered may be added to Intralinks again by another organization using an email address from that organization. They will not have access to your organization’s exchanges unless you allow them to do so.

Designated organization officials and compliance officers can contact Intralinks customer service to request that users be deregistered.

Individual users also can request that their own accounts be deregistered. Requests must be made in writing using the email account used to log into Intralinks.

Requests will be validated to ensure that users are not deregistered inappropriately. The user account will be suspended until the request is verified.
Chapter 5: Publishing documents

Overview

In this chapter you will learn how to:

• Create, organize and delete folders
• Add, replace, move and delete documents
• Use Multi-file Uploader to add multiple documents at the same time
• Set and update permissions for documents
• Set and update folder-level permissions that will be applied to all documents and subfolders within a selected folder
• Override folder-level permissions
• Give reviewers and previewers the ability to add documents to selected folders
• Alert users when new documents are available
• Copy and paste documents
• Use document collections, known as working sets, to perform tasks
• Prevent other users from updating documents using the checkout process
• Import information using Intralinks Designer
• Enable users to convert Microsoft Office documents to PDF format
• Use naming conventions to standardize document names

Before you begin

In order to perform the tasks in this chapter, Adobe Flash Player 9 must be installed on your computer.

When you select an Intralinks Platform exchange in the Intralinks Hub, a message will appear if Flash Player 9 is not installed. This message includes links to information about the Flash Player software and to a location on the Adobe website where you can download this free software utility. Your organization’s IT department may be required to install this software for you.

If Flash Player 9 is not installed, you can open the exchange, but you will be able to perform only basic reviewer-related tasks like reading and printing documents.

Managing folders

Creating folders

Folders are used to organize the contents of your exchange and to group related documents. Depending upon how your exchange was set up, you may be able to
index new folders and their contents. For more information about indexing, see "Indexing folders and documents” on page 64.

To create a folder

The Documents tab should be displayed.

1. If you want to create a top-level folder, highlight the Folders folder in folder list on the left side of the screen.

   Top-level folders are those that appear at the exchange level; that is, they are not subfolders inside of any other folders.

   If you want to create a subfolder (that is, a folder inside another folder), highlight the folder that will contain the new folder.

2. Click the Add Folder button near the top of the screen. The Add New Folder screen appears.

3. Add a title that clearly describes the contents that will appear in the folder.

   Note that the following characters cannot appear in folder titles:
   \ / : * " < > ? |

4. If you are creating a top-level folder and indexing is being used on this exchange, you have the choice to make the folder either indexed or unindexed. To index the folder, leave the Do not assign index numbers to the folder and its contents option unmarked. To create an unindexed folder, mark this option.

   If indexing is not being used on the exchange, or if you are creating a subfolder, the Do not assign index numbers to the folder and its contents option does not appear.

5. You can add notes about the folder if you like. These notes can be viewed by any user who has access to the folder. For this reason, do not include information that should not be seen by reviewers. The notes are for reference purposes only and will not appear on reports.

6. If a Save button appears, your entries are complete. Click Save to create the folder. Skip the remaining steps in this procedure.

   If a Next button appears, click it to go on to the next screen. Depending upon how the exchange is set up, you will enter values for custom fields associated with the folder or set permissions for it. Click Next to proceed.

7. Custom fields provide a structured way for you to describe your folders in greater detail. Custom fields enable you to enter specific pieces of information, such as expiration dates, locations, and the like. You could use the Notes field in the first step of the wizard to keep track of this information, but with custom fields you can more easily manage the information and ensure that it is entered consistently.

8. Make an entry or selection for each field that applies to this folder. Required fields are marked with an asterisk (*).

9. Depending upon how your exchange is set up, either a Save button or a Next button appears.
If a **Save** button appears, the **Remember selections for future documents and subfolders** exchange setting is disabled and your exchange is using document-level permissioning. Click **Save** to create the folder. Skip the rest of the steps in this procedure.

If a **Next** button appears, the **Remember selections for future documents and subfolders** exchange setting is enabled and your exchange is using folder-level permissioning. Click **Next** to display the **Permission Groups** step of the Add Folder Wizard. A list of unpermissioned groups appears on the left side of the screen, and the groups that already have been permissioned to the folder appear on the right.

To learn more about document-level and folder-level permissioning, see “Setting permissions for all the documents in one or more folders” on page 76.

10. In the **Not Permissioned Groups** list, locate the groups whose members should be able to use the documents in the selected folder. Highlight the groups and click the arrow button to move them to the **Permissioned Groups** list. (Note that exchange managers are able to view all documents regardless of their group memberships.)

You can select multiple groups at the same time by pressing the **SHIFT** or **CTRL** key while clicking the groups to highlight them.

11. Review the selections in the **See** column. Typically this option should be marked for every group unless permission to view the documents in this folder has been revoked for a particular group.

The **All Users - Current and Future** option is used to give all users on the exchange permission to view documents. It appears automatically in the **Permissioned Users and Groups** column, but it is unmarked. If you want for every exchange user, including those who have not been added to the exchange yet, to have permission to view the documents in this folder, mark the **See** box for this option. (Note: If this option has been disabled for your exchange, it does not appear.)

12. Determine whether the groups will be able to control the documents. Do this by marking the **Control** option next to the name of each group that will have this permission. Members of these groups will be able to modify the document only if their exchange roles (for example, manager or publisher) allow them to do so.

Document control allows users to change other users’ permissions to the document, update the document or delete it.

13. Depending upon how your exchange has been set up, additional options may be displayed, allowing you to specify whether reviewers and previewers will be able to add documents or folders to this folder, and whether they will be able to edit the values for the folder’s custom fields. (This functionality sometimes is referred to as “limited publisher.”)

You may have to scroll horizontally to display these options.

- **Allow adding documents** — Mark this option for each group that contains reviewers and previewers who will be allowed to add documents to the selected folder. This option appears only if the **Allow Reviewers and Previewers to add documents to select folders** exchange setting is enabled.

If the **Remember selections for future documents and subfolders** exchange setting also is enabled, reviewers and previewers who have
permission to add documents to a folder will be able to add documents to subfolders within that folder, as well. This can be overridden for each subfolder.

• **Allow adding folders & documents** — Mark this option for each group that contains reviewers and previewers who will be allowed to add both subfolders and documents to the selected folder. This option appears only if the **Allow Reviewers and Previewers to add documents to select folders** exchange setting is enabled.

If the **Remember selections for future documents and subfolders** exchange setting also is enabled, reviewers and previewers who have permission to add documents to a folder will be able to add documents to subfolders within that folder, as well. This can be overridden for each subfolder.

When members of the selected groups add documents, they will be able to send an email alert to other limited publishers with permission to the folder where the new documents are stored. Alerts will be sent to all limited publishers with permission to the folder. Reviewers and previewers without limited publisher permission will not receive alerts.

If folder custom fields are being used on this exchange, members of the selected groups will be able to edit the name and set custom field values for the folders that they have created.

This option appears only if the **Allow Reviewers and Previewers to create subfolders and add documents to select folders** exchange setting is enabled.

• **Allow editing of folder custom fields** — Mark this option for each group that contains reviewers and previewers who will be allowed to edit the values of custom fields for the selected folder. This option appears only if the **Allow Reviewers and Previewers to edit custom fields to select folders** exchange setting is enabled.

14. Determine whether the documents will be protected.

If the documents in this exchange are protected (the **enable protection of PDF and Microsoft Office documents** exchange setting is marked), a Protection column is displayed. For each permissioned group, you can choose an additional level of security for these documents. With document protections, you can prevent users from downloading copies of the documents or require them to enter their email address and password before viewing a downloaded copy of the documents. You also can prevent users from printing the documents.

The type of browser, browser version, and browser settings determine whether the document can be downloaded, or must be viewed on the exchange. For detailed information about document protections, see Chapter 5, *Publishing documents*, on page 60.

For each group, select one of the following options from the Protection list:

• **Do not protect**

• **Protect**

• **Protect/No Print**
15. When you have finished setting permissions, click **OK**.

16. Click **Save**.

### Organizing folders

Once you’ve added folders to your exchange, you can organize them in any order you like. Simply drag folders from one location to another in the folder list to place them in the order you wish them to have.

If you wish to provide additional structure for your folders and documents, you can index them. Indexing assigns numbers to folders and their contents, making it easy to trace documents and to identify related documents when they appear in search lists and on reports. For more information about indexing, read the following section, “Indexing folders and documents.”

### Indexing folders and documents

As noted above, index numbers provide a way for you to structure your folders and documents, making them easier to find.

**Note:** Depending upon how your exchange was set up, indexing may not be available.

If indexing is allowed on your exchange, you have the option whether to index folders and their contents. Your exchange can have a mix of indexed and unindexed folders. If a top-level folder is indexed, all the subfolders and documents within it are indexed automatically. Likewise, if a top-level folder is unindexed, all the subfolders and documents within it are unindexed.

All the index numbers on your exchange use the same format. The first number indicates the top-level folder, and each subsequent decimal number indicates a subfolder. The final decimal number indicates the subfolder’s or document’s position within the subfolder that contains it. For example, if a document has the index number **2.1.2.16**, to find it, you would open top-level folder 2, then the first subfolder within it, and then the second subfolder within that folder, and finally document 16.

Index numbers in Intralinks are consecutive. If you move, delete or insert an indexed item, other items will be reindexed automatically to ensure that there are neither duplicate numbers nor gaps in the numbering sequence.

If subfolders or documents are moved from an indexed folder to an unindexed folder, their index numbers are removed. If items are moved from an unindexed folder to an indexed folder, index numbers will be added to the items.

**To index a new folder**

◊ By default, new top-level folders are indexed when they are created. For more information, see “To create a folder” on page 61.

**To index an existing folder**

The **Documents** tab should be displayed.

1. Highlight the **Folders** folder in the folder list on the left side of the screen. A list of top-level folders appears in the content area to the right.
2. In the content area, highlight the top-level folder you want to be indexed.

3. From the More Actions menu, select Properties. The properties window for the folder appears.

4. Unmark the Do not assign index numbers to the folder and its contents option.

5. Click Save.

Freezing and unfreezing exchange items

If your exchange allows folders to be indexed, you can “freeze” items once the exchange is fully organized and no further changes to the structure are planned. Freezing affects both indexed and unindexed items. Once an exchange is frozen, no changes can be made to its structure or the documents within it.

If, after you’ve frozen your exchange, you discover that additional changes need to be made that will affect the order of items, you can “unfreeze” the index and make the needed changes. Then you can freeze the index again as needed.

▶ To freeze exchange items

1. From the More Actions menu, select Freeze Index.
2. An alert message appears asking you to confirm your choice. Click Yes.

▶ To unfreeze exchange items

1. From the More Actions menu, select Unfreeze Index.
2. An alert message appears asking you to confirm your choice. Click Yes.

Moving folders

Folders can be moved simply by dragging them to the desired location.

If you want to undo a move action, select Undo Move from the More Actions menu, or simply drag the folder back to its original location.

Renaming folders and changing custom field values

Information that describes a folder — its name, notes about it and any custom field values that have been selected for it — are referred to as folder metadata.

If folder-level permissioning is being used on this exchange (the Remember selections for future documents and subfolders exchange setting is marked), you can use the steps below to review the permissions currently in place for the folder and make any needed changes, as well.

▶ To rename folders, review folder permissions and change other folder metadata

1. Highlight the folder that you want to change.
2. From the More Actions menu, choose Properties. The properties screen for the folder appears.
3. Review the name and notes about the folder and make any needed changes.
4. If a Custom Fields tab is displayed, click it to view the current values selected for the folder. Make any needed changes.

5. If a Permissions tab is displayed, click it to view the permissions set for this folder. Make any needed changes.

6. When you have finished making changes, click OK.

Deleting folders

If a folder is no longer needed, you can delete it and its contents in a single step. Use care when deleting folders; once deleted, they cannot be restored; you would have to manually recreate a deleted folder and its contents.

► To delete a folder

1. Highlight the folder.
2. From the More Actions menu, select Delete.
3. A message appears asking you to confirm your selection. Click Yes.

Adding documents

Documents are the heart of any exchange. Use the New Document Wizard to quickly add documents to your exchange and to select the groups of users who will be able to view and work with them. You also can determine whether users can print or download copies of the documents, and alert users that the documents are available for use.

Using the New Document Wizard

The New Document Wizard is a series of screens that enable you to add documents and document placeholders to your exchange. You also can determine who will be able to use them, and whether their use will be restricted in any way.

You can add up to 20 documents to a single folder at the same time. The total size of the documents cannot exceed 2GB. The permissions, notes and alert options that you enter or select will be applied to all the selected documents.

You also can use the New Document Wizard to create placeholders if you’re setting up your exchange and you do not have the files that you plan to add to the exchange at hand. You then can add the documents at a later time. For more information, see “Replacing a placeholder with a document” on page 71.

Important: If your exchange is in the open phase, do not permission users until you replace the placeholder with the actual file you want the users to view.

You can enter a combination of documents and document placeholders at the same time if you like.

Depending upon how your exchange has been set up, some of the screens below may not appear. If this is the case, simply skip to the next section and continue entering information about the documents or placeholder.
To add one or more documents or placeholders

The Documents tab should be displayed.

Select the document and set its properties

1. Open the folder that will contain the new document or placeholder.

2. Click the Add Document button near the top of the screen. The Set Properties view of the New Document Wizard appears.

   If you are adding only placeholders, skip to step 5. If you are adding documents, continue to step 3.

3. To add documents, click the Choose Files button. The Select File(s) to Upload dialog box appears.

4. Highlight the file or files that you want to add to the exchange and click Open. Information about the file, including its title and file type, are displayed in the New Document Wizard.

   You can select multiple files at the same time by pressing the SHIFT or CTRL key while clicking the files to highlight them.

   Note that the names of the files you select cannot contain the following characters:
   \ / : * " < > ? |

5. To add a placeholder, click the Add Placeholder button. You can add as many placeholders as you like.

6. If you want to enter a more descriptive title for the documents, enter the new name in the Document Title field. The original file on your computer or network drive will not be affected.

   If you are adding placeholders, you must enter a title for each placeholder in the Document Title field.

   Note that the document title cannot contain the following characters:
   \ / : * " < > ? |

7. (Optional) Enter or select an effective date for the documents. This is a date, typically in the future, when the information in the documents should begin being used. (If this exchange does not allow you to enter an effective date, the Effective Date field does not appear.)

8. (Optional.) Select the binder that is associated with these documents, if any. Binders allow you to organize documents in different locations either within an exchange or across multiple exchanges. You can create a new binder if you like. (If this exchange does not allow you to select binders, the Binder field does not appear.)

   If you created the binder that you selected or you have rights to change it, you can update the note that is attached to the binder. If you do so, the note will be updated for all documents to which the binder has been assigned.

9. (Optional.) Enter a note that provides additional information about the documents, as an aid to viewers. For example, you could add a note that provides a brief description of the documents’ contents, or you could provide contextual information that would help viewers to better understand the documents’ purpose or contents.
(Remember, if you are adding multiple documents or placeholders, the same note will be applied to all the items being added. If necessary, you can edit the note for individual documents by highlighting each document and selecting Properties from the Actions menu.)

10. (Optional.) If you entered a note in step 9, you can choose to display it automatically when users view the documents. To do this, mark the Display note before opening document option.

11. (Optional.) You can change the location on your exchange where the documents will appear. To select another location, click the Browse button next to the Folder Location field.

12. (Optional.) If you want the documents to appear in a new sub-folder within the folder that is selected in the Folder Location field, enter a name for the new folder in the Folder name field.
   
   If you leave the Folder name field blank, the documents will appear in the folder shown in the Folder Location field.

13. (Optional.) If a website or a particular webpage is associated with the document, click the Add Link button to enter the URL (Web address) for it. Your entry will appear as a clickable link on the Properties screen for the document, and in email alerts.

14. Click Next to continue entering information about your document.

   If you are creating placeholders and you do not wish to enter more information at this time, click Save. You can enter information on the remaining tabs when you replace the placeholders with actual documents.

**Add tags to the document(s)**

Depending upon how your exchange is set up, you may have the option of using tags to organize the documents on your exchange. These tags offer great flexibility in classifying and organizing information in ways that are meaningful to your organization. For example, using tags you can classify and locate documents dealing with Canadian commodity contracts no matter where they are located in the exchange.

The tags that are assigned to documents appear in the documents list, and users can use them when searching for documents.

Up to 25 tags can be assigned to each document. Tags are optional, and these steps can be skipped.

Complete the following steps to assign tags to the document or documents.

1. A list of all the tags for this exchange appears in the Available tags list.
   
   Highlight each tag that applies to the document and click the arrow button to move the tag to the Selected tags list on the right side of the screen.
   
   You can select multiple tags at the same time by pressing the SHIFT or CTRL key while clicking the tags to highlight them.

2. Click Next.
Enter information in custom fields

Custom fields provide a structured way for you to describe your documents in greater detail. Custom fields enable you to enter specific pieces of information, such as expiration dates, locations, and the like. You could use the Notes field in the first step of the wizard to keep track of this information, but with custom fields you can more easily manage the information and ensure that it is entered consistently.

1. Make an entry or selection for each field that applies to these documents.
2. Click Next.

Select an owner for the document(s)

Depending upon how your exchange is set up, you can identify a particular user or exchange group as the owner of the documents that you are adding. If you use this function, document ownership information can be used to select documents used by business processes.

1. Choose whether the owner will be a collaboration group or an individual person. Additional fields will appear on the screen.

   If the owner is a group: Click the Change button next to the Document Owner (Group) field, and select the owner from the list that appears. Then click the Change button next to the For Selected Group Member field and select the specific member of the group who will be designated as the document owner.

   If the owner is an individual: Click the Change button next to the Document Owner (User) field, and select the owner from the list that appears. Then click the Change button next to the For Selected Group field and select the group associated with the person.

2. Click Next.

Permission users to the document(s)

User groups that are allowed to view particular documents are permissioned to those documents. Permissioning provides an effective way for you to manage sensitive information, keeping them out of sight of users who should not have access to the information within them.

In the following steps you will permission groups to the documents that you are adding and indicate whether they can make changes to the documents.

1. A list of all the user groups for this exchange appears in a box on the left side of the New Document Wizard. Highlight each group that should have access to the documents and click the arrow button to move the group to the box on the right side of the screen. (Note that exchange managers are able to view all documents and their names appear automatically in the list.)

   You can select multiple groups at the same time by pressing the SHIFT or CTRL key while clicking the groups to highlight them.

   If you are unsure about who is included in a particular group, double-click the group’s name to view a list of the group’s members.
2. The **All Users - Current and Future** option is used to give all users on the exchange permission to view documents. It appears automatically in the **Permissioned Users and Groups** column, but it is unmarked. If you want for every exchange user, including those who have not been added to the exchange yet, to have permission to view this documents, mark the **See** box for this option.

(Note: If this option has been disabled for your exchange, it does not appear.)

3. When you have selected the groups that are permissioned to use the documents, select the groups, if any, that also have permission to control the document. Do this by marking the **Control** option next to the name of each group that will have this permission. Members of these groups will be able to modify the document only if their exchange roles (for example, manager or publisher) allow them to do so.

   Document control allows users to change other users' permissions to the document, update the documents or delete the documents.

4. Click **Next**.

**Choose protections for the document(s) (optional)**

For each permissioned group, you can choose an additional level of security for the documents that you are adding. With document protections, you can prevent users from downloading copies of the documents or require them to enter their email address and password before viewing a downloaded copy of the documents. You also can prevent users from printing the documents.

The type of browser, browser version, and browser settings determine whether the document can be downloaded, or must be viewed on the exchange. For detailed information about document protections, see Chapter 6, **Protecting documents**, on page 93.

1. For each group, select one of the following options from the **Protection** list:
   - **Do not protect**
   - **Protect**
   - **Protect/No Print**

   Document protections also can be applied to the All Users - Current and Future option if you selected it.

   **Note:** when printing is allowed, the file can be printed not only to paper but also to other file types using the browser’s “Print As” function. Copies created using “Print As” are no longer signed or protected documents, even though the original file was protected. Clients who are concerned that downloaded protected files may be saved in this fashion should select the **Protect/No Print** option for their documents.

2. Click **Next**.

**Alert users that the document(s) are available (optional) or save your changes**

In the final step of the New Document Wizard, you can select users who will be alerted by email that the documents have been added to the exchange and are available for viewing. Intralinks provides a standard alert message that identifies
the documents and provides a link to them. You can add a custom note to the alert message if you like.

You also can override individual users’ preferences for receiving exchange alerts; this is useful if, for example, you are posting a high-priority document and want users to know about it immediately.

**Important!** You are not required to send alert messages to users; however, if you do not, be sure to click the Save button to ensure that the information you entered in previous views of the Wizard is retained. (See step 5 below.)

Typically you do not alert users when placeholders are added. If you are adding only placeholders, click the Save button to save your entries.

1. Review the subject that will be used for the email alert and make any needed changes.
2. If you entered a note on the Set Properties tab, it appears in the Notes field on this tab. You can edit or remove the note if you like, or add a note if none is displayed. The note will be included in the alert.
3. A list of permissioned users and groups appears on the bottom half of the screen. Mark the Alert option next to each group or user who will receive the alert. To send an alert to all the users and groups displayed on the screen, mark the All Permissioned Users option.
4. If you want to override automatically permissioned users’ preferences to receive daily summary email alerts or no alerts, select Immediate from the Override Alert Preference list. This option does not appear for groups.
5. Click the Save button.

**Replacing a placeholder with a document**

Follow the procedure below when you are ready to replace a placeholder with an actual file from your computer or a network drive.

**To replace a placeholder with a document**

The Documents tab should be displayed.

1. Highlight the placeholder.
2. From the More Actions menu, select Properties. The properties screen for the placeholder appears.
3. Click the Replace button. The Select File to Upload dialog box appears.
4. Highlight the file you want to add to the exchange and click Open. Information about the file, including its title and file type, are displayed on the properties screen.
5. Depending upon the steps you followed when you created the placeholder, you may need to give users permission to the document, select security settings and alert users to the document. If this is the case, complete the additional steps below. Otherwise, click Save to save your change and close the screen.
6. If you wish to assign an owner to the document, click the Ownership tab.
7. Choose whether the owner will be a collaboration group or an individual person. Additional fields will appear on the screen.

   **If the owner is a group:** Click the Change button next to the Document Owner (Group) field, and select the owner from the list that appears. Then click the Change button next to the For Selected Group Member field and select the specific member of the group who will be designated as the group's owner.

   **If the owner is an individual:** Click the Change button next to the Document Owner (User) field, and select the owner from the list that appears. Then click the Change button next to the For Selected Group field and select the group associated with the person.

8. To set permissions for the documentation, click the Permissions tab. The permissions window for the placeholder appears.

9. Click the Permission Groups button. A window similar to the Permissions view of the New Document Wizard appears.

10. As you do when creating a new document, move the groups you want to permission from the box on the left to the box on the right.

11. If you want one or more of these groups to be able to control the document, mark the Control option next to the groups' names. If the document is in PDF or Microsoft Office (Word, Excel or PowerPoint) format and you want to change its security settings, select the appropriate setting from the Protection list.

12. If you want to alert the newly permissioned users that the document is available, click the Alerts tab. A window similar to the Alert Users view of the New Document Wizard appears.

13. Mark the groups you want to alert. If you wish to override the users' preferences for receiving exchange alerts or add a note to the alert, do so.

14. Click Save.

Adding multiple documents at the same time

If you want to add many documents to your exchange at once, consider using Intralinks Multi-file Uploader. This utility allows you to add up to 30 documents at the same time. We recommend that you upload no more than 50MB at once. If you plan to upload a larger amount, we recommend that you use Intralinks Designer to perform this task instead. For more information about that tool, see “Importing information using Intralinks Designer” on page 87.

You can select one or more files or folders, as well as a combination of files and folders, to add to the exchange.

▶ **To add documents using Multi-file Uploader**

The Documents tab should be displayed.

1. If the Folders folder is not highlighted, highlight it.

2. Click the File Uploader button at the top of the screen. The Multi-file Uploader application is launched. (An informational message may appear, as well; if it does, review the information, then click anywhere on the screen to hide the message.)
The contents of your computer are displayed on the top half of the Intralinks Multi-file Uploader screen; this area is known as the desktop area. The contents of your exchange appear on the bottom half of the screen; this is known as the staging area.

3. A list of folders on your exchange appears on the left side of the staging area. Highlight the folder where you want to place new documents.

4. Select the files or folders in the desktop area and drag them to the staging area. They will appear in the folder that you selected in the previous step.

You can select several documents at the same time if you like. To do this, press the SHIFT or CTRL key while clicking on each document; continuing to press the SHIFT or CTRL key, drag the documents to their new location.

Add custom fields to the document

If your exchange uses custom fields and your exchange role enables you to make selections for custom fields, the Apply Custom Fields screen appears when you drag documents to the staging area. Use this screen to make entries for the custom fields.

1. Make an entry or selection for each field that applies to this document.

   Depending upon your selections, additional fields may appear. Required fields appear in red, with an asterisk (*) next to them; you must make a selection for these fields before uploading the documents to your exchange.

2. Click Apply. The staging area reappears.

Permission the documents

You can permission the documents to one or more user groups. Permissioning will allow users in the selected groups to see and work with the documents.

1. If the documents are not highlighted already, press the SHIFT or CTRL key and click on the documents to highlight them.

2. From the toolbar, select Permissions. The Permissions screen appears.

3. Highlight a document that you want to permission from the list on the left side of the screen. To set permissions for all the documents within a folder, highlight the folder.

4. A list of user groups on your exchange is displayed in the middle of the screen. Highlight each group that should have access to the document and click the arrow button to move the group to the box on the right side of the screen.

   You can select multiple groups at the same time by pressing the SHIFT or CTRL key while clicking the groups to highlight them.

5. Mark the See option for each group that will be allowed to view the selected documents.

   The All Users - Current and Future option is used to give all users on the exchange permission to view documents. It appears automatically in the Permissioned Groups list, but it is unmarked. If you want for every exchange user, including those who have not been added to the exchange yet, to have permission to view the documents in this folder, mark the See box for this
option. (Note: If this option has been disabled for your exchange, it does not appear.)

6. When you have selected the groups that are permissioned to use the documents, select the groups, if any, that also have permission to control the document. Do this by marking the Control option next to the name of each group that will have this permission. Members of these groups will be able to modify the document only if their exchange roles (for example, manager or publisher) allow them to do so.

Document control allows users to change other users’ permissions to the document, update the document or delete it.

The All Users - Current and Future option allows users only to view documents. The option cannot be used to give users permission to control documents.

7. Select document protections.

For each permissioned group, you can choose an additional level of security for this document. With document protections, you can prevent users from downloading copies of the documents or require them to enter their email address and password before viewing a downloaded copy of the documents. You also can prevent users from printing the documents.

The type of browser, browser version, and browser settings determine whether the document can be downloaded, or must be viewed on the exchange. For detailed information about document protections, see Applying additional security to your documents.

For each group, select one of the following options from the Protection list:

- Do not protect
- Protect
- Protect/No Print

Document protections also can be applied to the All Users - Current and Future option if you selected it.

8. When all documents have been permissioned, click the Apply button to save your changes and close the Permissions window.

Add a note about the documents

If you like, you can add a note that describes the documents or provides further information about them. This information will appear on the properties screen for each document.

1. From toolbar, select Properties. The Properties screen appears.
2. Enter your note in the Note field.
3. Click Apply.

Alert users about the documents

If you like, you can send an email alert to let permissioned users know that the documents are available once they have been uploaded.

1. From toolbar, select Alerts. The Send Alert screen appears.
2. Mark the box next to each group that should be alerted.

3. If you want to override users’ alert preferences and have your alert sent immediately to all users, mark the *Deliver immediately (override user preferences)* option.

4. Review the default subject and note that will be used for the alert. If you wish to make a change, unmark the *Use default Subject text* and *Use default Message text* options and make your entry in the boxes to the right of these options.

5. Click **Apply**.

**Upload the documents**

1. When you are ready to upload the documents, click **Upload**. The documents are added to your exchange, and a message appears asking whether you wish to view the Upload Log.

2. To view the log, click **Yes**. The log appears in a Microsoft Excel spreadsheet; it provides general information about the changes made to your exchange and a list of the files that were uploaded. If any files could not be uploaded, that will be noted, as well.

**Replacing or updating documents**

Use the following procedure to replace a document with a newer version.

**To replace a document**

The **Documents** tab should be displayed.

1. Highlight the document that you want to change.

2. From the **More Actions** menu, select **Properties**. The properties window for the document appears.

3. Click the **Choose File** button. The **Select File to Upload** dialog box appears.

4. Highlight the updated file and click **Open**. Information about the file, including its title and file type, are displayed in the properties window.

5. Click **Replace**.

**Reviewing and modifying permissions**

Using the **Permissions Overview** screen, you can review and change the permissions for documents quickly and easily. You can view and change permissions for a single document, for multiple documents, or even for the documents in multiple folders. The **Permissions Overview** screen provides a snapshot of all the groups with permission to the document, along with their security settings. You can export this information to Microsoft Excel, as well.

**To review and modify permissions using the Permissions Overview screen**

The **Documents** tab should be displayed.

1. Highlight the document or documents that you want to view or change. To view all the documents in one or more folders, highlight the folders.
2. From the More Actions menu, select View All Permissions. The Permissions Overview screen appears displaying information about the top-level folders on the exchange.

3. Double-click a top-level folder to view the subfolders and documents stored within it.

4. If you want to change a particular group’s permissions to use a document, highlight the group’s current settings and then choose the settings you want from the Selected Permissions list. To change a particular group’s security settings for a document, highlight the group’s current settings and then choose the settings you want from the Protections list. To learn more about document protections, see Chapter 5, Publishing documents, on page 60.

You can select several documents and apply the same settings to them at the same time if you like. To do this, press the SHIFT or CTRL key while clicking on the permissions for each document. You also can click and drag the mouse to select rows or columns of permissions that are next to one another.

5. (Optional.) To export the permissions information for the selected document, click the Export button. Microsoft Excel is opened and a spreadsheet containing the document’s permissions information appears.

6. Click Save.

To apply a group’s document permissions to another group

If the same (or similar) document permissions apply to more than one group, you can set the permissions for a single group and then copy those permissions to one or more additional groups. Once you have copied the permissions, changes can be made to the permissions for individual documents if necessary. To make changes for individual documents, see “To review and modify permissions using the Permissions Overview screen” on page 75.

Use this feature with care; once changes are made, they cannot be undone.

The Users & Groups tab should be displayed.

1. Highlight the group whose permissions are already set — the group whose permissions will be copied to other groups.

2. From the More Actions menu, select Copy Group Permissions. The Copy Group Permissions window appears.

3. For each group whose permissions you want to update, mark the box in the Copy Permissions column.

4. Click Save. The settings for the group you selected in step 1 are applied to all the groups you selected in step 2.

Setting permissions for all the documents in one or more folders

You can set or change permissions for all the documents in a folder — or for the documents in multiple folders — at the same time. This is referred to as bulk permissioning.

Depending upon how your exchange has been set up, when you use bulk permissioning, you will either set permissions for the documents within the folder, or assign permissions to the folder itself:
• If your exchange allows you to set permissions for the documents within a folder, your selections are applied to whatever documents are located in the folder at the time of permissioning. Documents added at a later time are not affected and must be permissioned separately.

• If your exchange allows you to set permissions for the folder itself, your selections will be applied to the documents and subfolders within the folder at the time of permissioning. These selections will be remembered, and they will be assigned automatically to documents and subfolders added to the folder later.

Note that you can use one method of permissioning or the other, but not both at the same time. In either case, the permissions for individual documents (or subfolders, in the second instance) can be overridden, and different permissions assigned to them.

An exchange setting, Remember selections for future documents and subfolders, determines which method is used. For more information about exchange settings, see Appendix A, Exchange settings, on page 194.

You also can use the Permissions Overview and Copy Group Permissions screens to set permissions for many documents at once. For more information, see “To review and modify permissions using the Permissions Overview screen” on page 75 and “To apply a group’s document permissions to another group” on page 76.

If you use document-level permissioning

Use the procedure below if the Remember selections for future documents and subfolders exchange setting is unmarked for the exchange that you are using.

To modify permissions for all the documents within one or more folders

Note that you are setting permissions only for the documents currently in the folder(s). Any documents added to the folders in the future will have to be permissioned when they are added.

The Documents tab should be displayed.

1. Highlight one or more folders.

2. From the More Actions menu, select Set Folder Permissions. The Set Folder Permissions window appears.

3. For each group, use the list in the Permission column to change the group’s permissions for the selected documents. If you want to change permissions for all groups, make your selection from the All Groups list.

   • Keep existing permissions – No changes are made; whatever permissions currently are in place will continue to apply for this group.

   • No permission – Members of the selected group have no access to the documents in the selected folders. Neither the documents nor the folders will be visible to these users.
• **See** – Members of the selected group will be able to view documents in the selected folders, but will not be allowed to change them in any way.

• **Control** – Members of the selected group will be able to modify the documents if their exchange roles (for example, manager or publisher) allow them to do so. Document control allows users to change other users’ permissions to documents, update the documents or delete them.

4. Depending upon how your exchange has been set up, additional options may be displayed, allowing you to specify whether reviewers and previewers will be able to add documents or folders to this folder, and whether they will be able to edit the values for the folder’s custom fields. (This functionality sometimes is referred to as “limited publisher.”)

You may have to scroll horizontally to display these options.

• **Allow adding documents** — Mark this option for each group that contains reviewers and previewers who will be allowed to add documents to the selected folder. This option appears only if the **Allow Reviewers and Previewers to add documents to select folders** exchange setting is enabled.

If the **Remember selections for future documents and subfolders** exchange setting also is enabled, reviewers and previewers who have permission to add documents to a folder will be able to add documents to subfolders within that folder, as well. This can be overridden for each subfolder.

• **Allow adding folders & documents** — Mark this option for each group that contains reviewers and previewers who will be allowed to add both subfolders and documents to the selected folder. This option appears only if the **Allow Reviewers and Previewers to add documents to select folders** exchange setting is enabled.

If the **Remember selections for future documents and subfolders** exchange setting also is enabled, reviewers and previewers who have permission to add documents to a folder will be able to add documents to subfolders within that folder, as well. This can be overridden for each subfolder.

When members of the selected groups add documents, they will be able to send an email alert to other limited publishers with permission to the folder where the new documents are stored. Alerts will be sent to all limited publishers with permission to the folder. Reviewers and previewers without limited publisher permission will not receive alerts.

If folder custom fields are being used on this exchange, members of the selected groups will be able to edit the name and set custom field values for the folders that they have created.

This option appears only if the **Allow Reviewers and Previewers to create sub folders and add documents to select folders** exchange setting is enabled.

• **Allow editing of folder custom fields** — Mark this option for each group that contains reviewers and previewers who will be allowed to edit the values of custom fields for the selected folder. This option appears only if the **Allow Reviewers and Previewers to edit custom fields to select folders** exchange setting is enabled.
This option appears only if the Allow Reviewers and Previewers to add documents to select folders exchange setting is enabled. (This functionality sometimes is referred to as “limited publisher.”)

5. If the documents in this exchange are protected (the enable protection of PDF and Microsoft Office documents exchange setting is marked), a Protection column is displayed. For each permissioned group, you can choose an additional level of security for these documents. With document protections, you can prevent users from downloading copies of the documents or require them to enter their email address and password before viewing a downloaded copy of the documents. You also can prevent users from printing the documents.

The type of browser, browser version, and browser settings determine whether the document can be downloaded, or must be viewed on the exchange. For detailed information about document protections, see Chapter 5, Publishing documents, on page 60.

For each group, select one of the following options from the Protection list:

- **Do not protect**
- **Protect**
- **Protect/No Print**

6. When you have made all the needed changes, click Save.

If you use folder-level permissioning (permissions are inherited)

Use the procedure below if the Remember selections for future documents and subfolders exchange setting is marked for the exchange that you are using.

Using this procedure, you can set permissions for the contents of a folder (the documents and subfolders within it), and those settings are applied to existing contents and to all new content added to that folder. You will be able to override these default permissions for individual documents or subfolders if you like.

If you move documents or subfolders from one permissioned folder to another, the permissions are changed automatically. (Any changes you made to the inherited permissions will be remembered when the items are moved. All the inherited permissions for the old folder that have not been changed will be replaced by the inherited permissions for the new folder.)

**To modify permissions for folders**

The Documents tab should be displayed.

1. Highlight the folder whose permissions you want to modify.
2. From the More Actions menu, select Permissions. The Permissions view of the folder’s information screen appears, listing any groups that have been permissioned to the folder already.
3. Click Permission Groups. A list of unpermissioned groups appears on the left side of the screen, and the groups that already have been permissioned to the folder appear on the right. (Note that groups in the Permissioned Groups list do not have the ability to see documents in this folder if the See option has been unmarked for them.)
4. In the **Not Permissioned Groups** list, locate the groups whose members should be able to use the documents in the selected folder. Highlight the groups and click the arrow button to move them to the **Permissioned Groups** list. (Note that exchange managers are able to view all documents regardless of their group memberships.)

You can select multiple groups at the same time by pressing the SHIFT or CTRL key while clicking the groups to highlight them.

5. Review the selections in the **See** column. Typically this option should be marked for every group unless permission to view the documents in this folder has been revoked for a particular group.

6. Determine whether the groups will be able to control the documents. Do this by marking the **Control** option next to the name of each group that will have this permission. Members of these groups will be able to modify the document only if their exchange roles (for example, manager or publisher) allow them to do so. Reviewers and previewers can control only the documents that they have added to the exchange.

Document control allows users to change other users’ permissions to the document, update the document or delete it.

7. Depending upon how your exchange has been set up, additional options may be displayed, allowing you to specify whether reviewers and previewers will be able to add documents or folders to this folder, and whether they will be able to edit the values for the folder’s custom fields. (This functionality sometimes is referred to as “limited publisher.”)

You may have to scroll horizontally to display these options.

- **Allow adding documents** — Mark this option for each group that contains reviewers and previewers who will be allowed to add documents to the selected folder. This option appears only if the **Allow Reviewers and Previewers to add documents to select folders** exchange setting is enabled.

  If the **Remember selections for future documents and subfolders** exchange setting also is enabled, reviewers and previewers who have permission to add documents to a folder will be able to add documents to subfolders within that folder, as well. This can be overridden for each subfolder.

- **Allow adding folders & documents** — Mark this option for each group that contains reviewers and previewers who will be allowed to add both subfolders and documents to the selected folder. This option appears only if the **Allow Reviewers and Previewers to add documents to select folders** exchange setting is enabled.

  If the **Remember selections for future documents and subfolders** exchange setting also is enabled, reviewers and previewers who have permission to add documents to a folder will be able to add documents to subfolders within that folder, as well. This can be overridden for each subfolder.

  When members of the selected groups add documents, they will be able to send an email alert to other limited publishers with permission to the folder where the new documents are stored. Alerts will be sent to all limited publishers with permission to the folder. Reviewers and previewers without limited publisher permission will not receive alerts.
If folder custom fields are being used on this exchange, members of the selected groups will be able to edit the name and set custom field values for the folders that they have created.

This option appears only if the Allow Reviewers and Previewers to create subfolders and add documents to select folders exchange setting is enabled.

- **Allow editing of folder custom fields** — Mark this option for each group that contains reviewers and previewers who will be allowed to edit the values of custom fields for the selected folder. This option appears only if the Allow Reviewers and Previewers to edit custom fields to select folders exchange setting is enabled.

8. Determine whether the documents will be protected.

For each permissioned group, you can choose an additional level of security for PDF and Microsoft Office documents. For each group, select one of the following options from the Protection list:

- **Do not protect**
- **Protect**
- **Protect/No Print**

With document protections, you can prevent users from downloading copies of the documents or require them to enter their email address and password before viewing a downloaded copy of the documents. You also can prevent users from printing the documents.

The type of browser, browser version, and browser settings determine whether the document can be downloaded, or must be viewed on the exchange. For detailed information about document protections, see Chapter 5, Publishing documents, on page 60.

9. When you have finished setting permissions, click **Save**.

**Overriding folder-level permissions**

Once you have set permissions for a folder, you may find that specific documents or subfolders require different permissions. If this is the case, use the following procedure to override the default selections provided by the folder.

When you move documents and subfolders from one permissioned folder to another, the documents’ and subfolders’ permissions are changed to match the new folder. If you override any permissions settings, however, those settings will not be changed when the items are moved.

**To override folder-level permissions for subfolders and documents**

The **Documents** tab should be displayed.

1. Highlight the folder whose permissions you want to change.
2. From the More Actions menu, select Permissions. The Permissions view of the Set Folder Permissions window appears, listing the groups that have been permissioned to the folder.
3. Mark the Override option next to each group whose permissions you want to change. The Permission option becomes active for the selected group.
Depending upon how the exchange is set up, additional options may become active, as well.

To override the permissions for all groups, mark the box that appears at the top of the Override column.

4. If you do not want the group to view documents in the selected folder(s), select No permission in the Permission column. (If you select this option, other options for the group are dimmed and cannot be changed.)

5. Depending upon how your exchange is set up, you may be able to specify whether reviewers and previewers will be able to add documents or folders to this folder, and whether they will be able to edit the values for the folder’s custom fields. (This functionality sometimes is referred to as “limited publisher.”)

You may have to scroll horizontally to display these options.

- **Allow adding documents** — Mark this option for each group that contains reviewers and previewers who will be allowed to add documents to the selected folder. This option appears only if the Allow Reviewers and Previewers to add documents to select folders exchange setting is enabled.

  If the Remember selections for future documents and subfolders exchange setting also is enabled, reviewers and previewers who have permission to add documents to a folder will be able to add documents to subfolders within that folder, as well. This can be overridden for each subfolder.

- **Allow adding folders & documents** — Mark this option for each group that contains reviewers and previewers who will be allowed to add both subfolders and documents to the selected folder. This option appears only if the Allow Reviewers and Previewers to add documents to select folders exchange setting is enabled.

  If the Remember selections for future documents and subfolders exchange setting also is enabled, reviewers and previewers who have permission to add documents to a folder will be able to add documents to subfolders within that folder, as well. This can be overridden for each subfolder.

  When members of the selected groups add documents, they will be able to send an email alert to other limited publishers with permission to the folder where the new documents are stored. Alerts will be sent to all limited publishers with permission to the folder. Reviewers and previewers without limited publisher permission will not receive alerts.

  If folder custom fields are being used on this exchange, members of the selected groups will be able to edit the name and set custom field values for the folders that they have created.

  This option appears only if the Allow Reviewers and Previewers to create subfolders and add documents to select folders exchange setting is enabled.

- **Allow editing of folder custom fields** — Mark this option for each group that contains reviewers and previewers who will be allowed to edit the values of custom fields for the selected folder. This option appears
only if the Allow Reviewers and Previewers to edit custom fields to select folders exchange setting is enabled.

6. If the documents on this exchange are protected (the enable protection of PDF and Microsoft Office documents exchange setting is enabled), you can change the protections applied to this group; to do so, make a selection from the Protection list. Options in the Protection list are described in Chapter 6, Protecting documents, on page 93.

7. When you have made changes for all the groups you wish to change, click OK.

Making a document available to all exchange users

If the All Users - Current and Future option is enabled for your exchange, you can use this option to allow all users to view selected documents.

When you permission documents using the All Users - Current and Future option, all existing members of the exchange are given access to the documents, and new exchange users will be given access to the documents automatically when they are given access to the exchange. If your exchange uses folder-level permissioning, folders can be permissioned using the All Users - Current and Future option, as well.

When the All Users - Current and Future option is selected, users can view documents, but have no other capabilities unless their exchange role allows it. If you want specific user groups to be able to modify documents, you must give them permission to control the documents separately.

The All Users - Current and Future option may not appear on your exchange. It must be enabled or disabled by an Intralinks employee.

To make an individual document available to all exchange users

The Documents tab should be displayed.

1. Highlight the document that you want to make available to all users.
2. From the More Actions menu, select Permissions. The Permissioned Groups screen for the document appears.
3. Mark the See box that appears next to the All Users - Current and Future option.
4. Click Save.

Moving documents

In Intralinks Platform, moving documents is as easy as dragging them from their original location and dropping in the location where you want for them to appear.

You can select several documents and move them at the same time if you like. To do this, press the SHIFT or CTRL key while clicking on each document; continuing to press the SHIFT or CTRL key, drag the documents to their new location.

If you drag documents from an indexed folder to an unindexed folder, the documents’ index numbers are removed. Likewise, if you drag documents from an unindexed folder to an indexed folder, the documents are indexed.
(When you drag and drop documents in Intralinks, the documents are moved; they are not copied.)

If you want to undo a move action, click the **Undo Move** button in the menu bar at the top of the screen.

To learn more about indexing, see “Indexing folders and documents” on page 64. To learn more about how frozen exchange items are handled, see “Freezing and unfreezing exchange items” on page 65.

### Sending alerts

Email messages alerting users about a document generally are sent when a document is created or updated. If you want to send a message to users at another time, though — for example, to remind them to read a particular document — you can use the following procedures to do so.

#### To send alerts for a individual document

The **Documents** tab should be displayed.

1. Highlight the document for which you want to send an alert.
2. From the **More Actions** menu, select **Alerts**. The alerts window for the document appears.
3. For each user or group you want to receive an alert email, mark the **Alert** option. To send an alert to all exchange managers, mark the **Auto Permissioned Users** option.
4. If you want to override automatically permissioned users’ preferences to receive daily summary email alerts or no alerts, select **Immediate** from the **Override Alert Preference** list. This option does not appear for groups.
5. (Optional.) If you want to edit the subject line or add a note to the email alert, do so using the **Subject** and **Note** fields. Your note will appear in the body of the email message.
6. Click the **Save** button.

#### To send alerts for multiple documents

The **Documents** tab should be displayed.

1. Highlight the documents for which you want to send an alert. Do this by pressing and holding the **SHIFT** or **CTRL** key while you click each document to select it.
2. From the **More Actions** menu, select **Alerts**. The alerts window for the document appears.
3. For each user or group you want to receive an alert email, mark the **Alert** option. To send an alert to all exchange managers, mark the **Auto Permissioned Users** option.

The users you select will receive an alert only for the documents for which they have permission to see or control. They will not receive any sort of notice about documents they cannot view.
4. If you want to override automatically permissioned users' preferences to receive daily summary email alerts or no alerts, select Immediate from the Override Alert Preference list. This option does not appear for groups.

5. (Optional.) If you want to edit the subject line or add a note to the email alert, do so using the Subject and Note fields. Your note will appear in the body of the email message.

6. Click the Save button.

Deleting documents

To delete a document, follow the procedure below or simply highlight the document and press the DELETE key. Use care when deleting documents; once a document has been deleted, the action cannot be undone.

If the document being deleted is indexed, all items that appear below the document within this folder will be reindexed to reflect this change. When exchange items are frozen, documents cannot be deleted.

To learn more about indexing, see “Indexing folders and documents” on page 64. To learn more about how frozen exchange items are handled, see “Freezing and unfreezing exchange items” on page 65.

To delete a document from your exchange

The Documents tab should be displayed.

1. Using the Documents smart filters, locate the document that you want to delete. Click the document to highlight it.
   To select multiple documents, press the SHIFT or CTRL key while clicking the documents to highlight them.

2. From the More Actions menu, select Delete Document. A message appears asking you to confirm your decision.
   Note that if you remove a document from the exchange by mistake, the action cannot be undone; if you have a copy of the document on your computer or a network drive, you will have use that copy to re-add the document to the exchange as though it were a new document.

3. Click Delete.

Copying and pasting documents

You can copy any document or folder and paste it into another location on the exchange or into another exchange if you have the rights to add folders and documents in the new location. (That is, if you are a manager or publisher on the exchange where you want to paste the items.)

Note, however, that protected Microsoft Office and PDF documents can be pasted only in the exchange where they originated.

To copy and paste documents

◊ To copy and paste documents, use the Copy Document and Paste Document commands on the More Actions menu.
Using working sets to copy documents from one exchange to another

To learn how to create and manage working sets, see “Creating working sets” on page 36.

▶ To copy the documents in a working set to another exchange

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Select the Documents tab on the left side of the screen. The working sets that you have created appear in the lower left area of the screen.
2. Right-click the working set that contain the documents that you want to copy. A menu appears.
3. Select Copy Documents.
4. An informational message appears. Read the message, then click Close.
5. Display the exchange where the documents are to be copied and highlight the folder where you want to paste the documents.
6. From the More Actions menu, select Paste Items. The Paste Options screen appears.
7. Mark the Document notes option if you want the notes associated with the documents in the working set to be pasted along with the documents.
8. Click Save.
9. An informational message appears, alerting you that the documents are being copied; you will receive an email message when the files have been copied. Click Close.

Checking out documents

You can use the Check Out command to lock any document that you have the ability to update. While a document is checked out, other users cannot make any changes to it; they will be able to view and print the document, however. Checking out documents prevents multiple versions of the document from being created.

Once a document has been checked out, only the person who checked it out, a manager with the Manager Plus exchange role or an Intralinks administrator can check the document in again.

▶ To check out a document

1. Highlight the document that you want to check out and select Check-Out from the More Actions menu.
   You can select multiple documents at the same time by pressing the SHIFT or CTRL key while clicking the documents to highlight them.
2. (Optional.) Enter a comment to describe your reason for checking out the document. This comment will appear on the document’s Properties screen while it is checked out.
3. Click Check-Out.
To check in a document

◊ Highlight the document that you want to check back in and select Check In from the More Actions menu.

Importing information using Intralinks Designer

If you have been assigned the Manager Plus exchange role, you can use Intralinks Designer to organize and manage the contents of your exchange. Intralinks Designer allows managers to upload and manage content and users en masse.

Note: You can use Intralinks Designer only if you have one of the following exchange roles: Manager Plus, Hidden Manager Plus, Manager, Publisher Plus. Your organization’s software deployment policies may prevent you from installing and using Intralinks Designer even if you have one of these roles. If Intralinks Designer is not available to you, you can use Multi-file Uploader to add multiple documents at the same time from your computer or network drive. For more information, see “Adding multiple documents at the same time” on page 72.

This Windows-based application acts as a staging area; while viewing the content of the exchange through Intralinks Designer, you can update existing folders and documents and add new content from your local drives. You can use Intralinks Designer to reorganize and delete content. In addition, you can add, remove and synchronize participant information with other databases.

When you have finished staging the content and updating participant information, you can upload the new or modified information to your exchange.

Information about using Intralinks Designer can be found in the Intralinks Designer User Guide or the Intralinks Designer help system.

To start Intralinks Designer

◊ From the Hub: From the Actions menu, choose Intralinks Designer.

◊ From within an exchange: First, click the Documents or Users & Groups button on the left side of the screen. Then choose Intralinks Designer from the More Actions menu.

If Intralinks Designer is installed on your computer, it is launched. If you have not installed Intralinks Designer yet, a screen appears, providing you with information about installing the application and a link to the Intralinks Designer installer.

Note: If you launch Intralinks Designer from Intralinks Platform and then close either Intralinks Designer or Intralinks Platform, both applications will be closed.

Using naming conventions to standardize document names

You can create naming convention rules to ensure that document names conform to your organization’s standard operating procedures. Documents governed by the guidelines specified in a naming convention rule will be renamed automatically when it is added to the exchange, updated, copied into a new exchange or submitted to the exchange via a business process instance.

When creating naming conventions, you can use custom fields for exchanges, groups, users and documents in conjunction with the new naming conventions.
function to rename documents that are added to the exchange following preset rules. With naming conventions, you also can control how custom field data is captured in the name. For instance, you can remove spaces or replace them with underscores, convert text to lowercase or uppercase, convert the first letter of each word to uppercase, and select a specified number of characters from the beginning of an element to include (for example, the first three characters).

In order for you to use naming conventions, an exchange setting, naming rules, must be enabled by an Intralinks administrator. If you wish to use this function, contact Intralinks for assistance. Only users with the Manager Plus user role can create naming conventions.

Once enabled for use, naming conventions will automatically rename documents when they are added to the exchange, when a document’s custom field values are changed, when documents are copied from one exchange to another, and when documents that were submitted to the exchange using a business process are published. Documents are not renamed again if changes are made to custom fields for users, groups or the exchange, or if a change is made to the naming convention that was used to name the document.

Once naming conventions have been created, they must be activated in order to be used. Active naming conventions can be deactivated, and inactive conventions can be reactivated. If you modify a naming convention, existing documents that were named using the convention will not be affected. Also note that documents that existed on the exchange before the rule was created will not be renamed unless the documents are updated. Naming conventions for all your exchanges can be viewed in the Hub, and they can be copied from one exchange to another.

If documents are renamed using naming conventions, this action will be reflected on the History screen for the documents.

**To create a new naming convention rule**

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the Maintenance button to display a list of maintenance tasks. From the list of options, select Naming Conventions. A list of the naming convention rules created for the exchanges that you manage also appears.

2. From the Actions menu, select Add New Naming Convention. The Properties step of the Naming Conventions wizard appears.

3. Select the exchange in which the naming convention will be used: Click the Choose button to display a list of exchanges for which you have the Manager Plus exchange role; highlight the exchange that you want, then click the x button to close the list.

4. Enter a name for the rule and, if you like, a description of the rule.

5. Click Next. The Document Type step appears.

6. Using the custom fields that appear on the Document Type screen, select the attributes that describe the documents that are to be renamed. As you make your selections, additional fields may appear. Select information that applies to all the documents that you wish to be renamed; only documents that match all your selections will be renamed using this rule.
Be careful not to make selections that will exclude documents that you want. Some fields may be left blank; for example, if some of the target documents will not have an effective date, do not specify a range of effective dates.

**Note:** Only custom fields that are marked as required can be used to create naming conventions. Also note that the entries in the selected fields must exactly match your entry in this wizard in order for the document to be renamed. For example, if you create a rule for documents that contain *Europe* in the Region custom field, documents for which *Europe* is entered as the region will be renamed, but documents for which *EU*, *EMEA* or *europe* is entered will not be renamed.

7. When you have made your selections, click Next. The Template step of the wizard appears. The Template screen allows you to select the elements that will be used to name the documents governed by this rule.

8. Click Add Element to add an element to your new rule.

You can choose exchange or document attributes (such as owner name or effective date), or make a “free text” entry of your choosing. Depending upon your selection, additional fields will appear, allowing you to define this element of the rule that you are creating.

Once you have selected an element, review the formatting selections that appear for it and make any needed changes. For text elements, like names, you can choose to display all characters in the element (for example, the entire exchange name), a certain number of characters (for example, the first 10 characters in the name), or the first word in the element. You can remove spaces between words or replace them with underscore (_) characters, and you can make the text all uppercase (AAA), lowercase (aaa), or title case (Aaa) if you like. For date elements, you can choose the format of the date.

Click Add Another Element to continue adding elements. When you have added and formatted all the elements you want to include, click Done.

**Note:** You can include any number of elements in your naming convention rule, but keep in mind that document names can be no more than 245 characters long, plus an extension, in Intralinks exchanges. Names that exceed 245 characters will be automatically shortened to 245 characters, potentially circumventing your organization’s standard operating procedures for naming documents.

9. Review the sample name that appears in the middle of the Template screen. To make changes to a particular element, click on it, then choose to delete it, move it to the left or right, or edit its formatting. Click Add Element if additional elements are required.

10. (Optional.) You can apply formatting rules to all the elements if you like. As with individual elements, you can remove spaces between words or replace them with underscore (_) characters, and you can make the text all uppercase (AAA), lowercase (aaa), or title case (Aaa) if you like. Note that your selection here will be used regardless of any selections you might have made for individual elements.

11. (Optional.) Select a character to separate the elements that you have selected.

12. When the rule is complete, click Save to save your changes.
Activating naming conventions

After you have created naming conventions, you need to activate them before they can be used.

1. Click the Maintenance button to display a list of maintenance tasks. From the list of options, select Naming Conventions. A list of the naming convention rules created for the exchanges that you manage also appears.
2. Highlight the naming convention that you want to activate.
3. From the Action menu, select Activate Naming Convention.

Once a naming convention has been activated, you can deactivate it. This disables the naming convention, but does not remove it, and you can reactivate it later. To deactivate an active naming convention, highlight it and select Deactivate Naming Convention from the Action menu.

Copying naming conventions from one exchange to another

You can copy naming conventions from one exchange to another. The following restrictions apply, however:

- You must be assigned the Manager Plus exchange role on both the source exchange and the target exchange in order to copy naming conventions.
- Both exchanges must have been created using the same template, to ensure that custom fields that may be used in the naming conventions are the same in both exchanges.

To copy naming conventions from one exchange to another

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the Maintenance button to display a list of maintenance tasks. From the list of options, select Naming Conventions. A list of the naming convention rules created for the exchanges that you manage also appears.
2. Highlight the naming convention that you want to copy.
3. From the Action menu, select Copy Naming Convention. The Copy Naming Convention screens appears.
4. If you want to begin using the copied naming convention immediately, mark the Activate the Naming Convention after copy option.
5. Mark the box that appears next to each exchanges where you want to naming convention to be available.
6. When you have made all your selections, click Copy Naming Convention.
7. If you did not activate the naming convention, be sure to do so. For more information, see “Activating naming conventions” on page 90.
Enabling reviewers and previewers to publish documents, add folders and edit folder custom fields

Although managers and publishers generally publish documents and add folders, there may be instances where you want other people to be able to publish documents or add subfolders to a specific folder, but not have the ability to view the entire exchange or people other than the exchange managers. If this is the case, you may want to use Intralinks’ “limited publisher” function.

There are three separate limited publisher functions, and you can choose to use all of the functions, a combination of functions, or none of the functions. The functions are:

- **Adding documents** — enabled using the Allow Reviewers and Previewers to add documents to selected folders exchange setting

  If reviewers and previewers in selected groups have been given the ability to add documents, they also will be able to update, move and delete documents that they have added. (When moving documents, reviewers and previewers must have the ability to add documents to both the original folder and the new folder location.)

  When reviewers and previewers add documents, they will send an email alert to other limited publishers with permission to the folder where the new documents are stored. Alerts will be sent to all limited publishers with permission to the folder. Reviewers and previewers without limited publisher permission will not receive the alerts.

- **Creating subfolders and adding documents** — enabled using the Allow Reviewers and Previewers to create sub folders and add documents to selected folders exchange setting

  If reviewers and previewers in selected groups have been given the ability to create subfolders, they will be able to rename the folders and edit custom field values for them.

- **Editing custom field values for the selected folder** — enabled using the Allow Reviewers and Previewers to edit custom fields to selected folders exchange setting

  These exchange settings must be changed by an Intralinks administrator. If you decide that you want to enable one or more of these functions, contact Intralinks customer support for assistance.

  If one or more of these functions is enabled, managers can select the groups that are allowed to perform these functions on a folder-by-folder basis.

*If the exchange uses folder-level permissioning*

If the Remember selections for future documents and subfolders exchange setting is marked, folder-level permissioning is being used. Reviewers and previewers who have permission to add documents to a folder will be able to add documents to subfolders within that folder, as well. This can be overridden for each subfolder.
As you create folders, you can mark the limited publisher options on the Add New Folder screen for each group that will have permission to add documents to the folder. For more information, see “Creating folders” on page 60.

*If the exchange uses document-level permissioning*

If the Remember selections for future documents and subfolders exchange setting is *unmarked*, document-level permissioning is being used. Users will be able to add documents only to the folders for which they have been given permission. They will not be able to add documents to subfolders, except for the subfolders that they created themselves.

If the exchange uses document-level permissioning, you must use the Set Folder Permissions screen to assign limited publisher privileges to reviewers and previewers. For more information, see “If you use document-level permissioning” on page 77.

**Important!** Reviewers and previewers cannot set permissions for the documents they add to your exchange. Documents added by reviewers and previewers will be visible automatically to the people who added them and to users with the following exchange roles: Manager Plus, Hidden Manager Plus, Manager and Publisher Plus. If you want the documents to be visible to other users, you or another exchange manager will have to give those users permission to view the documents.
Chapter 6: Protecting documents

When you permission documents, you determine who is allowed to view the documents. Document protection provides an added level of security, allowing you to determine what users can do with the documents they have been given permission to view.


What is document locking and protection?

Document locking and protection — also known as Information Rights Management, or IRM — provides an added level of security for documents in PDF or Microsoft Office (Word, Excel and PowerPoint) format. With document locking and protection, users are either:

• Prevented from downloading documents from an exchange to their computer or network, or

• Required to enter their email address and Intralinks password before opening a downloaded copy of the document, which is encrypted.

The document format and browser that the individual is using determines whether the file can be downloaded or must be viewed online.

Protected documents can be identified in the Documents List by a lock icon that appears to the left of the document name. If the document is protected and printing is not allowed, a printer icon appears with a red X on top of it.

Exchange managers and publishers can determine whether protection will be applied to individual documents. In addition, exchange managers and publishers can prevent users from printing protected documents.

Document protection capabilities

Intralinks’ document protection solution includes the following capabilities:

• Supports access to protected documents on Windows and Mac OS.
  Supports Microsoft Office 2007, 2010 and 2013 documents (Windows), including those that have been digitally signed.
  Supports Microsoft Office 2009 and 2011 documents (Macintosh), including those that have been digitally signed.
  Supports PDF documents.

• Allows watermarks to be placed diagonally across documents, Watermarks appear when documents are displayed onscreen and on printed documents. Watermarks cannot be applied to Excel documents that contain dynamically generated charts or graphs. Watermarks can be applied to Excel documents that contain static images if they were
created using Excel 2007 or a later version. Watermarks can be positioned only at a diagonal across the center of the document; there are no options for placing them in other areas of the page.

Note that watermarks cannot be applied to documents, including Excel documents, that include dynamic charts or graphs.

- Prevents users from making screen captures using the Print Screen key or Microsoft’s Snipping Tool, but screen captures can be made using a third-party tool like Techsmith Corporation’s Snagit®. (The disallow use of Print Screen exchange option must be enabled.)

- Allows permissioned users of Microsoft Excel documents to perform a limited number of actions that allow the users to perform ad hoc analysis while maintaining document security. Supported actions include resizing of cells, editing of cell values, ability to add columns and rows, and the ability to sort data. Users cannot save the changes they make.

- Supports Single Sign-On (SSO) for both Windows and Mac OS.

- Allows users who are logged into Intralinks Platform or are connected to their organization’s network via SSO or Exclusive Single Sign-On (e-SSO) to view downloaded copies of protected documents without first entering his or her credentials.

Printing of protected Microsoft Office documents is not tracked, and printing instances not included in totals on the Exchange Activity Summary Report. If your organization requires this information, you can require users to view documents using Intralinks Viewer, which provides tracking of both the number of times a document is printed and the amount of time the document is viewed. (Printing is tracked for PDF documents, however.)

Requirements for end users

In most cases, end users will not have to take any action in order to view protected documents — they can simply enter their email address and Intralinks password, and the file will open.

Adobe Reader 10 or a later version is required in order to view protected PDFs. Files must be viewed in Adobe Reader; they cannot be viewed directly within a web browser or any other PDF reader application.

When a user attempts to open a protected Microsoft Office document in a new browser for the first time, a message will appear asking the user to download and open a registration file within a specified period of time. When the user opens the file, the browser is registered and the protected Microsoft Office file is opened. The user will not be asked to register that browser again unless the user removes the “cookie” files associated with the browser.

Applying protections

In order for you to apply protection to documents, the exchange option enable PDF and Microsoft Office protection must be selected on the settings screen for your exchange.

Protections can be applied using:
The New Document Wizard

The Permissions screen for individual documents

The Permission Overview screen

The Permissions tab (if you are working in an exchange that uses Intralinks’ M&A industry template)

Using any of these screens, select one of the following protection options:

- **No Protection** or **Do not protect** – Choose this option if selected users are allowed to print the document and to view downloaded copies of the document without entering their Intralinks credentials.

- **Protect** – Choose this option to limit users’ ability to modify the document or share it with others.

  Depending upon the browser being used and the settings selected for it, the user may be restricted to viewing documents on the exchange, or may be required to enter his or her email address and password in order to open the document, if the browser allows it to be downloaded. (Only the user who downloaded the document is allowed to open it.)

  If this option is selected, users cannot copy and paste text to another document. (To prevent users from capturing images of documents, be sure that the Disallow use of Print Screen exchange setting is enabled.)

  Protected documents are encrypted and are protected online, offline and while in transit.

- **Protect/Prevent Print** – Choose this option if the selected users are not allowed to print the document or open a downloaded copy of the document without first entering their credentials.

  Note that if you select Protect, viewers will be able to print the document and share the printed copy with others. If the document is particularly sensitive, consider enabling the watermarking feature for your exchange to ensure that any printed copies can be traced back to the user who printed them. Watermarking provides an extra measure of security in situations where you do not wish to prevent printing. Contact Intralinks customer support for assistance in setting up watermarks.

  Detailed instructions adding and modifying documents are found in Chapter 5, Publishing documents, on page 60.

**Changing protection settings**

**Note:** The instructions below are for changing protection settings only. If you wish to set both permissions and protection options for documents, see Chapter 7, Managing document permissions, on page 97.

You can change the protection settings for your documents at any time using the Permission Overview screen or the Permissions screen for individual documents.

▶ **To review and modify protections using Permission Overview**

  The Documents tab should be displayed.
1. Highlight the document or documents that you want to view or change. To view all the documents in one or more folders, highlight the folders.

2. From the More Actions menu, select View All Permissions. The Permission Overview screen appears displaying information about the top-level folders on the exchange.

3. Double-click a top-level folder to view the subfolders and documents stored within it.

4. To change a particular group’s protection settings for a particular document, highlight the group’s current settings and then choose the settings you want from the Protections list.

   You can select several documents and apply the same settings to them at the same time if you like. To do this, press the SHIFT or CTRL key while clicking on the protections for each document. You also can click and drag the mouse to select rows or columns of protections that are next to one another.

5. Click Save.

Tracking user activity

Three reports provide information about users’ document viewing time based on the length of time documents are displayed in Intralinks Viewer. These reports are:

- Document Access Report
- Group Coverage Report
- Multi-user Coverage Report

These reports display the total viewing time for each document by user or group. Keep in mind that the reports track only the time that the documents were displayed in Intralinks Viewer; if the documents are displayed in another application, that time is not included. As a result, time tracking is most effective in exchanges that do not allow users to open documents in applications other than Intralinks Viewer.

For more information about the these reports, see “Viewing document reports” on page 181, “The Group Coverage Report” on page 186 and “The Multi-user Coverage Report” on page 185. To learn more about Intralinks Viewer’s time tracking capabilities, see “Using Intralinks Viewer to track users’ viewing time” on page 26.
Chapter 7: Managing document permissions

Overview

User groups that are allowed to view particular documents are permissioned to those documents. Permissioning provides an effective way for you to manage sensitive information, keeping them out of sight of users who should not have access to the information within them. Permissions generally are set when documents or folders are added to the exchange. You can use the procedures in this chapter to change the permissions that were previously assigned to documents and folders.

In this chapter you will learn how to:

• Set and update permissions for documents
• Set and update folder-level permissions that will be applied to all documents and subfolders within a selected folder
• Override folder-level permissions

Reviewing and modifying permissions

Using the Permissions Overview screen, you can review and change the permissions for documents quickly and easily. You can view and change permissions for a single document, for multiple documents, or even for the documents in multiple folders. The Permissions Overview screen provides a snapshot of all the groups with permission to the document, along with their security settings. You can export this information to Microsoft Excel, as well.

To review and modify permissions using the Permissions Overview screen

The Documents tab should be displayed.

1. Highlight the document or documents that you want to view or change. To view all the documents in one or more folders, highlight the folders.
2. From the More Actions menu, select View All Permissions. The Permissions Overview screen appears displaying information about the top-level folders on the exchange.
3. Double-click a top-level folder to view the subfolders and documents stored within it.
4. If you want to change a particular group’s permissions to use a document, highlight the group’s current settings and then choose the settings you want from the Selected Permissions list. To change a particular group’s security settings for a document, highlight the group’s current settings and then choose the settings you want from the Protections list. To learn more about document protections, see Chapter 6, Protecting documents, on page 93.

You can select several documents and apply the same settings to them at the same time if you like. To do this, press the SHIFT or CTRL key while clicking on...
the permissions for each document. You also can click and drag the mouse to select rows or columns of permissions that are next to one another.

5. (Optional.) To export the permissions information for the selected document, click the Export button. Microsoft Excel is opened and a spreadsheet containing the document’s permissions information appears.

6. Click Save.

▶ To apply a group’s document permissions to another group

If the same (or similar) document permissions apply to more than one group, you can set the permissions for a single group and then copy those permissions to one or more additional groups. Once you have copied the permissions, changes can be made to the permissions for individual documents if necessary. To make changes for individual documents, see “To review and modify permissions using the Permissions Overview screen” on page 97.

Use this feature with care; once changes are made, they cannot be undone.

The Users & Groups tab should be displayed.

1. Highlight the group whose permissions are already set — the group whose permissions will be copied to other groups.
2. From the More Actions menu, select Copy Group Permissions. The Copy Group Permissions window appears.
3. For each group whose permissions you want to update, mark the box in the Copy Permissions column.
4. Click Save. The settings for the group you selected in step 1 are applied to all the groups you selected in step 2.

Setting permissions for all the documents in one or more folders

You can set or change permissions for all the documents in a folder — or for the documents in multiple folders — at the same time. This is referred to as bulk permissioning.

Depending upon how your exchange has been set up, when you use bulk permissioning, you will either set permissions for the documents within the folder, or assign permissions to the folder itself:

- If your exchange allows you to set permissions for the documents within a folder, your selections are applied to whatever documents are located in the folder at the time of permissioning. Documents added at a later time are not affected and must be permissioned separately.

- If your exchange allows you to set permissions for the folder itself, your selections will be applied to the documents and subfolders within the folder at the time of permissioning. These selections will be remembered, and they will be assigned automatically to documents and subfolders added to the folder later.

Note that you can use one method of permissioning or the other, but not both at the same time. In either case, the permissions for individual documents (or subfolders, in the second instance) can be overridden, and different permissions assigned to them.
An exchange setting, **Remember selections for future documents and subfolders**, determines which method is used. For more information about exchange settings, see Appendix A, *Exchange settings*, on page 194.

You also can use the **Permissions Overview** and **Copy Group Permissions** screens to set permissions for many documents at once. For more information, see “To review and modify permissions using the Permissions Overview screen” on page 97 and “To apply a group’s document permissions to another group” on page 98.

**If you use document-level permissioning**

Use the procedure below if the **Remember selections for future documents and subfolders** exchange setting is *unmarked* for the exchange that you are using.

**To modify permissions for all the documents within one or more folders**

Note that you are setting permissions only for the documents *currently* in the folder(s). Any documents added to the folders in the future will have to be permissioned when they are added.

The **Documents** tab should be displayed.

1. Highlight one or more folders.
2. From the **More Actions** menu, select **Set Folder Permissions**. The **Set Folder Permissions** window appears.
3. For each group, use the list in the **Permission** column to change the group’s permissions for the selected documents. If you want to change permissions for all groups, make your selection from the **All Groups** list.
   - **Keep existing permissions** – No changes are made; whatever permissions currently are in place will continue to apply for this group.
   - **No permission** – Members of the selected group have no access to the documents in the selected folders. Neither the documents nor the folders will be visible to these users.
   - **See** – Members of the selected group will be able to view documents in the selected folders, but will not be allowed to change them in any way.
   - **Control** – Members of the selected group will be able to modify the documents if their exchange roles (for example, manager or publisher) allow them to do so. Document control allows users to change other users’ permissions to documents, update the documents or delete them.
4. If the documents in this exchange are protected (the **enable protection of PDF and Microsoft Office documents** exchange setting is marked), a **Protection** column is displayed. For each permissioned group, you can choose an additional level of security for these documents. With document protections, you can prevent users from downloading copies of the documents or require them to enter their email address and password before viewing a downloaded copy of the documents. You also can prevent users from printing the documents.
The type of browser, browser version, and browser settings determine whether the document can be downloaded, or must be viewed on the exchange. For detailed information about document protections, see Chapter 6, Protecting documents, on page 93.

For each group, select one of the following options from the Protection list:

- Do not protect
- Protect
- Protect/No Print

Note: when printing is allowed, the file can be printed not only to paper but also to other file types using the browser’s “Print As” function. Copies created using “Print As” are no longer signed or protected documents, even though the original file was protected. Clients who are concerned that downloaded protected files may be saved in this fashion should select the Protect/No Print option for their documents.

5. When you have made all the needed changes, click Save.

If you use folder-level permissioning (permissions are inherited)

Use the procedure below if the Remember selections for future documents and subfolders exchange setting is marked for the exchange that you are using.

Using this procedure, you can set permissions for the contents of a folder (the documents and subfolders within it), and those settings are applied to existing contents and to all new content added to that folder. You will be able to override these default permissions for individual documents or subfolders if you like.

If you move documents or subfolders from one permissioned folder to another, the permissions are changed automatically. (Any changes you made to the inherited permissions will be remembered when the items are moved. All the inherited permissions for the old folder that have not been changed will be replaced by the inherited permissions for the new folder.)

**To modify permissions for folders**

The Documents tab should be displayed.

1. Highlight the folder whose permissions you want to modify.

2. From the More Actions menu, select Permissions. The Permissions view of the folder’s information screen appears, listing any groups that have been permissioned to the folder already.

3. Click Permission Groups. A list of unpermissioned groups appears on the left side of the screen, and the groups that already have been permissioned to the folder appear on the right. (Note that groups in the Permissioned Groups list do not have the ability to see documents in this folder if the See option has been unmarked for them.)

4. In the Not Permissioned Groups list, locate the groups whose members should be able to use the documents in the selected folder. Highlight the groups and click the arrow button to move them to the Permissioned Groups list. (Note that exchange managers are able to view all documents regardless of their group memberships.)
You can select multiple groups at the same time by pressing the SHIFT or CTRL key while clicking the groups to highlight them.

5. Review the selections in the See column. Typically this option should be marked for every group unless permission to view the documents in this folder has been revoked for a particular group.

6. Determine whether the groups will be able to control the documents. Do this by marking the Control option next to the name of each group that will have this permission. Members of these groups will be able to modify the document only if their exchange roles (for example, manager or publisher) allow them to do so. Reviewers and previewers can control only the documents that they have added to the exchange.

Document control allows users to change other users’ permissions to the document, update the document or delete it.

7. Depending upon how your exchange has been set up, additional options may be displayed, allowing you to specify whether reviewers and previewers will be able to add documents or folders to this folder, and whether they will be able to edit the values for the folder’s custom fields. (This functionality sometimes is referred to as “limited publisher.”)

You may have to scroll horizontally to display these options.

- **Allow adding documents** — Mark this option for each group that contains reviewers and previewers who will be allowed to add documents to the selected folder. This option appears only if the Allow Reviewers and Previewers to add documents to select folders exchange setting is enabled.

  If the Remember selections for future documents and subfolders exchange setting also is enabled, reviewers and previewers who have permission to add documents to a folder will be able to add documents to subfolders within that folder, as well. This can be overridden for each subfolder.

- **Allow adding folders & documents** — Mark this option for each group that contains reviewers and previewers who will be allowed to add both subfolders and documents to the selected folder. This option appears only if the Allow Reviewers and Previewers to add documents to select folders exchange setting is enabled.

  If the Remember selections for future documents and subfolders exchange setting also is enabled, reviewers and previewers who have permission to add documents to a folder will be able to add documents to subfolders within that folder, as well. This can be overridden for each subfolder.

When members of the selected groups add documents, they will be able to send an email alert to other limited publishers with permission to the folder where the new documents are stored. Alerts will be sent to all limited publishers with permission to the folder. Reviewers and previewers without limited publisher permission will not receive alerts.

If folder custom fields are being used on this exchange, members of the selected groups will be able to edit the name and set custom field values for the folders that they have created.
This option appears only if the Allow Reviewers and Previewers to create sub folders and add documents to select folders exchange setting is enabled.

- **Allow editing of folder custom fields** — Mark this option for each group that contains reviewers and previewers who will be allowed to edit the values of custom fields for the selected folder. This option appears only if the Allow Reviewers and Previewers to edit custom fields to select folders exchange setting is enabled.

8. Determine whether the documents will be protected.

For each permissioned group, you can choose an additional level of security for PDF and Microsoft Office documents. For each group, select one of the following options from the Protection list:

- **Do not protect**
- **Protect**
- **Protect/No Print**

With document protections, you can prevent users from downloading copies of the documents or require them to enter their email address and password before viewing a downloaded copy of the documents. You also can prevent users from printing the documents.

The type of browser, browser version, and browser settings determine whether the document can be downloaded, or must be viewed on the exchange. For detailed information about document protections, see Chapter 6, *Protecting documents*, on page 93.

9. When you have finished setting permissions, click **Save**.

### Overriding folder-level permissions

Once you have set permissions for a folder, you may find that specific documents or subfolders require different permissions. If this is the case, use the following procedure to override the default selections provided by the folder.

When you move documents and subfolders from one permissioned folder to another, the documents’ and subfolders’ permissions are changed to match the new folder. If you override any permissions settings, however, those settings will not be changed when the items are moved.

**To override folder-level permissions for subfolders and documents**

The *Documents* tab should be displayed.

1. Highlight the folder whose permissions you want to change.
2. From the More Actions menu, select Permissions. The Permissions view of the Set Folder Permissions window appears, listing the groups that have been permissioned to the folder.
3. Mark the Override option next to each group whose permissions you want to change. The Permission and Allow Add options become active for the selected group. If this exchange allows documents to be protected, the Protection option become active, as well.
To override the permissions for all groups, mark the box that appears at the top of the Override column.

4. If you do not want the group to view documents in the selected folder(s), select No permission in the Permission column. (If you select this option, other options for the group are dimmed and cannot be changed.)

5. If you want reviewers and previewers in the group to be allowed to add documents to the selected folder and its subfolders, mark the Allow Add option.

This option appears only if the Allow Reviewers and Previewers to add documents to selected folders exchange setting is enabled.

6. If the documents on this exchange are protected (the enable protection of PDF and Microsoft Office documents exchange setting is enabled), you can change the protections applied to this group; to do so, make a selection from the Protection list. Options in the Protection list are described in Chapter 6, Protecting documents, on page 93.

7. When you have made changes for all the groups you wish to change, click OK.

Making a document available to all exchange users

If the All Users - Current and Future option is enabled for your exchange, you can use this option to allow all users to view selected documents.

When you permission documents using the All Users - Current and Future option, all existing members of the exchange are given access to the documents, and new exchange users will be given access to the documents automatically when they are given access to the exchange. If your exchange uses folder-level permissioning, folders can be permissioned using the All Users - Current and Future option, as well.

When the All Users - Current and Future option is selected, users can view documents, but have no other capabilities unless their exchange role allows it. If you want specific user groups to be able to modify documents, you must give them permission to control the documents separately.

The All Users - Current and Future option may not appear on your exchange. It must be enabled or disabled by an Intralinks employee.

To make an individual document available to all exchange users

The Documents tab should be displayed.

1. Highlight the document that you want to make available to all users.

2. From the More Actions menu, select Permissions. The Permissioned Groups screen for the document appears.

3. Mark the See box that appears next to the All Users - Current and Future option.

4. Click Save.
Chapter 8: Reviewing documents

Overview

In this chapter you will learn how to:

- Locate documents
- Create a list of favorite documents
- Open documents
- Download documents
- Print documents
- Work with IRM-protected documents
- Use Intralinks Viewer to view PDF and Microsoft Office documents

You have been invited to one or more Intralinks exchanges to participate as a reviewer of the documents stored on the exchange. As a reviewer, you have access to documents as long as you have access to the exchange where they reside, and, depending upon the security settings for individual documents, you can download and print them, as well.

Depending upon the exchange manager’s preferences, you may receive email messages, or alerts, when new documents are available for you to read. You can click a link in the alerts to display the document, or you can view all of the documents that are available to you by logging into Intralinks and displaying the Documents List.

Viewing documents

All the documents that you have permission to view appear in the Documents List.

Depending upon the security settings for the document you select to view, you may be required to enter your Intralinks ID and password before opening the document.

► To view documents within Intralinks

1. Open your exchange.
2. Click the Documents tab on the top of the screen. The Document List appears.
3. Locate the document. Double-click it, or click on it to highlight it, and then select Open Document from the More Actions menu.

   You can use the Search tools to locate the document. For more information about searching, see “Finding documents” below.

   If you download a file that may contain malicious content, a message will appear to warn you of the risk and give you the option not to continue with the download. The warning is based upon the type of file that you selected, not the actual content of the file. The message does not appear for file types that are commonly used by Intralinks’ clients.
Finding documents

Depending upon how your exchange has been set up, you can perform either basic searches or full-text searches. Basic searches find terms only if they appear in document or folder titles or notes. Full-text searches also find terms within the contents of the documents on the exchange.

See “Tips for using Intralinks’ search tools” on page 108 for information on performing searches using Boolean operators, using wildcards in your searches, searching for negative numbers and special characters and other tools for finding the information that you want.

To search for a document

The Documents tab should be displayed.

1. Enter your search term in the Search box in the upper right corner of the Intralinks Platform screen, then click Go. A list of documents that contain your search term is displayed.

   The search results you see are based on basic document information (the documents’ titles and notes). If the exchange manager has chosen to enable full-text search, all the contents of the documents are searched, as well.

   Note: If you enter more than one search term, your search results will include all documents that contain one word or the other. Your entry can be uppercase or lowercase; the Search field is not case sensitive.

2. To open the document you wish to review, highlight it and click the Open Document button near the top of the screen.

   If you download a file that may contain malicious content, a message will appear to warn you of the risk and give you the option not to continue with the download. The warning is based upon the type of file that you selected, not the actual content of the file. The message does not appear for file types that are commonly used by Intralinks’ clients.

   This message will appear if you select any file with one of the following extensions: *.ade; *.adp; *.asd; *.asx; *.bas; *.bat; *.chm; *.class; *.cmd; *.com; *.cpl; *.crt; *.dat; *.dll; *.exe; *.hcp; *.hta; *.ht; *.htm; *.html; *.inf; *.js; *.jse; *.lnk; *.mda; *.mdb; *.mdn; *.msc; *.msi; *.msp; *.nws; *.ocx; *.pif; *.p; *.pm; *.pot; *.pps; *.reg; *.scr; *.sct; *.shb; *.shs; *.sys; *.vb; *.vbe; *.vbs; *.vcf; *.wmd; *.wms; *.wms; *.wsc; *.wsf; *.wsh; *.xlt; *.xlw; *.zlb

To view only new documents

The Documents tab should be displayed.

1. Click the arrow that appears to the left of the New Since folder in the Smart Filters area on the left side of the screen. A number of filtering options appear: Last Login, Last 24 Hours, Last Week and Last Month.
(If the smart filters are not displayed, click on the Filters button to hide the folders list and display the filters.)

2. Click the option that you want to use. The documents list displays all the documents that match the period of time that you specified.

▶ To view only unread documents

The Documents tab should be displayed.

1. Click the Advanced Filter smart filter. The Exchange Filter Criteria screen appears, allowing you to select a variety of options for limiting the information that is displayed.

(If the smart filters are not displayed, click on the Filters button to hide the folders list and display the filters.)

2. To view only documents you haven’t read yet, mark the Unread Only option.

3. Click Filter.

▶ To view documents that were available on a previous date using the Historic Filter

The Documents tab should be displayed.

1. Click the gear icon that appears below the search box to display the Tools menu. Select Historic Filter from the menu. The Historic Filter Criteria window is displayed.

2. Choose one of the viewing options from the List by list:

   Date — Use this option to view all the documents that were available on a particular date in the past. Only the documents that were available to you on that date will be displayed.

   Date Range — Use this option to view all the documents that were available during a particular time period. Documents that were available at any point during the time period will be displayed.

   Saved View — If you have saved a particular view (for example, a filtered list of documents that are relevant to a task that you are performing), use this option to redisplay the view you saved.

   Depending upon your selection, additional fields will be displayed, allowing you to select the date, date range or saved view that you want.

3. Click Filter. The documents that were available at the specified time are displayed.

4. When you have finished viewing the historical view, select Historic Filter from the Tools menu again to redisplay the standard (current) view of your exchange.

▶ To create a saved view for historic filtering

The Documents tab should be displayed.

1. Display the documents that you want to include in the view.

2. Click the Save Current View button at the top of the screen. The Save Current View window is displayed.
3. Enter a name for the view, and click **Save**.

**To view documents by effective date**

The **Documents** tab should be displayed.

1. Click on **Unfiltered** or the Filter icon in the upper right corner of the documents list. A number of filters appears.

2. In the **Effective From** and **Effective To** fields, enter a range of dates for the documents that you want to view. All documents that have been assigned effective dates within this time period will be displayed.

3. To view recently added documents, enter a date in the **New Since** field, in the format MM/DD/YY (month, day, year). Or click the calendar icon and select the date you want from the calendar that appears.

   If the exchange does not enable you to see the dates on which documents were added or made available to you, the **New Since** field does not appear.

4. To view only documents you haven’t read yet, mark the **Unread Only** option.

   The documents list displays all the documents that match the requirements you have entered.

**To search for documents across multiple exchanges**

You can search multiple exchanges at the same using a variety of filters to limit the search results to relevant documents.

**Note:** Exchanges that use enhanced security must be open if you want for them to be included in your search results.

1. If the **Hub** is not displayed already, click the **Hub** button to display it.

2. Select the **Documents** tab to display the Documents List.

3. Enter your search term in the search box, then click **Search**. A list of documents that contain your search term is displayed.

   The search results you see are based on basic document information (the documents’ titles, keywords and notes). If one or more exchange hosts have chosen to enable full-text search, all the content of documents for those exchanges is searched, as well.

   **Note:** If you enter more than one search term, your search results will include all documents that contain one word or the other. Your entry can be uppercase or lowercase; the search field is not case sensitive.

4. (Optional.) If you want to limit the number of documents that appear in your search results, make selections in the **Refine your results** section of the screen. You can limit your search to particular exchanges, organizations, tags and file types. Only the items you select will be included in your search.

5. (Optional.) If you want to further refine your search, click the **Advanced Search** link below the search box. Using the Advanced Search screen, you can search for documents using a wide range of criteria, including working sets that contain the document, exchanges, tags, file types, document creator, and others.

6. To open the document you wish to review, double-click it.
7. (Optional.) If you want to save your search criteria for use again in the future, click the Save link at the top of the Documents List. A box appears allowing you to name your search.

To use saved search criteria in the future, click the arrow next to the search field. A list of all your saved searches appears. Select the search criteria that you want to use; the documents matching those criteria are displayed.

8. To clear your search results and perform a new search, click the Clear link at the top of the Documents List.

▶ To view a URL that can be used as a shortcut for your document

The Properties screen for documents includes a URL (Web address) for the document that you have selected. You can click the link to display the document. You also can copy the link and create a shortcut for it in your Internet browser, or send it to colleagues. (They must have permission to view the document in order to display it.)

The Documents tab should be displayed.

1. Display the document whose URL you want to view.
2. From the More Actions menu, select Properties. The Properties screen for the selected document is displayed.
3. Locate the Document Link field. Either click the link to display the document or copy the text to paste into your browser or an email message.

Tips for using Intralinks’ search tools

Use the tips below to get the most out of Intralinks’ powerful search function.

Searching for a phrase
To search for a particular phrase, place the phrase in double quotation marks: “Quarterly statements”

(If you do not use double quotation marks with your phrase, your search results will include all documents that include the words you entered, even if the words are separated from one another.)

Searching for negative numbers
To search for a negative number, use a minus sign and place the entire number, including the minus sign, in double quotation marks: “-550.00”

Omitting words from your search results
To prevent documents that contain particular words from appearing in your search results, type a minus sign before the terms you want to omit: quarterly -Q2

Finding documents that contain two or more words
To find documents that contain two or more words, simply type the words with a space between them: regulated legal

In the example above, only the documents that contain both regulated and legal would be listed in your search results.
Finding documents that contain one word or another
To find documents that contain one word or another one, but not both, type OR (uppercase) between the terms: regulated OR legal

In the example above, documents that contain both regulated and legal would be omitted from your search results.

Using special characters in your searches
Some characters are used for particular purposes by the Intralinks search tool. These characters include: - \ " < > [ ] { } : ~ ^

To include any of these characters in a search term, type a backslash (\) character in front of it: 4\:00 o'clock

Using wildcards to find variations of your search terms
Two characters, the question mark (?) and the asterisk (*), can be used to find variations of your search term. When you use these characters, the search function will "fill in the blanks."

To replace a single character, use the question mark. In the following example, all documents for Q1, Q2, Q3 and Q4 2009 will be displayed: Q? 2009

You also can use multiple question marks. In the following example, all documents containing references to the 20th century will be displayed: 19??

To find all variations regardless of the number, use the asterisk. The following example will return documents that include document, documents, documented and documentation: document*

Searching only the documents that appear in the documents list
You can limit your search to the documents currently displayed on the screen by clicking the arrow icon in the Search box, then selecting This View.

Searching only the titles and notes for documents and folders
You can limit your search to the titles, notes and other information that appears on folders' and documents' Properties screens. To do this, click the arrow icon in the Search box and mark the Document & Folder Properties option; if you see a Document Content option, be sure that it is unmarked. (This option does not appear on all exchanges.)

Finding documents using smart filters
Smart filters provide alternative views of the documents that appear on your exchange. These filters can improve your productivity by giving you easy access to recently added documents, unread documents, and documents that you have indicated are your favorites — that is, the documents you return to most often or that hold information that is most important to you.

With the exception of the Favorites filter, the contents of the smart filters folders are updated automatically as documents are added to the exchange and as you read the documents.
When you add documents to Favorites, copies of the documents are placed in the Favorites folder. The original documents remain in the folders from which they were copied.

**To view the contents of a smart filter**

◊ Click on the smart filters folder whose contents you want to view. The documents in the folder appear in the Documents List on the right side of the window.

**To add documents to the Favorites menu**

◊ Click on the document you want to add to the Favorites menu, then click the Add to Favorites button near the top of the screen.

**Downloading documents**

Note that the security settings applied to the documents you select may prevent you from downloading the documents or from opening downloaded documents unless you enter your credentials (Intralinks ID and password).

**To download a document**

1. Locate the document you wish to download, and click on it to highlight it.
2. Click the Download button at the top of the screen. A message asking you whether you want to open or save the document appears.
3. Click Save. A Save As dialog box appears.
4. Choose a location on your local drive for the document, and click Save.

**Bulk downloading documents from a single exchange**

You can download several documents within an exchange at once; you can even download all the documents in several folders on the exchange at the same time if you like. The process is similar to downloading a single document.

**To download multiple documents**

1. In the Documents List, highlight the documents and/or the folders whose contents you want to download. You can select multiple documents and folders at the same time by pressing the SHIFT or CTRL key while clicking the items to highlight them.
2. Click the Download button at the top of the screen. A message asking you whether you want to open or save the document appears. Click Save.
3. Choose a location on your local drive for the documents, and click OK.

If you download a file that may contain malicious content, a message will appear to warn you of the risk and give you the option not to continue with the download. The warning is based upon the type of file that you selected, not the actual content of the file. The message does not appear for file types that are commonly used by Intralinks’ clients.

This message will appear if you select any file with one of the following extensions: *.ade; *.adp; *.asd; *.asf; *.asx; *.bas; *.bat; *.chm; *.cil; *.class; *.cmd; *.com; *.cpl; *.crt; *.dat; *.dll; *.exe; *.hcp; *.hlp; *.hta; *.ht; *.htm; *.html;
Bulk downloading documents from multiple exchanges

Using Download Wizard, you can download all the contents of one or more exchanges, the contents of selected folders, and individual files.

Note that some documents or attachments may have protections applied to them that will prevent you from downloading or printing them. You may be required to view protected documents or attachments in the Intralinks environment only.

In order for you to download items from an exchange, the **allow bulk downloading of documents** option on the exchange's **settings** screen must be marked.

**Note:** If you are using a Macintosh computer, or a Windows browser other than Internet Explorer, you may need to use an alternative version of Download Wizard. If Download Wizard does not appear when you perform step 1 below, select **Compatibility Download** from the Tools menu, then repeat the procedure below. Note that with this version of the Download Wizard you cannot print or view documents. Click the gear icon 🛠️ that appears below the search box to display the Tools menu.

▶ **To download documents using Download Wizard**

If the **Hub** is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select **Hub** from the list that appears.

1. Click the **Download** button at the top of the screen
2. If you have not run Download Wizard previously, a message appears asking whether you want to run Download Wizard, which is a separate application. Click **Run**.
3. Download Wizard's **Select Items** view appears. Click the **Show all exchanges** button to display a list of the exchanges to which you have access.
4. Using the **Available** list, locate the items you want to download. Either double-click an exchange's name or click the plus-sign (+) icon to the left of it to view the contents of the exchange. You can view the contents of folders within the exchange in the same way.
5. When you have located an item (exchange, folder or document) that you want to download, highlight it and click the **Add** button. The individual documents that you selected appear in the **Target** list. Continue selecting items until you have selected all the items that you want to download.
6. Click **Next**. The **Locations & Settings** view of the wizard appears.
7. Select the location on your computer or network where the items will be downloaded. Also select options for organizing and processing files, along with advanced options.
8. Click **Next**. The **Download** view of the wizard appears.
9. Review your selections. Highlight an exchange to see all the documents that will be downloaded from it. Click the Back button to make any needed changes.

10. Click the Start button to begin downloading the items to the selected location. As items are downloaded, information about them is displayed. You can halt the download if necessary by clicking the Stop button.

If you download a file that may contain malicious content, a message will appear to warn you of the risk and give you the option not to continue with the download. The warning is based upon the type of file that you selected, not the actual content of the file. The message does not appear for file types that are commonly used by Intralinks’ clients.


11. Once the items have been downloaded, you can choose to print the documents and view a download log, which shows detailed information about items you downloaded, including their title and extension, status (completed, failed to be downloaded, completed with warnings), the date and time each item was downloaded, their location on the exchange and on your computer or network, and error messages if the items could not be downloaded or was downloaded with a warning. (For example, the document's name was modified because another document with the same name already exists in the selected location.) If effective dates were entered for your documents, these dates appear on the log, as well.

To print the documents, click Print These Documents. The Bulk Print Documents window appears. Review the documents displayed; to remove a document from the list, highlight it and then click Remove Selected. When you have finished reviewing the list, click Print.

To view the Download Log, click Open Download Log.

12. Click Close.

Printing documents

Note that security settings for individual documents may prevent you from printing some of the documents that you select.

▶ To print a document

1. Locate the document in the Documents List, and click on it to highlight it.

2. From the More Actions menu, select Print Document. The Print dialog box appears.

3. Review the options in the dialog box, and click OK.

▶ To print all the currently displayed documents

You can use the following steps to print all the documents that appear in the Documents List.
1. From the More Actions menu, select Print Documents in This View. A Print screen appears listing all the documents on the exchange, along with details about the document, such as the file type and number of pages.

2. Review the documents in the list. To remove a document from the list, highlight it and click Remove Selected.

3. When you are satisfied with the contents of the list, click Print to begin printing.

To print all the documents on the exchange

The Documents tab should be displayed.

1. From the More Actions menu, select Print All Documents. A Print screen appears listing all the documents on the exchange, along with details about the document, such as the file type and number of pages.

2. Review the documents in the list. To remove a document from the list, highlight it and click Remove Selected.

3. When you are satisfied with the contents of the list, click Print to begin printing.

Working with protected documents

What is document locking and protection?

Document locking and protection — also known as Information Rights Management, or IRM — provides an added level of security for documents in PDF or Microsoft Office (Word, Excel and PowerPoint) format. Exchange managers may have a variety of reasons for protecting documents, but generally, document protection is applied to documents that contain sensitive or confidential information that should not be shared with people who have not been given permission to view it.

With document locking and protection, users are either:

- Prevented from downloading documents from an exchange to their computer or network, or
- Required to enter their email address and Intralinks password before opening a downloaded copy of the document, which is encrypted.

The document format and browser that the individual is using determines whether the file can be downloaded or must be viewed online.

Exchange managers and publishers can determine whether protection will be applied to individual documents. In addition, exchange managers and publishers can prevent users from printing protected documents.

Protected documents can be identified in the Documents List by a lock icon that appears to the left of the document name. If the document is protected and printing is not allowed, a printer icon appears with a red X on top of it.

For more information, see Chapter 6, Protecting documents, on page 93.
Performing ad hoc analysis using IRM-protected Excel documents

If you have been permissioned to use Microsoft Excel documents protected, you can perform a limited number of actions that will allow you to perform ad hoc analysis. You cannot save the changes that you make.

You can perform the following tasks:

- Resize cells
- Edit cell values
- Add columns and rows
- Sort data

You cannot perform the following actions:

- Create pivot tables
- Create graphs
- Save changes using either the Save or Save As command
- Copy protected files’ contents
- Print protected documents, if the Protect/No Print option has been selected for them

You can manipulate data only in Microsoft Excel documents. No changes can be made to other protected document types.

You can perform ad hoc analysis on documents created using Microsoft Excel 2007 or later (Windows) or Excel 2011 or later (Macintosh). Analysis can be performed using documents that are protected using either the Protect or Protect/No Print option.

Viewing PDF and Microsoft Office documents using Intralinks Viewer

Depending upon how an exchange is set up, you may be able to view PDF documents and Microsoft Excel and Word files using Intralinks Viewer.

**Note:** Intralinks Viewer is not available on all exchanges and may not be available to you. If you are an exchange manager and want to use Intralinks Viewer with your exchange, contact Intralinks for assistance. To learn more about Intralinks Viewer, see “Enabling Intralinks Viewer” on page 25.

Intralinks Viewer is an alternative to Adobe Reader and similar tools.

As you use Intralinks Viewer, you will find many of the functions that are found in Adobe Reader and other PDF viewers, including search, zoom and navigation tools. Functions that cannot be used with protected PDFs, such as text touchup and commenting, are not available.

Depending upon how Intralinks Viewer has been set up on your exchange, you may be allowed to use Intralinks Viewer only for documents that have printing or downloading restrictions, or for all PDF, Excel and Word documents on the exchange. If Intralinks Viewer is not used for unprotected files, they are displayed...
in your Internet browser, Excel, Word or Adobe Reader or Acrobat, depending upon how your Adobe software is set up.

Using Intralinks Viewer

Adobe Flash Player 9 or a later version must be installed on your computer in order for you to use Intralinks Viewer. No additional software is required.

Using the Curtain
If the Disallow use of Print Screen exchange setting is enabled, a “curtain” appears over documents, obscuring the text, when you first display the documents in Intralinks Viewer. The curtain prevents others from reading text on your screen. To view the document, click the message that appears in the middle of the screen and press the ENTER key until the document is displayed. The curtain reappears if you select another document or application.

If the Disallow use of Print Screen exchange setting is enabled and you attempt to make images of your screen while a document is visible in the Intralinks Viewer window, the message Data Protection Policy Applied will appear when you attempt to paste the screen image. You can use the print screen key when Intralinks Viewer is in the background and the curtain is displayed, however. (Only the curtain, and not the document’s contents, will be displayed.)

Using the Spotlight
Intralinks Viewer’s Spotlight function allows only a few lines of text to be displayed at once. You can use the Spotlight to limit the amount of text that is displayed, preventing unauthorized people from viewing the document as you read it in public areas such as airports. You can resize the Spotlight if you like. To use the Spotlight, click the Spotlight icon at the top of the Intralinks Viewer screen. To resize the Spotlight, adjust the slider tool that appears to the right of the Spotlight icon.

Navigating through documents
You can view documents using the scroll bar on the right side of the Intralinks Viewer screen or the tools that appear in the bar at the top of the screen. You also can use the toolbar at the top of the screen (shown below) to zoom in, zoom out, reset the zoom to 100%, search for particular words or phrases, display the next or previous page using arrow buttons, or go to a specific page in the document.

![Intralinks Viewer toolbar](image)

If you are viewing a PDF document with bookmarks, you can click the bookmarks icon to display the document’s bookmarks. If the PDF document includes documents, click the attachments icon to display a list of attachments. Similarly, click the comments icon to view any comments that have been added to the document. (These icons do not appear if the PDF document does not include these items.)

Printing documents
You can print documents that appear in Intralinks Viewer. (Protected documents for which the Prevent print option has been selected cannot be printed, of course.)
To print a document, click the printer icon on the upper left side of the Intralinks Viewer screen:

When you print a PDF document, a box appears allowing you to select a range of pages to print. After you have made your selection, click Print to display a Print dialog box, where you can select the printer that you want to use.

When you print an Excel spreadsheet, a box appears allowing you to print the current worksheet, another worksheet, if the document includes multiple worksheets, or the entire workbook (all the worksheets in your document). After you have made your selection, click Print to display a Print dialog box, where you can select the printer that you want to use.

**Using the PRINT SCREEN key**

You cannot make images of your screen while a document is visible in the Intralinks Viewer window. If you attempt to do so, the message *Data Protection Policy Applied* will appear when you attempt to paste the screen image. You can use the PRINT SCREEN key when Intralinks Viewer is in the background and the curtain is displayed, however. (Only the curtain, and not the document’s contents, will be displayed.)
Chapter 9: Managing standard and rules-based business processes

Overview

In this chapter you will learn about Intralinks’ business processes and how they can be used to create controlled document submission and review workflows. You also will learn how to:

• Create, configure and activate business processes
• Inactivate and reactivate business processes
• Delete business processes in draft stage
• Rename business processes
• Copy business processes from one exchange to another

Before you begin

In order to perform the tasks in this chapter, Adobe Flash Player 9 must be installed on your computer.

When you select an exchange in the Hub, a message will appear if Flash Player 9 is not installed. This message includes links to information about the Flash Player software and to a location on the Adobe website where you can download this free software utility. Your organization’s IT department may be required to install this software for you.

If Flash Player 9 is not installed, you can open the exchange, but you will be able to perform only basic reviewer-related tasks like reading and printing documents.

What are business processes?

Business processes are predefined interactions that are designed to control the flow of documents and ensure that they are handled in a consistent way. These interaction can be as simple as the submission of a weekly progress report or as complex as a document review requiring multiple levels of approval.

Business processes serve as templates from which exchange users can create business process instances — the actual requests for approval or for documents. Intralinks provides several types of business processes (known as business process definitions) for you to use. You can choose from three types of business processes — standard, rules based and multi-task.

Standard processes can be set up quickly and are ideal for situations where you know the people and documents involved. Rules-based processes require a bit more setup effort, but they offer great flexibility in selecting documents, users and groups — even those that do not exist yet. Rules can be based on a variety of information about the users, groups and documents, including the entries that have been made for them in custom fields. (This information is referred to as metadata.)
Multi-task processes combine elements of standard and rules-based processes and can be used to manage and coordinate many tasks related to a single activity. For information about multi-task processes, see Chapter 10, *Managing multi-task processes*, on page 146.

All business processes are set up using wizards.

Standard processes include:

- Document date trigger
- Document submission for approval
- Document submission with two-step approval
- Document submission (without any approval)
- Document submission for review
- Request for documents

Rules-based processes include:

- Group-triggered document distribution
- Rules-based document distribution
- Rules-based submission

Business processes can be created only by those with the Manager Plus exchange role. Users with any exchange role can be task initiators (submitters or requestors of documents) or document reviewers.

**Standard processes**

**Document date trigger**
In this standard business process, alerts will be sent to specified exchange members based on dates associated with documents. For example, this process can be used to alert you if the expiration date for a license or contract is approaching. The steps used to create a document date trigger process are slightly different from those used for other standard processes, since no documents are being submitted or distributed.

To create a business process of this type, see “Setting up a document date trigger process” on page 124.

**Document submission for approval**
In this standard business process, a submitter sends a document to a reviewer, who can:

- Accept the document
- Reject the document
- Request that it be resubmitted with changes

If the document is accepted or rejected, no further action is required; the business process instance is considered complete.
To create a business process of this type, see “Creating and configuring standard business processes” on page 121.

**Document submission with two-step approval**
This standard business process is a bit more complex, but is fundamentally the same as the document submission for approval. In it, a submitter sends a document to an initial reviewer who can accept or reject the document or request that it be resubmitted. If the initial reviewer accepts the document, it is submitted to a second reviewer, who also can accept or reject the document or request that it be resubmitted. If either reviewer rejects the document, or if the second reviewer accepts it, the process is considered complete.

To create a business process of this type, see “Creating and configuring standard business processes” on page 121.

**Document submission (without any approval)**
This is the simplest and most straightforward of the standard business processes. In it, the submitter sends a document to a reviewer, who reviews the document and then marks the task complete. No further communication with the submitter is required once the document has been sent to the reviewer.

To create a business process of this type, see “Creating and configuring standard business processes” on page 121.

**Document submission for review**
In this standard business process, a submitter sends a document to a reviewer, who can:

- Review the document
- Request that it be resubmitted

The reviewer can request that the document be resubmitted if more information is needed or can mark the process as done if the submitter has provided all the information that was needed. This process is similar to the request for documents business process, which is explained below.

To create a business process of this type, see “Creating and configuring standard business processes” on page 121.

**Request for documents**
This standard business process is initiated by a reviewer who requests a document from a submitter. The reviewer can request that the document be resubmitted if more information is needed or can mark the process is done if the submitter has provided all the information that was needed.

To create a business process of this type, see “Creating and configuring standard business processes” on page 121.

**Rules-based processes**

**Group-triggered document distribution**
This rules-based business process is similar to the rules-based document distribution process, but documents are automatically distributed to new and updated groups if they match the criteria in the rules you set. Once a group-
triggered document distribution business process is created and configured, no additional human intervention is required to distribute the documents identified by the business process. After the documents have been distributed, other tasks, such as response acknowledgments and approvals, must be completed by users.

To create a business process of this type, see “Creating and configuring a group-triggered document distribution business process” on page 138.

Rules-based document distribution
This highly configurable business process allows you to automate document distribution processes based on predefined rules that you establish. Using rules, you can identify the documents that will be distributed, the groups that will receive them, and different handling instructions for particular documents and groups. You can require that users acknowledge receipt of the documents and that they complete documents associated with the process. You can auto-publish the attachments to users’ acknowledgments, again using rules that will determine which documents will be published, the location on your exchange where they will be published, the documents’ recipients, their permissions for using the documents, and the contents of email alerts sent to the recipients of newly published documents.

To create a business process of this type, see “Creating and configuring a rules-base document distribution business process” on page 133.

Rules-based submission
This business process allows you to standardize and automate document submission processes based on predefined rules that you establish. As with the rules-based document distribution business process, this process is highly configurable. You can determine who will view submitted documents, who will approve them, and whether they will be auto-published.

To create a business process of this type, see “Creating and configuring a rules-based submission business process” on page 127.

Setting up standard business processes

**Note:** This section applies only to standard business processes. For information about group-triggered document distribution, rules-based document distribution and rules-based submission, see “Setting up rules-based business processes” on page 127. To create a document date trigger process, see “Setting up a document date trigger process” on page 124.

You can configure standard business processes using a series of multi-step wizards. The steps include:

- Selecting the exchanges to which the business process applies
- Selecting the exchange users who will be able to view the process
- Selecting task initiators — the people who are responsible for creating and routing documents, or who are requesting documents
- Selecting task recipients — the people responsible for receiving and approving (or rejecting) documents, or who are responsible for providing documents that have been requested
• Selecting task details

You can save your configurations as drafts before making them active. If changes are needed, they can be made during the draft stage.

Business processes can have one of the following statuses:

• **Draft** — The business process has been saved as a draft, but is not considered ready for use. It is not activated. Draft templates are visible only to the person who created them; once they are made active, templates are visible to all users with the Manager Plus exchange role. Once activated, a template cannot be returned to draft status.

• **Active** — The business process is ready for use, but no one has used it yet — no business process instances have been created from it.

• **In Use** — The business process is active and has been used; one or more business process instances have been created from it.

• **Inactive** — The business process has been made unavailable for creating future business process instances. Any instances already in process are not affected if a business process is made inactive. Inactive business processes can be reactivated.

About submitters, reviewers and approvers

*Submitters provide documents to reviewers and approvers.* Except for requests for information, submitters initiate business process instances. (That is, the submitters begin the process by submitting a document for review or approval.) You can select one or more individuals, the members of a user group or all the exchange members with a particular exchange role (such as Reviewer) to be submitters.

When you select reviewers and submitters for a business process, you can select one or more individuals, the members of a collaboration group, or all the exchange members with a particular exchange role (such as Manager) for these tasks.

Creating and configuring standard business processes

**Note:** This section applies only to standard business processes. For information about group-triggered document distribution, rules-based document distribution and rules-based submission, see “Setting up rules-based business processes” on page 127.

You must be assigned the Manager Plus exchange role in order to create business processes.

When you create a business process, it is created in Draft mode. This allows you to make changes before making the process available to exchange users. When you are ready for users to begin performing the tasks associated with the new process, activate the process. For more information, see “Activating business processes” on page 143.

Note that you can change the users who are assigned to a business process at any time, but only future business process instances will be affected. Any users
assigned to existing business process instances will be allowed to complete them even if they are removed from the list of users assigned to the process.

▶ To create a standard business process

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the Maintenance button to display a list of maintenance tasks. A list of the business processes created for the exchanges that you manage also appears.

2. From the Action menu, select Add Business Process. The Select Process Definition screen appears.

3. Highlight the type of business process that you want to create:
   - Document submission
   - Document submission for approval
   - Document submission with two-step approval
   - Document submission for review
   - Request for document

   Each of these options is described in detail in the previous section, "What are business processes?"

4. Click Next. The Select Exchange view appears.

Naming the business process and associating it with an exchange

1. Enter a name for the business process. Be sure the name clearly identifies the process for the people who will be using it.

2. Highlight the exchange in which the business process will be used.

3. Click Next. The Make Available to Users view appears.

Determining who will be able to see, and use, this business process

Use the Make Available to Users screen to create the rules that will determine which exchange users will be allowed to create business process instances from this business process.

1. To begin creating a new rule, click the Add Visibility button in the lower right corner of the screen. The fields needed to create a new rule are displayed.

2. Enter a name for the rule.

3. Indicate how you want users to be selected using this rule.

   - Groups — Select this option if you want to give access to this business process to specific groups that may not share common attributes. A list of groups on your exchange appears; highlight the groups that you want and click the arrow button (>) to move the groups to the Selected Groups list. To select multiple groups, press the SHIFT or CTRL key while clicking the groups' names.
Role Group — Select this option if you want to give access to this business process to all users who are assigned a particular exchange role, such as Reviewer. You can select multiple roles if you like.

Users — Select this option if you want to give access to this business process to specific people. You can select as many individuals as you like.

Group Metadata — Select this option if all the groups you want to select share a common attribute, such as the country in which they are located. A number of custom fields will appear, allowing you to identify the attributes that the groups have in common. All the groups that match the criteria that you set will have access to this business process.

4. To create another rule, click the Add Visibility button again. You can create as many rules as you like. This business process will be available to anyone who meets the criteria of one or more rules.

5. When you have finished creating rules, click Next. The Cancel Business Process Instances screen appears.

Allowing users to cancel the business process instances that they have created

1. If users who create (initiate) a business process instance will be allowed to cancel the instances they have created, mark the Users can cancel business process instances option.

2. Click Next. The Enter Instructions screen appears.

Entering instructions for business process initiators (optional)

1. You can add a note to provide any additional instructions that will appear on the email alert sent to document submitters.

2. You can attach additional instructions or other documents to the email alert sent to document submitters.

   To attach a document that is located on your computer or a network drive, click Attach new document. A dialog box appears allowing you to select the files that you want.

   To attach a document that is located on your exchange, click Add linked documents. A pane appears, allowing you to select the file to be attached. Highlight the documents that you want and then click Attach. To select multiple documents, press the SHIFT or CTRL key while clicking the documents’ names.

3. Click Next. Depending upon the type of business process you are creating, Select Reviewers, Select Approvers, Select Submitters or Select Approver 1 screen appears. The steps that you will follow are the same regardless of the process selected.

Selecting document reviewers, approvers or submitters

1. Enter a note to provide any additional instructions that you want to appear for the document reviewers, approvers or submitters.

2. You can attach additional instructions or other documents to the email alert sent to document reviewers, approvers and submitters.
To attach a document that is located on your computer or a network drive, click **Attach new document**. A dialog box appears allowing you to select the files that you want.

To attach a document that is located on your exchange, click **Add linked documents**. A pane appears, allowing you to select the file to be attached. Highlight the documents that you want and then click **Attach**. To select multiple documents, press the SHIFT or CTRL key while clicking the documents’ names.

1. Click **Add Rule**. The fields needed to create a new rule are displayed.
2. Enter a name for the rule.
3. Indicate how you want users to be selected using this rule.
   - **Groups** — Use this option if you want to select specific groups that may not share common attributes. A list of groups on your exchange appears; highlight the groups that you want and click the arrow button (>) to move the groups to the **Selected Groups** list. To select multiple groups, press the SHIFT or CTRL key while clicking the groups’ names.
   - **Role Group** — Use this option if you want to select all users who are assigned a particular exchange role, such as Manager Plus. You can select multiple roles if you like.
   - **Users** — Use this option if you want to select specific people. You can select as many individuals as you like.
   - **Group Metadata** — Use this option if all the groups you want to select share a common attribute, such as the country in which they are located. A number of custom fields will appear, allowing you to identify the attributes that the groups have in common. All the groups that match the criteria that you set will be selected.
4. To create another rule, click the **Add rule** button again. You can create as many rules as you like. This business process will be available to anyone who meets the criteria of one or more rules.
5. If you are creating a Document Submission with Two-Step Approval business process, click **Next** and repeat steps 1 through 4 to select the individuals or groups that are responsible for the second level of approval.
6. Click **Save** to save your changes and close the screen.

When you are ready for users to begin performing the tasks associated with this process, activate the process. For more information, see “Activating business processes” on page 143.

### Setting up a document date trigger process

As noted earlier, document date trigger processes can be used to send email alerts to selected exchange members when certain date criteria are met. For example, you can use this process to alert managers when contracts or licenses are about to expire.

**To create a document date trigger process**

If the **Hub** is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select **Hub** from the list that appears.
1. Click the **Maintenance** button to display a list of maintenance tasks. A list of the business processes created for the exchanges that you manage also appears.

2. From the **Action** menu, select **Add Business Process**. The **Select Process Definition** screen appears.

3. Highlight **Document Date Trigger**.

4. Click **Next**. The **Select Exchange** view appears.

**Naming the business process and associate it with an exchange**

1. Enter a name for the business process. Be sure the name clearly identifies the process for the people who will be using it.

2. Highlight the exchange in which the business process will be used.

3. Click **Next**. The **Event Criteria** view appears.

**Selecting event criteria**

Use event criteria to determine when, and how often, email alerts will be sent when this process is triggered.

1. Indicate when you want the business process to be triggered:
   - On a specified number of days before the trigger date
   - On the trigger date itself
   - On a specified number of days after the trigger date.

   The initial alert will be sent on this date.

2. If you want more than one alert to be sent, indicate the frequency with which the alerts should be sent, and the period of time in which they should be sent.

   For example, if you use the default selections, an alert will be sent once every 7 days for 28 days. In this case alert recipients will receive a total of five alerts (the original alert and a repeating alert once a week for the next four weeks).

   Click **Next**. The **Event Trigger** view is displayed.

**Creating event triggers**

Use the **Event Trigger** screen to create the rules for specific documents that will determine when email alert is required for these documents.

1. To begin creating a new rule, click the **New Event Trigger** button in the lower right corner of the screen. The fields needed to create a new rule are displayed.

2. Enter a name for the rule.

3. Enter the name of the document for which this rule applies.

4. (Optional.) Enter a range of dates for which this rule is effective.

5. Click the **Identify Date Field** button. A panel appears displaying the date fields that can be used as triggers.

6. Select the date field that you want to use as a trigger, and then click the x icon to hide the date fields panel.
7. If you want to create another event trigger, click **Create** additional trigger and repeat steps 2 through 6.

8. When you have finished creating triggers, click **Next**. The **Select Alert Recipients** view appears.

**Determining who will receive email alerts for this business process**

Use the **Select Alert Recipients** screen to create the rules that will be used to select the people who will be allowed to submit documents using this business process.

1. To begin creating a new rule, click the **Add Rule** button in the lower right corner of the screen. The fields needed to create a new rule are displayed.

2. Enter a name for the rule.

3. Indicate how you want users to be selected using this rule.
   - **Group Name** — Select this option if you want to email alerts to be sent to specific groups that may not share common attributes. A list of groups on your exchange appears; highlight the groups that you want and click the arrow button (>) to move the groups to the **Selected Groups** list. To select multiple groups, press the **SHIFT** or **CTRL** key while clicking the groups’ names.
   - **User** — Select this option if you want email alerts to be sent to specific people. You can select as many individuals as you like.
   - **Group Metadata** — Select this option if all the groups you want to select share a common attribute, such as the country in which they are located. A number of custom fields will appear, allowing you to identify the attributes that the groups have in common. All the groups that match the criteria that you set will have access to this business process.

4. To create another rule, click the **Add Rule** button again. You can create as many rules as you like. Alerts will be sent to anyone who meets the criteria of one or more rules.

5. When you have finished creating rules, click **Next**. The **Alert Details** screen appears.

**Configuring email alerts that will be sent to document recipients**

The **Enter Alert Details** step should be displayed.

1. In the **Subject** field, enter the text that you want to appear in the subject line for the email alerts.

2. In the **Note** field, enter a note that will appear in the body of the email alerts.

   **Important!** Do not enter more than 2,500 characters in this field! Although you may be allowed to enter a larger number of characters, the alerts may not be sent if the note exceeds 2,500 characters.

3. From the **Include Custom Fields** field, indicate whether you want for custom fields to be displayed on the alerts.

**Saving your changes**

◊ Once you are satisfied with your configuration selections, click **Save**.
Setting up rules-based business processes

**Note:** This section applies only to rules-based business processes. For information about standard business processes, see “Setting up standard business processes” on page 120.

You must be assigned the Manager Plus exchange role in order to create business processes.

Rules-based business processes provide greater flexibility in selecting both documents and recipients than similar standard business processes do. They also enable you to automatically publish recipients’ response documents and give permission to user groups to view the documents. Configuration rules can be based on a number of criteria, including custom fields (metadata) assigned to documents and groups.

You can create rules-based submission processes. You also can create two types of document distribution processes: the rules-based document distribution process and the group-triggered document distribution business process. Both processes are similar in that they enable you to automate the document distribution process and to set up rules for selecting the documents to be distributed and the groups that will receive them. You can require that users acknowledge receipt of the documents and that they complete documents associated with the process. You can auto-publish the attachments to users’ acknowledgments, again using rules to automate the process and to govern who will be given access to the documents.

Creating and configuring a rules-based submission business process

Rules-based business processes can be created and configured using a single multi-step wizard. Most configuration steps are optional, and they can be performed in any order.

Note that you can change the users who are assigned to a business process at any time, but only future business process instances will be affected. Any users assigned to existing business process instances will be allowed to complete them even if they are removed from the list of users assigned to the process.

**To create a rules-based submission business process**

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the Maintenance button to display a list of maintenance tasks. A list of the business processes created for the exchanges that you manage also appears.

2. From the Action menu, select Add Business Process. The Select Process Definition screen appears.


4. Enter a name for the business process. be sure the name clearly identifies the process for the people who will be using it.
5. Highlight the exchange in which the distributed documents will be stored.

If you manage many exchanges, you can use the filters to display a shorter list of exchanges. You can filter the list by exchange name and ID, the name of the exchange host, and the exchange’s phase (hold, preparation or open). You can make entries in two or more of the filter fields if you like.

6. Click **Next**.

**Defining the functions that submitters will be allowed to perform**

Using this screen, set up a business process for submitting documents. Your selections here will determine the functions that users will be allowed, or required, to perform when they submit documents using this process.

1. Begin by indicating whether users can submit documents of any type using this process, or whether they will be limited to a specific document type.

   If you select **Select Document Type from Dropdown**, select one or more document types from the list below the field. To select multiple items, press the **CTRL** key while clicking the items.

2. Indicate which of the following options apply to this business process:

   - **Is working set execution allowed?** — Select **Yes** if submitters who have created working sets (personal collections of exchanges that are related to one another in some way) will be allowed to use those working sets to submit documents to the exchange that you are currently accessing.

   - **Approval required?** — Select **Yes** if submitted documents must be approved by an exchange manager before they are published to the current exchange.

   - **Allow approvers to attach documents?** — Select **Yes** if document approvers are allowed to attach additional instructions or other documents to a submission when they request that a document be resubmitted. This option is available only if you marked the **Approval required?** option.

   - **Autopublishing allowed?** — Select **Yes** if documents will be automatically published to a predefined location on your exchange. Autopublished documents can be made available to users based on rules that you specify. Rules also can be used to limit these users’ permissions to the documents. If approval is required, the documents will not be published until they have been approved.

   - **Fax In** — Mark this option if users will be able to submit their documents via fax.

3. Click **Next**. The **Instructions** screen should be displayed. (This screen is optional; if you do not wish to provide response instructions, click **Next** again and skip to the next procedure.)

**Entering instructions for submitters**

1. In the **Note** field, provide any additional instructions that you want to appear on the email alert sent to document recipients.
2. To attach additional instructions or other documents, click Add attachment(s). A pane appears, allowing you to select the file to be attached.

To attach a document that is located on your computer or a network drive, click Attach new document. A dialog box appears allowing you to select the files that you want.

To attach a document that is located on your exchange, click Add linked documents. A pane appears, allowing you to select the file to be attached. Highlight the documents that you want and then click Attach. To select multiple documents, press the SHIFT or CTRL key while clicking the documents’ names.

You can attach multiple files if you like. You can attach files from the exchange or your computer or network drive.

Note: If you use eForms, be sure to attach only one eForm to each submission.


Determining who will be able to see, and use, this business process

Use the Add Visibility Configuration Rules screen to create the rules that will be used to select the people who will be allowed to submit documents using this business process.

1. In the Collaboration Group Access field, mark the Full control option to indicate that members of the submitter’s collaboration group are allowed to act as co-monitors if a document approver requests that documents be resubmitted. If you mark the View Only option, other members of the user’s collaboration group will be able to view documents submitted by the user, but only the user will be able to respond to requests for resubmission. Select No Access if you do not want members of the submitter’s collaboration group to see the documents at all.

2. To begin creating a new rule, click the Create New Rule button in the lower right corner of the screen. The fields needed to create a new rule are displayed.

3. Enter a name for the rule.

4. Indicate how you want users to be selected using this rule.

   • Group Name — Select this option if you want to give access to this business process to specific groups that may not share common attributes. A list of groups on your exchange appears; highlight the groups that you want and click the arrow button (>) to move the groups to the Selected Groups list. To select multiple groups, press the SHIFT or CTRL key while clicking the groups’ names.

   • Role Group — Select this option if you want to give access to this business process to all users who are assigned a particular exchange role, such as Reviewer. You can select multiple roles if you like.

   • User — Select this option if you want to give access to this business process to specific people. You can select as many individuals as you like.

   • Group Metadata — Select this option if all the groups you want to select share a common attribute, such as the country in which they are located.
A number of custom fields will appear, allowing you to identify the attributes that the groups have in common. All the groups that match the criteria that you set will have access to this business process.

5. To create another rule, click the Create New Rule button again. You can create as many rules as you like. This business process will be available to anyone who meets the criteria of one or more rules.

6. When you have finished creating rules, click Next. The Respond by Date screen appears.

**Setting a response date**

This screen is optional. You can require document recipients to acknowledge response of the documents within a set number of days. If you do not want to set a response period, click Next and skip to the next procedure.

1. In the Number of days to respond after document is received field, enter the number of days within which recipients are expected to respond.

2. Using the Send daily alert and Send alert once options, indicate the number of times that you want reminders to be sent to recipients who have not responded within the required number of days.

3. Click Next.

*If you selected “Yes” for the Approval Required field:*

The Add Submission Approver Rules screen should be displayed.

Use this step to create the rules that will be used to select the people who will approve recipients’ submission responses.

If you indicated that approval is required, your process must include at least one submission approver rule. You can create as many rules as you like. If you create multiple rules, anyone who meets the criteria of one or more rules will be allowed to approve recipients’ responses.

You can designate any of the following to be approvers:

- Individual users
- All users with specific exchange roles (for example, the manager plus role)
- Selected groups
- Groups that share a common attribute, such as the country in which they are located, or title

1. Click the Create a new rule button in the lower right corner of the screen. The fields needed to create the rule are displayed.

2. Enter a name for the rule.

3. If you want specific people or groups, or people with specific exchange roles to be approvers, select one of the following options:

   - **Collaboration Group** — Select this option if you want specific groups that may not share common attributes to be approvers. A list of groups on your exchange appears; highlight the groups that you want and click the
arrow button (>) to move the groups to the Selected Groups list. To select multiple groups, press the SHIFT or CTRL key while clicking the groups’ names.

- **Role Group** — Select this option if you want to all users who are assigned a particular exchange role, such as Manager Plus, to be approvers. You can select multiple roles if you like.

- **Users** — Select this option if you want specific individuals to be approvers. You can select as many individuals as you like.

4. If all the groups you want to select share a common attribute, such as their group type, click the **Add Group Metadata Rule** button. A number of custom fields will appear, allowing you to identify the attributes that the groups have in common. All the groups that match the criteria that you set will be selected as submission approvers.

   Click **Add Group Metadata Rule** to create another rule.

5. Click **Next** when you have finished creating submission approver rules.

*If you selected Yes for the Auto-Publishing Allowed field:*

The **Auto Publish Configuration** screen should be displayed.

You can set rules to allow users other than exchange managers to view these attachments. You also must select a location on your exchange where the attachments will be published.

1. Click **Next**. The **Response Publishing Folder** screen appears, displaying a list of the folders on your exchange.

2. Either highlight the folder where you want submission response attachments to be published, or opt to have a new folder created for each response. You can include the submitter’s name, or the name of the submitter’s group in the folder name, along with text that identifies the files that will be posted. For example, you could select **User Name**, then enter text before the user name to create a folder named “Quarterly Report — Terry Lee” when user Terry Lee submitted a report using this business process. If you choose to create folders, they will appear at the top level of your exchange’s Folders List.

3. Click **Next**. The **Published Document Recipients** screen appears.

4. If other members of the submitter’s collaboration group (typically coworkers at the same worksite) should be able to view submitted documents, mark the **Allow the submitter’s collaboration group to view the document** option. (If the submitter does not belong to any groups, the attachment will not be visible to him.)

5. Click the **Create a new rule** button in the lower right corner of the screen. The fields needed to create the rule are displayed.

6. Enter a name for the rule.

7. Select one of the following options:

   - **Group Name** — Select this option if you want to make documents available to specific groups that may not share common attributes. A list of groups on your exchange appears; highlight the groups that you want and click the arrow button (>) to move the groups to the Selected Groups list.
list. To select multiple groups, press the SHIFT or CTRL key while clicking the groups’ names.

- **Group Metadata** — Select this option if all the groups you want to select share a common attribute, such as the country in which they are located. A number of custom fields will appear, allowing you to identify the attributes that the groups have in common. All the groups that match the criteria that you set will receive the documents that are distributed.

8. Your changes are saved automatically. Click **Create a new rule** to create another rule, or **Next** if you have finished creating recipient rules.

**Setting levels of protection for auto-published documents**

The **Published Document Permissions** screen should be displayed.

You can use the fields on this screen to control how users will be able to use documents that are made available to them.

1. Using the **Permissions** field, indicate whether selected groups will be able to make changes to the field.

   If users will be allowed only to view the documents, select **See**. If they will be able to make changes to the document or delete it, select **Control**. Members of these groups will be able to modify the document only if their exchange roles (for example, manager or publisher) allow them to do so.

2. For each group, select one of the following options from the **Protection** list:
   - **Do not protect**
   - **Protect**
   - **Protect/No Print**

   With document protections, you can prevent users from downloading copies of the documents or require them to enter their email address and password before viewing a downloaded copy of the documents. You also can prevent users from printing the documents.

   The type of browser, browser version, and browser settings determine whether the document can be downloaded, or must be viewed on the exchange. For detailed information about document protections, see Chapter 6, **Protecting documents**, on page 93.

3. Click **Next**.

**Configuring email alerts that will be sent to document recipients**

The **Published Document Alert Configuration** step should be displayed.

1. In the **Subject** field, enter the text that you want to appear in the subject line for the email alerts.

2. In the **Note** field, enter a note that will appear in the body of the email alerts.

3. From the **Include Custom Fields** field, indicate whether you want for custom fields to be displayed on the alerts.
Saving your changes

◊ Once you are satisfied with your configuration selections, click Save.

Creating and configuring a rules-base document distribution business process

Rules-based document distribution business processes are useful for automatically distributing new documents to a preconfigured group of recipients.

You can configure your processes to require that recipients acknowledge receipt of distributed documents, and set up an approval process for recipients’ acknowledgment responses. You can require that recipients respond with a form or document in a predetermined format. Rules can be set up for automatically publishing files attached to acknowledgment responses.

Group-triggered document distribution business processes can be used to automatically distribute documents to newly added or updated groups that meet specified criteria. For information on creating a business process of this type, see “Creating and configuring a group-triggered document distribution business process” on page 138.

Rules-based business processes can be created and configured using a single multi-step wizard. Most configuration steps are optional, and they can be performed in any order.

Note that you can change the users who are assigned to a business process at any time, but only future business process instances will be affected. Any users assigned to existing business process instances will be allowed to complete them even if they are removed from the list of users assigned to the process.

To create a rules-based document distribution business process

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the Maintenance button to display a list of maintenance tasks. A list of the business processes created for the exchanges that you manage also appears.

2. From the Action menu, select Add Business Process. The Select Process Definition screen appears.


4. Enter a name for the business process. be sure the name clearly identifies the process for the people who will be using it.

5. Highlight the exchange in which the distributed documents will be stored.

   If you manage many exchanges, you can use the filters to display a shorter list of exchanges. You can filter the list by exchange name and ID, the name of the exchange host, and the exchange’s phase. You can make entries in two or more of the filter fields if you like.

Creating the rules that identify documents to be distributed

The Document Metadata Rules step should be displayed.

1. Click Create a new rule. The fields needed to create the rule appear.
   Your process must include at least one document selection rule. You can create as many rules as you like.

2. Enter the following information:
   - **Rule Name** – Enter a descriptive name for the rule.
   - **Document Name** – If this rule will be used to select documents that have a particular name, enter that name here.
   - **Effective Date (From) and Effective Date (To)** – If you want to use this rule to select documents that are effective during a particular time frame, specify the range of dates here. If you leave these fields blank, all documents that meet other criteria will be selected, regardless of the effective dates that may be assigned to them.

   Additional custom fields that are based on the market segment selected for this exchange also may be displayed. Review these fields and make any selections that are needed to create your rule.

   Only the documents that match all the criteria that you specify will be distributed.

3. Your changes are saved automatically. Click Create a new rule to create another rule, or Next if you have finished creating document selection rules.

Creating the rules that will identify the documents’ recipients

The Document Recipients step should be displayed.

1. Click the Create a new rule button in the lower right corner of the screen. The fields needed to create the rule are displayed.
   Your process must include at least one permission rule. You can create as many rules as you like. If you create multiple rules, any group that meets the criteria of one or more rules will be given access to the documents that are distributed using this business process.

2. Enter a name for the rule.

3. From the Select recipients using field, select one of the following options:
   - **Collaboration Group** — Select this option if you want to distribute documents to specific groups that may not share common attributes. A list of groups on your exchange appears; highlight the groups that you want and click the arrow button (> ) to move the groups to the Selected Groups list. To select multiple groups, press the SHIFT or CTRL key while clicking the groups’ names.
   - **Group Metadata** — Select this option if all the groups you want to select share a common attribute, such as the country in which they are located. A number of custom fields will appear, allowing you to identify the attributes that the groups have in common. All the groups that match the criteria that you set will receive the documents that are distributed.
4. Your changes are saved automatically. Click **Create a new rule** to create another rule, or **Next** if you have finished creating recipient rules.

**Setting levels of protection for distributed documents**

The **Permissions & Protections** step should be displayed.

You can use the fields on this screen to control how users will be able to use documents that are distributed to them.

1. Using the **Permissions** field, indicate whether selected groups will be able to make changes to the field.
   
   If users will be allowed only to view the documents, select **See**. If they will be able to make changes to the document or delete it, select **Control**. Members of these groups will be able to modify the document only if their exchange roles (for example, manager or publisher) allow them to do so.

2. For each group, select one of the following options from the **Protection** list:
   - **Do not protect**
   - **Protect**
   - **Protect/No Print**

   With document protections, you can prevent users from downloading copies of the documents or require them to enter their email address and password before viewing a downloaded copy of the documents. You also can prevent users from printing the documents.

   The type of browser, browser version, and browser settings determine whether the document can be downloaded, or must be viewed on the exchange. For detailed information about document protections, see Chapter 6, *Protecting documents*, on page 93.

3. Click **Next**.

**Configuring email alerts that will be sent to document recipients**

The **Document Alert Configuration** step should be displayed.

1. In the **Subject** field, enter the text that you want to appear in the subject line for the email alerts.

2. (Optional.) In the **Note** field, enter a note that will appear in the body of the email alerts.

3. (Optional.) Using the **Include Custom Fields** field, indicate whether you want for custom fields to be displayed on the alerts.

4. If you do not want permissioned groups to receive an email notification when documents are distributed to them using this business process, mark the **Disable Notification** option.

5. Click **Next**.

**Configuring acknowledgment responses**

The **Response Configuration** step should be displayed.
Use this step to determine whether recipients will be required to acknowledge that they have received documents after they have been distributed. You can attach a form to your document distributions and require that recipients complete and return the form.

If you require that recipients submit a response form, you also can require approval of the form and assign auto-publishing rules to the form. Both of these functions are optional. (If you require approval, the response must be approved before the form will be published.)

**Note:** If you use eForms, be sure to attach only one eForm to each distribution.

Additional setup is required for each of the options for which you select **Yes**. You can set these options up on subsequent screens in this wizard.

If you select **No** for all the options on this screen, documents will be distributed to recipients and no further follow-up will be required.

Click **Next** to display the next screen in the configuration process.

*If you selected Yes for the Response Form Required field:*

The **Respond by Date** screen should be displayed. (This screen is optional; if you do not wish to set a due date, skip to step 6.)

1. (Optional.) In the **Number of days to respond after document is received** field, enter the number of days within which recipients are expected to respond.

2. Using the **Send daily alert** and **Send alert once** options, indicate the number of times that you want reminders to be sent to recipients who have not responded within the required number of days.

3. Click **Next**. The **Instructions** screen should be displayed. (This screen is optional; if you do not wish to provide response instructions, skip to step 6.)

4. In the **Note** field, provide any additional instructions that you want to appear on the email alert sent to document recipients.

5. To attach additional instructions or other documents, click **Add attachment(s)**. A pane appears, allowing you to select the file to be attached. You can attach multiple files if you like. You can attach files from the exchange or your computer or network drive.

6. Click **Next**.

*If you selected Yes for the Approval Required field:*

The **Response Approvers** screen should be displayed.

Use this step to create the rules that will be used to select the people who will approve recipients’ acknowledgment responses.

Your process must include at least one rule. You can create as many rules as you like. If you create multiple rules, anyone who meets the criteria of one or more rules will be allowed to approve recipients’ responses.

You can designate any of the following to be approvers:
• Individual users
• All users with specific exchange roles (for example, the manager plus role)
• Selected groups
• Groups that share a common attribute, such as the country in which they are located, or title

1. Enter a name for the rule.

2. If you want specific people or groups, or people with specific exchange roles to be approvers, select one of the following options:

• **Collaboration Group** — Select this option if you want specific groups that may not share common attributes to be approvers. A list of groups on your exchange appears; highlight the groups that you want and click the arrow button (>) to move the groups to the Selected Groups list. To select multiple groups, press the SHIFT or CTRL key while clicking the groups’ names.

• **Role Group** — Select this option if you want to all users who are assigned a particular exchange role, such as Manager Plus, to be approvers. You can select multiple roles if you like.

• **Users** — Select this option if you want specific individuals to be approvers. You can select as many individuals as you like.

3. If all the groups you want to select share a common attribute, such as their group type, click the **Add Group Metadata Rule** button. A number of custom fields will appear, allowing you to identify the attributes that the groups have in common. All the groups that match the criteria that you set will be selected as submission approvers.

   Click **Add Group Metadata Rule** to create another rule.

4. Click **Next** when you have finished creating response approver rules.

*If you selected “Yes” for the Auto-Publishing Allowed field:*

The **Auto Publish Configuration** screen should be displayed.

You can set rules to allow users other than exchange managers to view these attachments. You also must select a location on your exchange where the attachments will be published.

1. Click **Next**. The **Response Publishing Folder** screen appears, displaying a list of the folders on your exchange.

2. Highlight the folder where you want acknowledgment response attachments to be published, and click **Next**. The **Recipient** screen appears.

3. If other members of the submitter’s collaboration group (typically coworkers at the same worksite) should be able to view submitted documents, mark the **Allow the submitter’s collaboration group to view the document** option. (If the submitter does not belong to any groups, the attachment will not be visible to him.)

4. Click the **Create a new rule** button in the lower right corner of the screen.
Your process must include at least one permission rule. You can create as many rules as you like. If you create multiple rules, any group that meets the criteria of one or more rules will be given access to acknowledgment response attachments.

5. Create rules following the same steps that you used previously for determining who would receive distributed documents.

6. The remaining steps for configuring acknowledgement responses are the same as those you used earlier for distribution of documents. Repeat the steps that you performed earlier.

When you are ready for users to begin performing the tasks associated with this process, activate the process. For more information, see “Activating business processes” on page 143.

Creating and configuring a group-triggered document distribution business process

Group-triggered document distribution business processes are useful for automatically distributing existing documents to newly added or updated collaboration groups that match specified criteria. You can configure your processes to require that recipients acknowledge receipt of distributed documents, and set up an approval process for recipients’ acknowledgment responses. You can required that recipients respond with a form or document in a predetermined format. Rules can be set up for automatically publishing files attached to acknowledgment responses.

Note that only collaboration groups can be used for document distribution and approval. If your exchange uses other types of groups, they will be ignored even if they otherwise match the criteria of one of your rules.

Rules-based document distribution business processes can be used to automatically distribute new documents to existing groups. For information on creating a business process of this type, see “Creating and configuring a rules-base document distribution business process” on page 133.

Rules-based business processes can be created and configured using a single multi-step wizard. Most configuration steps are optional, and they can be performed in any order.

Note that you can change the users who are assigned to a business process at any time, but only future business process instances will be affected. Any users assigned to existing business process instances will be allowed to complete them even if they are removed from the list of users assigned to the process.

To create a group-triggered document distribution business process

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the Maintenance button to display a list of maintenance tasks. A list of the business processes created for the exchanges that you manage also appears.
2. From the Action menu, select Add Business Process. The Select Process Definition screen appears.


4. Enter a name for the business process. Be sure the name clearly identifies the process for the people who will be using it.

5. Highlight the exchange in which the distributed documents will be stored.
   If you manage many exchanges, you can use the filters to display a shorter list of exchanges. You can filter the list by exchange name and ID, the name of the exchange host, and the exchange’s phase. You can make entries in two or more of the filter fields if you like.

6. Click Next.

Creating the rules that will identify the documents’ recipients

The Group Metadata Rules step should be displayed.

1. Click the Create a new rule button in the lower right corner of the screen. The fields needed to create the rule are displayed.
   Your process must include at least one permission rule. You can create as many rules as you like. If you create multiple rules, any collaboration group that meets the criteria of one or more rules will be given access to the documents that are distributed using this business process.

2. Enter a name for the rule.

3. A number of custom fields are displayed, allowing you to identify the attributes that the collaboration groups have in common. All the collaboration groups that match the criteria that you set will receive the documents that are distributed.

4. Your changes are saved automatically. Click Create a new rule to create another rule, or Next if you have finished creating recipient rules. Any collaboration group that matches the criteria set for one or more rules will receive documents distributed through this business process.

Creating the rules that identify documents to be distributed

The Document Metadata Rules step should be displayed.

1. Click Create a new rule. The fields needed to create the rule appear.
   Your process must include at least one document selection rule. You can create as many rules as you like.

2. Enter the following information:
   • Rule Name – Enter a descriptive name for the rule.
   • Document Name – If this rule will be used to select documents that have a particular name, enter that name here.
   • Effective Date (From) and Effective Date (To) – If you want to use this rule to select documents that are effective during a particular time frame, specify the range of dates here. If you leave these fields blank, all
documents that meet other criteria will be selected, regardless of the effective dates that may be assigned to them.

Additional custom fields that are based on the market segment selected for this exchange also may be displayed. Review these fields and make any selections that are needed to create your rule.

Only the documents that match all the criteria that you specify will be distributed.

3. Your changes are saved automatically. Click Create a new rule to create another rule, or Next if you have finished creating document selection rules.

Setting levels of protection for distributed documents

The Permissions & Protections step should be displayed.

You can use the fields on this screen to control how users will be able to use documents that are distributed to them.

1. Using the Permissions field, indicate whether selected collaboration groups will be able to make changes to the field.

   If users will be allowed only to view the documents, select See. If they will be able to make changes to the document or delete it, select Control. Members of these groups will be able to modify the document only if their exchange roles (for example, manager or publisher) allow them to do so.

2. For each group, select one of the following options from the Protection list:
   
   - Do not protect
   - Protect
   - Protect/No Print

   With document protections, you can prevent users from downloading copies of the documents or require them to enter their email address and password before viewing a downloaded copy of the documents. You also can prevent users from printing the documents.

   The type of browser, browser version, and browser settings determine whether the document can be downloaded, or must be viewed on the exchange. For detailed information about document protections, see Chapter 6, Protecting documents, on page 93.

3. Click Next.

Configuring email alerts that will be sent to document recipients

The Document Alert Configuration step should be displayed.

1. In the Subject field, enter the text that you want to appear in the subject line for the email alerts.

2. (Optional.) In the Note field, enter a note that will appear in the body of the email alerts.

3. (Optional.) From the Include Custom Fields field, indicate whether you want for custom fields to be displayed on the alerts.
4. If you do not want permissioned groups to receive an email notification when documents are distributed to them using this business process, mark the Disable Notification option.

5. Click Next.

Configuring acknowledgment responses

The Response Configuration step should be displayed.

Use this step to determine whether recipients will be required to acknowledge that they have received documents after they have been distributed. You can attach a form to your document distributions and require that recipients complete and return the form.

If you require that recipients submit a response form, you also can require approval of the form and assign auto-publishing rules to the form. Both of these functions are optional. (If you require approval, the response must be approved before the form will be published.)

Additional setup is required for each of the options for which you select Yes. You can set these options up on subsequent screens in this wizard.

If you select No for all the options on this screen, documents will be distributed to recipients and no further follow-up will be required.

Click Next to display the next screen in the configuration process.

If you selected “Yes” for the Response Required field:

The Respond by Date screen should be displayed. (This screen is optional; if you do not wish to set a due date, skip to step 6.)

1. (Optional.) In the Number of days to respond after document is received field, enter the number of days within which recipients are expected to respond.

2. Using the Send daily alert and Send alert once options, indicate the number of times that you want reminders to be sent to recipients who have not responded within the required number of days.

3. Click Next. The Instructions screen should be displayed. (This screen is optional; if you do not wish to provide response instructions, skip to step 6.)

4. In the Note field, provide any additional instructions that you want to appear on the email alert sent to document recipients.

5. To attach additional instructions or other documents, click Add attachment(s). A pane appears, allowing you to select the file to be attached. You can attach files from the exchange or your computer or network drive. You can attach multiple files if you like.

6. Click Next.

If you selected “Yes” for the Approval Required field:

The Response Approvers screen should be displayed.

Use this step to create the rules that will be used to select the people who will approve recipients’ acknowledgment responses.
Your process must include at least one rule. You can create as many rules as you like. If you create multiple rules, anyone who meets the criteria of one or more rules will be allowed to approve recipients' responses.

You can designate any of the following to be approvers:

- Individual users
- All users with specific exchange roles (for example, the manager plus role)
- Selected groups
- Groups that share a common attribute, such as the country in which they are located, or title

1. Click the Create a new rule button in the lower right corner of the screen. The fields needed to create the rule are displayed.
2. Enter a name for the rule.
3. If you want specific people or groups, or people with specific exchange roles to be approvers, select one of the following options:
   - Collaboration Group — Select this option if you want specific groups that may not share common attributes to be approvers. A list of groups on your exchange appears; highlight the groups that you want and click the arrow button (>) to move the groups to the Selected Groups list. To select multiple groups, press the SHIFT or CTRL key while clicking the groups’ names.
   - Role Group — Select this option if you want to all users who are assigned a particular exchange role, such as Manager Plus, to be approvers. You can select multiple roles if you like
   - Users — Select this option if you want specific individuals to be approvers. You can select as many individuals as you like.
4. If all the groups you want to select share a common attribute, such as their group type, click the Select Approvers by Group Metadata button. A number of custom fields will appear, allowing you to identify the attributes that the groups have in common. All the groups that match the criteria that you set will be selected as submission approvers.
5. Your changes are saved automatically. Click Create a new rule to create another rule, or Next if you have finished creating response approver rules.

If you selected “Yes” for the Auto-Publishing Allowed field:

The Auto Publish Configuration screen should be displayed.

You can set rules to allow users other than exchange managers to view these attachments. You also must select a location on your exchange where the attachments will be published.

1. Click Next. The Response Publishing Folder screen appears, displaying a list of the folders on your exchange.
2. Highlight the folder where you want acknowledgment response attachments to be published, and click Next. The Recipient screen appears.
3. If other members of the submitter’s collaboration group (typically coworkers at the same worksite) should be able to view submitted documents, mark the **Allow the submitter’s collaboration group to view the document** option. (If the submitter does not belong to any groups, the attachment will not be visible to him.)

4. Click the **Create a new rule** button in the lower right corner of the screen.
   
   Your process must include at least one permission rule. You can create as many rules as you like. If you create multiple rules, any group that meets the criteria of one or more rules will be given access to acknowledgment response attachments.

5. Create rules following the same steps that you used previously for determining who would receive distributed documents.

6. The remaining steps for configuring acknowledgement responses are the same as those you used earlier for distribution of documents. Repeat the steps that you performed earlier.

When you are ready for users to begin performing the tasks associated with this process, activate the process. For more information, see “Activating business processes” on page 143.

### Activating business processes

When you create a new business process, it is created in draft mode. This allows you to review the process configuration and make any needed changes before the process becomes available to the users who are responsible for performing the tasks associated with the process. When you are ready for users to begin performing tasks, **activate** the process.

**To activate a business process**

The **Hub** should be displayed; if it is not, click the **Hub** button in the upper left corner of the screen.

1. Click the **Maintenance** button on the left side of the screen. A list of the business processes created for the exchanges that you manage should be displayed; if it is not, click the **Business Process** button.

2. Highlight the business process that you want to activate.

3. From the **Action** menu, select **Activate Business Process**.

The process is activated and is ready for use by all the users who are assigned to it. It also becomes visible to all users with the Manager Plus role.

### Inactivating, reactivating and deleting business processes

If you create a business process and then discover that you do not need it before it has been activated, you can delete. Once the process is activated, you cannot inactivate it, but you cannot delete it. Users will be able to complete business process instances that were created while the business process was active, but they will not be able to create new business process instances unless you reactivate the business process.

You can make changes to inactive processes; these changes will be applied to any business process instances that are already underway.
To inactivate a business process

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the Maintenance button. A list of the business processes created for the exchanges that you manage appears.
2. Highlight the business process that you want to inactivate.
3. From the Action menu, select Deactivate Business Process.

The process is inactivated. The users who are assigned to the process no longer can create new business process instances using this business process, but they can complete any business process instances that are already underway.

To reactivate a business process

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the Maintenance button. A list of the business processes created for the exchanges that you manage appears.
2. Highlight the business process that you want to reactivate.
3. From the Action menu, select Reactivate Business Process.

The process is reactivated and becomes available to all the users who are assigned to it.

To delete a business process

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the Maintenance button. A list of the business processes created for the exchanges that you manage appears.
2. Highlight the business process that you want to delete. Remember, only draft business processes can be deleted. Once a process has been activated, it can be inactivated, but it cannot be deleted.
3. From the Action menu, select Delete Business Process.
4. A message appears asking you to confirm your selection. Type yes and then click the Yes button.

The process is deleted.

Renaming a business process

To rename a business process

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the Maintenance button. A list of the business processes created for the exchanges that you manage appears.
2. Highlight the business process that you want to rename.
4. Enter the new name for the business process in the Enter new name field.
5. Click Rename.

Copying a business process

You can copy business processes to other exchanges, as long as the exchanges were created using the same template.

► To copy a business process

If the Hub is not already displayed, roll your mouse over the exchange name in upper left corner of the screen and select Hub from the list that appears.

1. Click the Maintenance button. A list of the business processes created for the exchanges that you manage appears.
2. Highlight the business process that you want to copy.
4. Mark the Activate the copy of the business process option if you want the process to be immediately available in the new exchange.
5. Highlight the exchange where the business process is to be copied.
6. Click Copy Business Process.
Chapter 10: Managing multi-task processes

Overview

In this chapter you will learn about Intralinks Platform’s multi-task business processes and how they can be used to manage and track the progress of complex activities involving many related tasks.

You also will learn how to:

- Create, configure and activate multi-task processes
- Inactivate and reactivate multi-task processes
- Delete multi-task processes in draft stage
- Rename multi-task processes
- Making changes to multi-task processes
- Managing processes and the tasks associated with them

Before you begin

In order to perform the tasks in this chapter, Adobe Flash Player 9 must be installed on your computer.

When you select an Intralinks Platform exchange in the Intralinks Hub, a message will appear if Flash Player 9 is not installed. This message includes links to information about the Flash Player software and to a location on the Adobe website where you can download this free software utility. Your organization’s IT department may be required to install this software for you.

If Flash Player 9 is not installed, you can open the exchange, but you will be able to perform only basic reviewer-related tasks like reading and printing documents.

What are multi-task processes?

Multi-task processes combine elements of standard and rules-based processes and can be used to manage and coordinate many tasks related to a single activity. Intralinks Global Enterprise Services team members will work with your organization to create these processes to expedite your specific business processes.

Multi-task processes can be created only by those with the Manager Plus exchange role. Users with any exchange role can be task initiators (submitters or requestors of documents) or document reviewers.

Setting up multi-task business processes

Note: This section applies only to multi-task business processes. For information about standard business processes, see “Setting up standard business processes” on page 120. For information about rules-based business processes, see “Setting up rules-based business processes” on page 127.
You must be assigned the Manager Plus exchange role in order to create multi-task processes. In addition, the following exchange settings must be active for your exchange: custom fields, workflow, collaboration groups and document ownership.

Unlike other business processes, which are created at the Hub, multi-task processes are created within the exchange where they will be used.

Although you can create multi-task processes yourself, the Intralinks Global Enterprise Services team is available to configure these processes for you. A customer service representative will meet with you to understand your business needs and then create multi-task processes that are designed to improve organizational productivity and reduce the amount of time needed to execute and manage repeatable business processes.

**To configure a multi-task process**

The exchange where the process will be used should be displayed.

1. Roll your mouse over the Maintenance tab at the top of the screen. Additional options appear.
2. Select the Processes option. A list of the multi-task processes created for this exchange appears.
4. Enter a name and description for the process that you are creating, and indicate whether users will be allowed to fax in documents for the tasks associated with the process.
5. When you have made your entries, click Next. The Target view of the wizard appears.
6. Identify the collaboration groups that will be responsible for completing the tasks associated with this process. You can select specific groups, or you can select groups that share the same group attributes (for example, groups located in Canada). Attributes are identified using custom fields.

   Each process can include a combination of groups and group attributes selections.

   **To select specific groups:** From the Add Target list, select By Group Name and click Go. In the screen that appears, highlight the groups that you want to select and click the arrow button to move them to the list on the right. When you have selected all the groups you want, click Done.

   **To select groups using group attributes:** From the Add Target list, select By Group Attributes and click Go. In the screen that appears, a number of custom fields appear; using these fields select the attributes that describe the groups who will perform the tasks associated with this process. When you have selected all the groups you want, click Done.

   **Important!** Be sure that the groups you select are collaboration groups. If other group types are selected, you may not be able to publish documents that are associated with the tasks assigned to those groups, and members of these groups may be allowed to view tasks that should not be visible to them.

7. When you have made all of your selections, click Next. The Visibility view of the wizard appears.
8. Select the members of the target groups who will be able to view the process, based on the group member roles that have been assigned to them. Select the group member roles that are allowed to view the process. If no roles are selected, then all group members will be allowed to see the process.

For more information about group member roles, see “Group member roles” on page 48.

9. When you have made your entries, click Next. The Tasks view of the wizard appears.

10. If you wish to set a due date for this process (that is the date on which all tasks associated with the process are expected to be completed), use the Due Date fields to do so. Note that this due date is for all tasks, not individual tasks. If you set a due date, you will have the option in a later step to send alerts to members of the target group(s) to alert them that the process due date is pending or that the due date has passed.

You can select:

- No due date
- A due date that is a specified number of days after the process is initiated (for example, 7 days from the time the process is activated)
- A specific date

11. (Optional.) Enter a comment about, or description of, the business process. This comment is for the overall process; you can enter comments for individual tasks as you add the task. The comment will appear in the Process Monitor for all viewers.

12. Next, add a task. From the Add Task list, select one of the following options:

- Distribute Document
- Distribute Document with Confirmation
- Distribute Document with Reply
- Request Document
- Request Document from Owner
- Request Review by Owner
- Distribute Document for Edit & eSign
- Request eSignature
- To-Do

Select the task you want and click Go. A new screen will open, allowing you to set up the new task. The specific information that you need to enter will depend upon the type of task that you selected. You can create as many tasks as you like. For step-by-step instructions for creating each of these types of tasks, see “Creating tasks for a multi-task process” on page 150.

13. When you have added all the tasks that are required for this process, click Next. The Owners view of the wizard appears.

14. Select the process owners — the people who are responsible for monitoring the tasks associated with the process.
Owners have the ability to perform any of the tasks associated with the process, regardless of the group or group member role targeted to perform the tasks. This can be useful if, for example, documents are posted incorrectly. Rather than returning the documents to the target group for corrections, the owner can choose to make the corrections himself. In addition, owners can view all members of the target groups. For this reason, we recommend that you avoid selecting users who have been assigned the Reviewer, Previewer or Publisher role.

You can select specific users or groups, you can select users who have a particular exchange role (for example, Manager Plus), or you can select groups that share the same group attributes. Attributes are identified using custom fields.

Each process can include a combination of these selections.

**To select groups using group attributes:** From the Add Owner list, select **By Group Attributes** and click Go. In the screen that appears, a number of custom fields appear; using these fields select the attributes that describe the groups that will own the tasks associated with this process. When you have selected all the groups you want, click Done.

**To select specific groups:** From the Add Owner list, select **By Group Name** and click Go. In the screen that appears, highlight the groups that you want to select and press the arrow button to move them to the list on the right. When you have selected all the groups you want, click Done.

**To select individuals with a particular exchange role:** From the Add Owner list, select **By Exchange Role** and click Go. In the screen that appears, highlight the exchange role(s) that you want to select and press the arrow button to move them to the list on the right. When you have selected all the roles you want, click Done.

**To select specific individuals:** From the Add Owner list, select **By UserName** and click Go. In the screen that appears, highlight the names of the users whom you want to select and press the arrow button to move them to the list on the right. When you have selected all the names you want, click Done.

15. When you have made all of your selections, click Next. The Alerts view of the wizard appears.

16. Select the name that you wish to appear in the From: field on email alerts. Select one of the following options:

   - **Name of user initiating the process**
   - **Name of user configuring the process**
   - **Name of exchange host**
   - **Intralinks**

17. Enter the subject line and a message that will accompany the email alerts that are sent to the task’s target groups and owners. You can modify the alerts that are sent to invite users to the process, to update the process, to alert owners when the process is complete, and to warn users when a due date is approaching or past.

   If you do not want a particular alert to be sent for this process, unmark the box that appears next to the alert’s title.
Note that the Due Date Approaching and Overdue alerts are available only if you set a due date for the process on the Tasks tab.

If you choose to send alerts for updates to tasks, alert summaries will be sent to process owners and target group members roughly every 8 hours. Users will not receive a separate alert for each update. Alerts will be sent only if changes have been made to business process instances since the last alert. (Users will not receive empty alerts.) Alerts are sent regardless of a user’s preference for receiving other alerts (immediately, once daily, and so on.).

Alert summaries will provide a snapshot of the business process instances that have changed since the last alert. Only instances that had a status of Open at the time of the change are included. (Instances that had a status of Closed, Suspended or Deleted are not included.) Alert summaries are tailored to the users who receive them; only the instances that apply to a particular user will be included on the summaries that are sent to that person.

Each alert summary will include the name of the exchange being reported on, the number of business process instances that have been changed, and the time the report was created.

18. When you are satisfied with all your selections, click Save to create the process.

When you are ready for users to begin performing the tasks associated with this process, activate the process. For more information, see “Activating multi-task processes” on page 156.

Creating tasks for a multi-task process

Use the following procedures to create the tasks associated with a multi-task business process. For more information about these processes, see “Setting up multi-task business processes” on page 146.

To create a Distribute Document task

Use this task type to route documents on your exchange that do not require either approval or a response from the recipient.

1. If you have not already displayed the screen used to create this task type, do so. In the Tasks step of the Multi-Task Process Wizard, select Distribute Document from the Task List field and click Go. The Add a Document Distribution Task screen appears.

2. Enter a descriptive name for the task.

3. Attach the document that you want to distribute, or identify the document’s attributes if you want the document to be selected automatically based on those attributes. You can select only one document for each Distribute Document task.

   To select documents using document attributes: From the Attach Document list, select By Document Attributes and click Set Attributes. In the panel that appears, a number of custom fields appear; using these fields select the attributes that describe the document that is to be distributed. When you have selected all the attributes that you want, click Done.

   To select a specific document: From the Attach Document list, select By Document Name. In the panel that appears, locate and highlight the
document that you want to select. When you have selected all the groups you want, click **Done**.

4. If you want the document to be distributed to a person with a particular group member role, mark the **Target Role** option, then choose the group member role you want from the list to the left. You can select multiple roles if you like. Each selected group member role appears below the list. A separate task will be created for each person with the selected role(s).

If you do not mark the **Target Role** option, a single task will be created for all members of the target group.

5. (Optional.) Enter a comment that describes the document and the reason it is being distributed to the target group. The comment will appear in the **Process Monitor** for all viewers.

6. To create another task, select the task type from the **Add Another Task** list and click **Go**. If no more tasks are required, click **Done**.

**To create a Distribute Document with Confirmation task**

Use this task type to route documents on your exchange and require the recipients to confirm that they have received the documents.

1. If you have not already displayed the screen used to create this task type, do so. In the **Tasks** step of the Multi-Task Process Wizard, select **Distribute Document with Confirmation** from the **Task List** field and click **Go**. The **Add a Document Distribution with Confirmation Task** screen appears.

2. Enter a descriptive name for the task.

3. Attach the document that you want to distribute, or identify the document’s attributes if you want the document to be selected automatically based on those attributes. You can select only one document for each Distribute Document with Confirmation task.

   **To select documents using document attributes:** From the **Attach Document** list, select **By Document Attributes** and click **Set Attributes**. In the panel that appears, a number of custom fields appear; using these fields select the attributes that describe the document that is to be distributed. When you have selected all the attributes that you want, click **Done**.

   **To select a specific document:** From the **Attach Document** list, select **By Document Name**. In the panel that appears, locate and highlight the document that you want to select. When you have selected all the groups you want, click **Done**.

4. If you want the document to be distributed to a person with a particular group member role, mark the **Target Role** option, then choose the group member role you want from the list to the left. You can select multiple roles if you like. Each selected group member role appears below the list. A separate task will be created for each person with the selected role(s).

If you do not mark the **Target Role** option, a single task will be created for all members of the target group.

5. (Optional.) Enter a comment that describes the document and the reason it is being distributed to the target group. The comment will appear in the **Process Monitor** for all viewers.
6. To create another task, select the task type from the Add Another Task list and click Go. If no more tasks are required, click Done.

**To create a Distribute Document with Reply task**

Use this task type to route documents on your exchange and require the recipients to return documents to you in response. With this task type, separate tasks are created for distributing the original document and requesting additional documents from the tasks’ targets.

1. If you have not already displayed the screen used to create this task type, do so. In the Tasks step of the Multi-Task Process Wizard, select Distribute Document with Reply from the Task List field and click Go. The Add a Document Distribution with Reply Task screen appears.

2. Enter a descriptive name for the document distribution task.

3. Attach the document that you want to distribute, or identify the document’s attributes if you want the document to be selected automatically based on those attributes. You can select only one document for each Distribute Document with Confirmation task.

   **To select documents using document attributes:** From the Attach Document list, select By Document Attributes and click Set Attributes. In the panel that appears, a number of custom fields appear; using these fields select the attributes that describe the document that is to be distributed. When you have selected all the attributes that you want, click Done.

   **To select a specific document:** From the Attach Document list, select By Document Name. In the panel that appears, locate and highlight the document that you want to select. When you have selected all the groups you want, click Done.

4. Enter a descriptive name for the document request task.

5. Identify the attributes of the document that you want to the recipient to submit.

   Click the Set Attributes button that appears next to the Request Document by Attributes field. In the panel that appears, a number of custom fields appear; using these fields select the attributes that describe the document that the recipient is to submit. When you have selected all the attributes that you want, click Done.

6. If you want to assign the task to a person with a particular group member role, mark the Target Role option, then choose the group member role you want from the list to the left. You can select multiple roles if you like. Each selected group member role appears below the list. A separate task will be created for each person with the selected group member role(s).

   If you do not mark the Target Role option, a single task will be created for all members of the target group.

7. (Optional.) Enter a comment that describes the document and the reason it is being distributed to the target group. The comment will appear in the Process Monitor for all viewers.

8. To create another task, select the task type from the Add Another Task list and click Go. If no more tasks are required, click Done.
A single task is created for distributing the document and requesting a reply. If you discover that you need to update the document associated with this task, you can do so until a reply is sent by the target group for the task.

**To create a Request Document, Request Document from Owner, or Request Review by Owner task**

The steps that you need to follow for these task types are identical; the business process instances that will be created will vary, however, depending upon the type of task you choose to create here.

Use this task type to request documents from members of the target group.

1. If you have not already displayed the screen used to create this task type, do so. In the Tasks step of the Multi-Task Process Wizard, select Request Document from the Task List field and click Go. The Request Document, Request Document from Owner or Request Review by Owner screen appears.

2. Enter a descriptive name for the task.

3. If the document request should be assigned to a person with a particular group member role, mark the Target Role option, then choose the group member role you want from the list to the left. You can select multiple group member roles if you like. Each selected group member role appears below the list. A separate task will be created for each person with the selected role(s).

   If you do not mark the Target Role option, a single task will be created for all members of the target group.

4. (Optional.) Enter a comment that describes the document and the reason it is being requested. The comment will appear in the Process Monitor for all viewers. Click Set Attributes. A panel appears on the left side of the screen.

5. Select the type of document that you are requesting. Additional fields may appear; if they do, make entries in them, as well. When you have finished, click Done to hide the panel.

6. To create another task, select the task type from the Add Another Task list and click Go. If no more tasks are required, click Done.

**To create a Distribute Document for Edit & eSign task**

Use this task type to route forms that must be completed or documents that must be edited and then eSigned by the recipient, the initiator or both. Once the documents have been signed, they can be published.

For more information about using tasks to collect eSignatures, see “Using multi-task business processes to apply electronic signatures to documents” on page 158.

1. If you have not already displayed the screen used to create this task type, do so. In the Tasks step of the Multi-Task Process Wizard, select Distribute Document for Edit & eSign from the Task List field and click Go. The Add a Distribute Document for Edit/Sign screen appears.

2. Enter a descriptive name for the task.
3. Attach the document that you want to distribute, or identify the document’s attributes if you want the document to be selected automatically based on those attributes. You can select only one document for each task.

**To select documents using document attributes:** From the Select Document list, select By Document Attributes and click Select Attributes. In the panel that appears, a number of custom fields appear; using these fields select the attributes that describe the document that is to be distributed. When you have selected all the attributes that you want, click Done.

**To select a specific document:** From the Select Document list, select By Document Name. In the panel that appears, locate and highlight the document that you want to select. When you have selected all the groups you want, click Done.

4. Next, select the custom fields that will be applied to submitted documents.

**To select documents using document attributes:** From the Select Document list, select By Document Attributes and click Select Attributes. In the panel that appears, a number of custom fields appear; using these fields select the attributes that describe the document that is to be distributed. When you have selected all the attributes that you want, click Done.

**To select a specific document:** From the Select Document list, select By Document Name. In the panel that appears, locate and highlight the document that you want to select. When you have selected all the groups you want, click Done.

5. (Optional.) If you want the document to be distributed to a person with a particular group member role, choose the group member role you want from the Assign by Member Role list. You can select multiple roles if you like. Each selected group member role appears below the list. A separate task will be created for each person with the selected role(s).

   If you do not select any group membership roles, a single task will be created for all members of the target group.

6. Enter the number of eSignatures that are required for the document. Signatures can be required for members of the target group, members of the owner group, or both groups. You must require at least one signature from one of the groups.

7. (Optional.) Enter a comment that describes the document and the reason it is being distributed to the target group. The comment will appear in the Process Monitor for all viewers.

8. To create another task, select the task type from the Add Another Task list and click Go. If no more tasks are required, click Done.

**To create a Request eSignature task**

Use this task type to route documents on your exchange that require an eSignature from the recipient, the initiator or both. Once the documents have been signed, they can be published.

For more information about using tasks to collect eSignatures, see “Using multi-task business processes to apply electronic signatures to documents” on page 158.
1. If you have not already displayed the screen used to create this task type, do so. In the Tasks step of the Multi-Task Process Wizard, select Request eSignature from the Task List field and click Go. The Request eSignature screen appears.

2. Enter a descriptive name for the task.

3. Attach the document that you want to distribute, or identify the document’s attributes if you want the document to be selected automatically based on those attributes. You can select only one document for each Distribute Document task.

   **To select documents using document attributes:** From the Select Document list, select By Document Attributes and click Select Attributes. In the panel that appears, a number of custom fields appear; using these fields select the attributes that describe the document that is to be distributed. When you have selected all the attributes that you want, click Done.

   **To select a specific document:** From the Select Document list, select By Document Name. In the panel that appears, locate and highlight the document that you want to select. When you have selected all the groups you want, click Done.

4. Next, select the attributes by which the signed document will be selected.

   **To select documents using document attributes:** From the Select Document list, select By Document Attributes and click Select Attributes. In the panel that appears, a number of custom fields appear; using these fields select the attributes that describe the document that is to be distributed. When you have selected all the attributes that you want, click Done.

   **To select a specific document:** From the Select Document list, select By Document Name. In the panel that appears, locate and highlight the document that you want to select. When you have selected all the groups you want, click Done.

5. If you want the document to be distributed to a person with a particular group member role, choose the group member role you want from the Assign by Member Role list. You can select multiple roles if you like. Each selected group member role appears below the list. A separate task will be created for each person with the selected role(s).

   If you do not select any group membership roles (or if group membership roles are not enabled for this exchange), a single task will be created for all members of the target group.

6. Enter the number of eSignatures that are required for the document. Signatures can be required from members of the target group, members of the owner group, or both groups. You must require least one signature from one of the groups.

7. (Optional.) Enter a comment that describes the document and the reason it is being distributed to the target group. The comment will appear in the Process Monitor for all viewers.

8. To create another task, select the task type from the Add Another Task list and click Go. If no more tasks are required, click Done.

   **To create a To Do task**

   Use this task type to request documents from members of the target group.
1. If you have not already displayed the screen used to create this task type, do so. In the Tasks step of the Multi-Task Process Wizard, select To Do from the Task List field and click Go. The To Do screen appears.

2. Enter a descriptive name for the task.

3. If the task should be assigned to a person with a particular group member role, mark the Target Role option, then choose the group member role you want from the list to the left. You can select multiple group member roles if you like. Each selected group member role appears below the list. A separate task will be created for each person with the selected role(s).

   If you do not mark the Target Role option, a single task will be created for all members of the target group.

4. (Optional.) Enter a comment that describes the task in greater detail or provides instructions for completing the task. The comment will appear in the Process Monitor for all viewers.

5. To create another task, select the task type from the Add Another Task list and click Go. If no more tasks are required, click Done.

Activating multi-task processes

When you create a new business process, it is created in draft mode. This allows you to review the process configuration and make any needed changes before the process becomes available to the users who are responsible for performing the tasks associated with the process. When you are ready for users to begin performing tasks, activate the process.

To activate a multi-task process

The exchange to which the process belongs should be displayed.

1. Roll your mouse over the Maintenance tab at the top of the screen. Additional options appear.

2. Select the Processes option. A list of the multi-task processes created for this exchange appears.

3. Highlight the business process that you want to activate.

4. Click the Activate Process button.

The process is activated and is ready for use by all the users who are assigned to it. It also becomes visible to all users with the Manager Plus exchange role.

Inactivating, reactivating and deleting multi-task processes

If you create a business process and then discover that you do not need it before it has been activated, you can delete. Once the process is activated, you can inactivate it, but you cannot delete it. Users will be able to complete business process instances that were created while the business process was active, but new business process instances will not be created unless you reactivate the business process.

You can make changes to inactive processes; these changes will be applied to any business process instances that are already underway.
To inactivate a multi-task process

The exchange to which the process belongs should be displayed.

1. Roll your mouse over the Maintenance tab at the top of the screen. Additional options appear.
2. Select the Processes option. A list of the multi-task processes created for this exchange appears.
3. Highlight the business process that you want to inactivate.
4. Click the Deactivate Process button.

The process is inactivated. The users who are assigned to the process no longer can create new business process instances using this business process, but they can complete any business process instances that are already underway.

To reactivate a multi-task process

The exchange to which the process belongs should be displayed.

1. Roll your mouse over the Maintenance tab at the top of the screen. Additional options appear.
2. Select the Processes option. A list of the multi-task processes created for this exchange appears.
3. Highlight the business process that you want to reactivate.
4. Click the Activate Process button.

The process is reactivated and becomes available to all the users who are assigned to it.

To delete a multi-task process

Note: Multi-task processes that have not been activated yet can be deleted using the procedure below. Once multi-task processes have been activated and put into use, they can be deleted only if all the business process instances associated with them have been deleted first. If you do not wish to delete the business process instances that are currently in process, you can inactivate the multi-task process instead. When a multi-task process is inactivated, work can continue with existing business process instances remain, but no new instances will be created.

The exchange to which the process belongs should be displayed.

1. Roll your mouse over the Maintenance tab at the top of the screen. Additional options appear.
2. Select the Processes option. A list of the multi-task processes created for this exchange appears.
3. Highlight the business process that you want to delete. Remember, only draft business processes can be deleted. Once a process has been activated, it can be inactivated, but it cannot be deleted.
4. Click the Delete Process button.
5. A message appears asking you to confirm your selection. Type yes and then click the Yes button.

The process is deleted.
Renaming a multi-task process

**To rename a multi-task process**

The exchange to which the process belongs should be displayed.

1. Roll your mouse over the Maintenance tab at the top of the screen. Additional options appear.
2. Select the Processes option. A list of the multi-task processes created for this exchange appears.
3. Highlight the business process that you want to rename.
4. Click the Overview button.
5. The Overview tab of the Update Process window appears.
6. In the Properties section of the screen, click the Modify button. The Properties view is displayed.
7. Enter the new name for the business process in the Process Name field.
8. Click Save.

Making changes to a multi-task process

Before an active multi-task process can be updated, it must be inactivated. For instructions on inactivating processes, see “To inactivate a multi-task process” on page 157.

**To update a multi-task process**

The exchange to which the process belongs should be displayed.

1. Roll your mouse over the Maintenance tab at the top of the screen. Additional options appear.
2. Select the Processes option. A list of the multi-task processes created for this exchange appears.
3. Highlight the business process that you want to change.
4. Click the Overview button.
5. The Overview tab of the Update Process window appears, displaying a list of items that can be modified.
6. Click the Modify button for the item you want to update. The screen used to modify that item is displayed.
7. Make whatever changes are needed.
8. Click Save.
9. If you inactivated this process, reactivate it using the instructions in “To reactivate a multi-task process” on page 157.

Using multi-task business processes to apply electronic signatures to documents

You can set up multi-task business processes to collect and manage electronic signatures (eSignatures) on documents that you distribute. Users who receive
documents for signing have the option either to sign or refuse to sign the documents. If multiple signatures are required from document or form recipients, group member roles must be enabled.

Any document type can be submitted for signing; documents do not have to be in Microsoft Word or PDF format, for example. Signature pages are maintained as separate attachments to the documents.

Two task types are used to request eSignatures:

- **Distribute Document for Edit & eSign**
- **Request eSignature**

Using these task types, users can attach documents from a computer or network drive, or to select documents from an Intralinks Platform exchange based on the document’s name or attributes. The initiator can define the users who are to sign the document, along with the number of signatures required (zero or one for target groups, and zero or one for owner groups). At least one signature from either a target group member or an owner is required.

A document custom field, **eSignature State**, can be used to track a document’s progress through the eSignature process. It has two values: **Ready to be eSigned** and **eSigned**.

The task types support the distribution of both documents to be signed and forms that must be completed and then signed. Documents must be signed (or rejected) as they are presented; amended copies cannot be uploaded and then signed. Forms can be completed and then signed; if updates are needed, they can be made before the completed forms are signed. Completed forms are returned to the process initiator, who can publish them if appropriate.

Either the initiator or a member of the target group can replace a document that has been signed already; in this case, the signatures are invalidated, and the document must be signed again.

Multi-task business processes can be configured to allow users to select a reason for signing the document. By default the reason provided will be “Approved.” Users who refuse to sign (reject) a document will be provided with a comment field to allow them to provide an explanation for their action. For example, a user might note that the document contains errors and cannot be signed until the errors are corrected.

Two actions help process owners to manage eSignature tasks. **Restart** allows process owners to return eSignature tasks to their original state. This action is similar to the **Resubmit** action for other business processes. **Accept** can be used to return a task in its current state to the owner’s control even if the required number of signatures has not been obtained. The **Restart** and **Accept** actions can be selected at any point in the eSignature cycle; if one of these actions is selected, all previous actions are undone, but a record of the actions is retained in the task’s history. The process owner will be warned about the implications of their selection.

Documents can be published at any time, regardless of whether the required number of signatures has been obtained. The process owner will be warned if a document does not have the required number of signatures.
Process owners can track the progress of signature tasks using the **Last Interaction** column on the **Process List** screen.

Once a signed document has been published, any user who has permission to access the document can print a page with eSignature information for the document. Use the **View & Print eSignature** command on the document **Actions** menu to enable this. The signature page displays the name and organization of each signatory, the action they took (signed or refused to sign), the reason for their action, and the time it was made.

Documents are assigned a unique ID that allows users to match signatures to a specific version of a document. A new ID will be assigned to the document if its contents change. The ID will not be updated if the document’s metadata (custom field selections) are updated.

Process owners can search their exchanges for documents based on their eSignature status (eSigned or Ready to be eSigned).

A report listing all the eSigned documents on a particular exchange, along with detailed history for each document is available to users who are preparing for an audit. Users must request the report from Intralinks customer service.

If documents are copied, eSignature information is not copied with them. eSignature information is not affected if documents are moved. eSignature information also is not affected if a signed document is deleted from an exchange for which the **Save deleted documents** exchange setting is enabled.

**Electronic signatures are Title 21 CFR Part 11 compliant**

The following features have been implemented to ensure that eSignatures are Title 21 CFR Part 11 compliant:

- The ability to view eSignature information for specific documents
- The ability to print eSignature information for each version of a specific document using a unique signature code
- Audit support via a report that lists documents associated with eSignature tasks
- The ability for users to search for documents that have been signed
- The ability for users to search for documents that are waiting to be signed

To ensure full compliance, your organization may have to implement additional procedures. For example, you may need to perform some measure of physical validation that the person you have assigned a particular user ID (email address) to is in fact the same person specified in your organization’s Human Resources records.
Chapter 11: Completing tasks that are assigned to you

Overview

In this chapter you will learn how to:

- View tasks that are assigned to you
- Submit documents for review or approval
- Approve and reject documents, and ask for them to be resubmitted
- Request information
- Add co-monitors
- Rename a business process instance
- Cancel tasks
- Add comments to tasks
- Use the Process Monitor screen to manage processes and the tasks associated with them

Before you begin

In order to perform the tasks in this chapter, Adobe Flash Player 9 must be installed on your computer.

When you select an exchange in the Hub, a message will appear if Flash Player 9 is not installed. This message includes links to information about the Flash Player software and to a location on the Adobe website where you can download this free software utility. Your organization’s IT department may be required to install this software for you.

If Flash Player 9 is not installed, you can open the exchange, but you will be able to perform only basic reviewer-related tasks like reading and printing documents.

Business processes serve as templates from which exchange users can create business process instances — the actual requests for approval or for documents. Intralinks provides several types of business processes — standard, rules based and multi-task.

Standard processes can be set up quickly and are used in situations where both the people and documents involved are known. Rules-based processes require a bit more setup effort, but they offer great flexibility in selecting documents, users and groups — even those that do not exist yet. Rules can be based on a variety of information about the users, groups and documents, including the entries that have been made for them in custom fields. (This information is referred to as metadata.)

Multi-task processes combine elements of standard and rules-based processes and can be used to manage and coordinate many tasks related to a single activity.
Standard processes include:

- Document date trigger
- Document submission for approval
- Document submission with two-step approval
- Document submission (without any approval)
- Document submission for review
- Request for documents

Rules-based processes include:

- Group-triggered document distribution
- Rules-based document distribution
- Rules-based submission

Using standard and rules-based business processes

Viewing tasks that are assigned to you

When tasks are assigned to you, an email alert containing a link to the task is sent to you. You also can view a list of tasks that are assigned to you, as well as those that you have assigned or submitted to other people, within Intralinks.

**Note:** If you use the **Tasks** list within an exchange, you will view only tasks that are associated with a multi-task process. Tasks associated with other business processes can be viewed only on the **Hub**.

The **Tasks** list displays current tasks that still need to be completed.

*To view all tasks that are assigned to you, or by you*

You should be viewing the **Hub**.

1. In the navigation pane on the left side of the screen, click the **Tasks** option. Additional options appear.
2. Click the **By Task Name** option. A list of tasks that are assigned to you and that you have assigned to others (if your exchange role allows this).
3. To view tasks assigned to you, click the **Open tasks assigned to me** option in the **Saved Searches** box that appears to the right of the navigation pane.

To view tasks that you have assigned to others, click the **Open tasks assigned by me** option in the **Saved Searches** box.

Submitting documents

Use the following procedure to create a standard business process instance and use it to submit documents to reviewers or approvers.
Note that you can create business process instances only for business processes to which you have been assigned. If you have not been identified as a submitter for any business processes, you will not be to perform this procedure.

**To submit a document**

You should be viewing the exchange where the document will be submitted.

1. Click the **Tasks** tab at the top of the screen.
2. From the **Actions** menu, select **New To Do or Submission**. The **Select Business Process** wizard appears.
3. Highlight the business process you want to use, and click **Continue**. The **Instructions** view of the wizard for your business process instance appears.
4. Review the instructions and any attached documents, then click **Next**. The **Submission** view of the wizard appears.
5. In the **Process Instance** field, enter a descriptive name for the task.
6. Enter other notes to explain the purpose of the submission.
7. Attach the document(s) that will be submitted. You can attach a document from the exchange or your computer or network. (If necessary, you can select documents from both the exchange and your computer or network.)

   To attach a document on the exchange, click the **Attach Link** button. A pane appears showing the folders on your exchange. Locate the document you want and highlight it, then click the **Attach** button that appears above the folder list. You can select as many documents as needed. When you have finished selecting documents, click the **x** button above the **Attach** button to close the selection pane.

   To attach a document on your computer or a network drive, click the **Attach Document** button. A **Select file(s) to upload** dialog box appears, allowing you to select the document you want.

   To select multiple items, press the **SHIFT** or **CTRL** key while clicking the items to highlight them.

8. You may be required to enter additional details, such as the type of document that you are submitting. If this is the case, a new screen with a number of additional fields appears. Make an entry in each field that applies to the document.

9. Click **Save**.

   A task will appear in the **Tasks** list for the person who is supposed to receive your document, and an email alert will be sent to the person, alerting him or her that your document has been submitted.

**Faxing in documents**

Depending upon the way your exchange is set up, you may be able to fax document into the exchange for some business processes. In order to do this, you must print a cover sheet that will be used to direct your document to the correct exchange.

**To create a fax-in cover sheet**

You should be viewing the exchange where the document will be submitted.
The **Tasks** tab should be selected.

1. From the **Actions** menu, select **Create a Fax Cover Sheet**. The **Select Business Process** view of the **Fax in Cover Sheet** screen is displayed.

2. Highlight the business process that you want, and click **Next**. The **Create Cover Sheet** view is displayed.

   **Note:** If the business process that you want does not appear in the list, the exchange manager does not allow you to fax documents to it. You must submit your document online using the previous procedure.

3. Enter a title and note that will appear on the cover sheet.

4. Click **Create Cover Sheet**.

Fax the document, including the cover sheet, to the phone number that appears on the cover sheet. The documents and notes are uploaded to Intralinks, and the exchange manager is alerted.

### Resubmitting documents

The managers of your exchange may have set up an approval process for document submissions. If your submission is reviewed and additional information is required, you may receive an email asking you to resubmit your documents with changes. A new task also will appear in the **By Task Name** view of your **Tasks** list. The process for resubmitting documents is very similar to the process that you used to submit the original documents.

#### To review a document that does not require approval

You should be viewing the exchange where the document will be submitted.

The **Tasks** tab should be selected.

1. In the **Tasks** list, highlight the task.

2. From the **Actions** menu, select **View Details**. The **Submission Request** view of the task wizard appears, displaying any notes and supporting documents that the reviewer or approver provided to explain the changes that you are required to make.

3. After you have reviewed the instructions, click **Next**. The **Response** view of the task wizard appears.

4. Enter any notes that you wish to include in the **Submission Instructions** field.

5. Attach the document(s) that will be submitted. You can attach a document from the exchange or your computer or network. (If necessary, you can select documents from both the exchange and your computer or network.)

   To attach a document on the exchange, click the **Attach Link** button. A pane appears showing the folders on your exchange. Locate the document you want and highlight it, then click the **Attach** button that appears above the folder list. You can select as many documents as needed. When you have finished selecting documents, click the **x** button above the **Attach** button to close the selection pane.

   To attach a document on your computer or a network drive, click the **Attach Document** button. A **Select file(s) to upload** dialog box appears, allowing you to select the document you want.
To select multiple items, press the SHIFT or CTRL key while clicking the items to highlight them.

6. When you have selected all the documents that you wish to submit, click **Save**.

A task will appear in the approver’s **Tasks** list, and an email alert will be sent to the person, alerting him or her that your document has been resubmitted.

Reviewing and approving documents that have been submitted to you

Use the following steps to respond to a document submission. Depending upon the type of business process that the task is based upon, you may be able to approve or reject the submission, return it to the submitter and request a resubmission, or simply mark the task as done.

**To review a document**

You should be viewing the Hub. If you have opened the task wizard using the link in the email alert that was sent to you, skip to step 6.

1. In the navigation pane on the left side of the screen, click the **Tasks** option. Additional options appear.

2. Click the **By Task Name** option. A list of tasks that are assigned to you and that you have assigned to others (if your exchange role allows this).

3. Click the **Open tasks assigned to me** option in the Saved Searches box that appears to the right of the navigation pane.

4. Locate the task that you want to view.

5. From the Actions menu, select **View Details**. The Submission view of the task wizard appears.

6. Read any notes provided by the person who submitted the document, then read the document. You can open documents by double-clicking them.

7. When you have finished viewing the document, return to the task wizard and click **Next**. The Response view of the wizard appears.

8. Review the instructions and reference documents, if any, that have been provided for you.

9. (Optional.) Enter a note. If the document is being returned to the submitter (you are asking for it to be resubmitted with changes, for example), use the note to provide the submitter with information about any changes that are needed.

10. (Optional.) You can attach a document from the exchange or your computer or network. (If necessary, you can select documents from both the exchange and your computer or network.)

   To attach a document on the exchange, click the Attach Link button. A pane appears showing the folders on your exchange. Locate the document you want and highlight it, then click the **Attach** button that appears above the folder list. You can select as many documents as needed. When you have finished selecting documents, click the **x** button above the **Attach** button to close the selection pane.
To attach a document on your computer or a network drive, click the **Attach Document** button. A **Select file(s) to upload** dialog box appears, allowing you to select the document you want.

To select multiple items, press the **SHIFT** or **CTRL** key while clicking the items to highlight them.

11. From the **Status** field, select an action. The selections available to you vary depending upon the type of business process that was used to create this task.

   - **Done** — The task will be marked as **Done** in the **Tasks** list, and no further steps are required. When you view it in the **Tasks** list in the future, only the history view will appear, showing the actions taken by you and the submitter.

   - **Reviewed** — The task will be marked as **Reviewed** in the **Tasks** list, and no further steps are required. When you view it in the **Tasks** list in the future, only the history view will appear, showing the actions taken by you and the submitter.

   - **Approve** — If the Document Submission with Approval business process was originally used to create this task, the task will be marked as **Approved** in the **Tasks** list, and no further steps are required. If the Document Submission with Two-Step Approval business process was used to create this task, the task will be marked as **Pending Approval 2** in the **Tasks** list, and it will be transferred to the second approver. When you view it in the **Tasks** list in the future, only the history view will appear, showing the actions taken by you and the submitter. (Note, however, that if the second reviewer rejects a document that you have approved, you will be asked to approve the resubmitted document.)

   - **Reject** — The task will be marked as **Rejected** in the **Tasks** list, and no further steps are required. When you view it in the **Tasks** list in the future, only the history view will appear, showing the actions taken by you and the submitter.

   - **Resubmit** — The task will be returned to the submitter’s **Tasks** list. Its status in the **Tasks** list is **Pending Resubmission** until the submitter responds.

12. Click **Save**.

### Requesting a document

The process for requesting a document is very similar to the one used for submitting documents.

#### To request a document

You should be viewing the exchange where the document will be submitted.

The **Tasks** tab should be selected.

1. From the **Actions** menu, select **New To Do or Submission**. The **Select Business Process** wizard appears.
2. Highlight the business process you want to use, and click **Continue**. The **Instructions** view of the wizard for your business process instance appears.

3. Review the instructions and any attached documents, then click **Next**. The **Select Submitters** view of the wizard appears.

4. In the **Process Instance** field, enter a descriptive name for the task.

5. Enter other notes to explain the purpose of your request.

6. (Optional.) Attach document(s) that further explain your request. You can attach a document from the exchange or your computer or network. (If necessary, you can select documents from both the exchange and your computer or network.)

   To attach a document on the exchange, click the **Attach Link** button. A pane appears showing the folders on your exchange. Locate the document you want and highlight it, then click the **Attach** button that appears above the folder list. You can select as many documents as needed. When you have finished selecting documents, click the **x** button above the **Attach** button to close the selection pane.

   To attach a document on your computer or a network drive, click the **Attach Document** button. A **Select file(s) to upload** dialog box appears, allowing you to select the document you want.

   To select multiple items, press the SHIFT or CTRL key while clicking the items to highlight them.

7. When you have selected all the documents that you wish to attach, click **Add Rule**. The **Submission Rule 1** view of the task wizard appears.

8. Select the individuals who can provide the document that you need.

   The people who can be document submitters have been defined for you.

   You can select a combination of users and roles. If your exchange is set up to include collaboration groups, you can select these groups, as well. Choose **Groups**, **Role Group**, **Users**, or **Group Metadata** from the list that appears on the left side of the screen. Depending upon your selection, a list of users, roles, collaboration groups or custom fields appears.

   Highlight the users, groups or roles that you want to assign to the process, and click the arrow button to move them to the list on the right. If you selected **Group Metadata**, select the attributes that match the groups that you want to select.

9. Repeat steps 7 and 8 to select additional document submitters.

10. Click **Save**.

    A task will appear in the **Tasks** list for the person who is supposed to provide the document, and an email alert will be sent to the person, alerting him or her to your request.

**Responding to document requests**

Use the steps below if you are asked to provide a document.

**To respond to a document request**

You should be viewing the exchange where the document will be submitted.
The Tasks tab should be selected.

1. In the Tasks list, highlight the task.

2. From the Actions menu, select View Details. The Response view of the task wizard appears, displaying any notes and supporting documents that the reviewer or approver provided to explain the changes that you are required to make.

3. After you have reviewed the instructions, enter any notes that you wish to include in the Submission Instructions field.

4. Attach the document(s) that will be submitted. You can attach a document from the exchange or your computer or network. (If necessary, you can select documents from both the exchange and your computer or network.)

   To attach a document on the exchange, click the Attach Link button. A pane appears showing the folders on your exchange. Locate the document you want and highlight it, then click the Attach button that appears above the folder list. You can select as many documents as needed. When you have finished selecting documents, click the x button above the Attach button to close the selection pane.

   To attach a document on your computer or a network drive, click the Attach Document button. A Select file(s) to upload dialog box appears, allowing you to select the document you want.

   To select multiple items, press the SHIFT or CTRL key while clicking the items to highlight them.

5. When you have selected all the documents that you wish to submit, click Save.

   A task will appear in the approver's Tasks list, and an email alert will be sent to the person, alerting him or her that you have provided the requested document.

Acknowledging receipt of documents

Exchange managers may, at their discretion, require that you acknowledge that you have received documents that have been distributed to you using a document distribution business process. You may be required to complete and submit a form with your acknowledgment. Additional instructions and other documents may be attached to this request. Review all the attached files, complete the documents (if any) using the instructions provided, along with the fields on the subsequent screens, and then submit your acknowledgment.

If the distributor of the original documents requires an acknowledgment by a specified date and you do not respond by that date, an email reminder will be sent to you and other members of your group.

▶To acknowledge receipt of a document that has been distributed to you

You should be viewing the Hub. If you have opened the task wizard using the link in the email alert that was sent to you, skip to step 6.

1. In the navigation pane on the left side of the screen, click the Tasks option. Additional options appear.
2. Click the **By Task Name** option. A list of tasks that are assigned to you and that you have assigned to others (if your exchange role allows this).

3. Click the **Open tasks assigned to me** option in the **Standard Searches** box that appears to the right of the navigation pane.

4. Locate the task that you want to view.

5. From the **Actions** menu, select **View Details**. The **Instructions** view of the task wizard appears, displaying instructions for acknowledging that you have received the documents. Additional files may be attached.

6. Review the instructions. To view attached files, double-click them.

7. When you have finished reviewing the instructions, click **Next**. The **Response** view is displayed.

8. (Optional.) Enter a note for your acknowledgment response.

9. Attach any document(s) (if any) that need to be submitted.

   To attach a document on the exchange, click the **Attach Link** button. A pane appears showing the folders on your exchange. Locate the document you want and highlight it, then click the **Attach** button that appears above the folder list. You can select as many documents as needed. When you have finished selecting documents, click the **x** button above the **Attach** button to close the selection pane.

   To attach a document on your computer or a network drive, click the **Attach Document** button. A **Select file(s) to upload** dialog box appears, allowing you to select the document you want.

   To select multiple items, press the **SHIFT** or **CTRL** key while clicking the items to highlight them.

10. If an eForm was attached, complete it and click the **Submit Using Intralinks** button on the form. (eForms are PDF documents that allow you enter information onscreen, just as you would with a paper-based form.)

11. (Optional.) When you have added all the documents that are needed for the response, highlight the first document beneath the **Response** tab on the left side of the screen.

12. (Optional.) A number of custom fields may appear on the screen. Make the appropriate selection or entry for each field.

13. (Optional.) Click **Next Doc** to display the fields for the next file that you attached, and make the appropriate selection or entry for each field.

   Repeat this step until you have made entries for all the files that are attached to this submission.

14. Click **Save**.

   Your acknowledgment response is uploaded to Intralinks, and the exchange manager is alerted.

   The exchange manager may have a response approval process; if this is the case, acknowledgment responses may be returned to you for clarification or additional information if needed. If this is the case, the task will be redisplayed in your **Tasks** list and will include instructions from the manager about the clarifications or other changes that are needed.
Resubmitting acknowledgment responses

The exchange manager may have set up an approval process for acknowledgment responses. If your response is reviewed and additional information is required, you may receive an email from the exchange manager (or other contact) asking you to resubmit your response with changes. The process for resubmitting responses is very similar to the process that you used to make your original acknowledgment response.

To respond to a request to resubmit information

1. The email alert that you received requesting that documents be resubmitted includes a link to your exchange. Click this link to display the screen used for resubmission.
2. Review the message from the document approver. Make any required changes to your original documents.
3. Click Next. The Response view is displayed.
4. (Optional.) Enter a note about the resubmitted documents.
5. Attach the documents you updated and any additional documents requested by the document approver.

To attach a document on the exchange, click the Attach Link button. A pane appears showing the folders on your exchange. Locate the document you want and highlight it, then click the Attach button that appears above the folder list. You can select as many documents as needed. When you have finished selecting documents, click the x button above the Attach button to close the selection pane.

To attach a document on your computer or a network drive, click the Attach Document button. A Select file(s) to upload dialog box appears, allowing you to select the document you want.

To select multiple items, press the SHIFT or CTRL key while clicking the items to highlight them.
6. (Optional.) When you have added all the documents that are needed for the resubmission, highlight the first document beneath the Response tab on the left side of the screen.
7. (Optional.) A number of custom fields may appear on the screen. Make the appropriate selection or entry for each field.
8. (Optional.) Click Next Doc to display the fields for the next file that you attached, and make the appropriate selection or entry for each field.

Repeat this step until you have made entries for all the files that are attached to this submission.
9. (Optional.) You can view information about the original document, your acknowledgment response and any resubmissions that you have made by clicking the Submission History tab on the left side of the screen.
10. When you are ready to resubmit your response, click Save.

Your documents and/or notes are uploaded to Intralinks, and the exchange manager is alerted.
Adding co-monitors

Co-monitors are people who have been given permission to monitor your document submissions and to resubmit documents if required. Co-monitors are optional.

To add co-monitors to a business process instance

You should be viewing the exchange where the assignments were made.

1. Roll your mouse over the Tasks tab. Additional options appear.
2. Select By Process Name. A list of business processes with tasks that have been assigned to you, or that you have initiated, is displayed.
3. Highlight a business process instance that you want to be co-monitored.
4. From the Actions menu, select Add Co-monitor. The Select Co-monitors screen appears.
5. Select the individuals who will be co-monitors.
   The people who can be co-monitors have been defined for you.
   You can select a combination of users and roles. If your exchange is set up to include collaboration groups, you can select these groups, as well. Choose User, Role or Collaboration Groups from the list that appears on the left side of the screen. Depending upon your selection, a list of users, roles or collaboration groups appears.
   Highlight the users, groups or roles that you want to assign to the process and click the arrow button to move them to the list on the right.
6. Repeat step 5 until you have selected all the document reviewers or approvers.
7. Click Save.

Renaming a business process instance

To rename a business process instance

1. Roll your mouse over the Tasks tab. Additional options appear.
2. Select By Process Name. A list of business processes with tasks that have been assigned to you, or that you have initiated, is displayed.
3. Highlight a business process instance that you want to rename.
4. From the Actions menu, select Rename Task. The Rename Task window appears.
5. Enter the new name for the business process instance in the Enter new name field.
6. Click Rename.

Canceling a task

Depending upon the way your business process has been set up, you may be able to cancel a task that is not needed if no action has been taken on the task yet.
To cancel a task

1. Locate the task using the Tasks list and highlight it.
2. From the Actions menu, select Cancel task. A message appears asking you to confirm your selection.
3. Select Yes.

Using multi-task processes

As noted earlier, multi-task processes are collections of related tasks that must be completed to achieve a particular goal. Tasks are the individual, discrete actions that users must take while working to achieve the goal. For instance, you may have a separate task for reviewing each document that is associated with a process.

Use the procedures in this section to view processes and tasks, to complete tasks, and to add comments on tasks and processes.

Viewing processes and tasks

You can view the processes and tasks created by or assigned to using process lists and task lists that can be accessed from the Hub or from individual exchanges. In the Hub, the process lists and task lists displays both multi-task processes created within your exchanges and standard and rules-based business processes created and managed at the Hub level. If you view these lists within an exchange, only the processes and tasks created within the exchange are displayed.

To view lists of processes and tasks

Display the Hub.

1. Click the Tasks tab.

   The By Process Name option is selected automatically, displaying a list of processes that you have created or that include tasks that you are assigned to, either as a target group member or as an owner.

   For all processes, the process name and status is listed. Additional information is listed for multi-task processes, including the number of days since the process was initiated; the number of pending tasks awaiting your action; a calculation of the percentage of the process that has been completed; If you are viewing processes within an exchange you also can view the target group selected to perform tasks; the number of unread documents, the due date for completing the process, if any; and information about the last action taken for the process. If you are viewing multi-task processes on the Hub, the exchange and host organization associated with each process also is displayed.

2. To view only the tasks that are assigned to you, click the By Task Name option.

   When you double-click a multi-task process, all the tasks associated with it are displayed.
To view the details of a process

Display the Hub.

1. Click the Tasks tab.

   The By Process Name option is selected automatically, displaying a list of processes that you have created or that include tasks that you are assigned to, either as a target group member or as an owner.

2. Highlight the multi-task process that you want to view.

3. From the Actions menu, select View Details. All the tasks associated with the process are displayed, as are comments about the process.

To export task information

1. Display the details of the process for which you want to export information. For information on displaying process details, see “To view the details of a process” on page 173.

2. From the Actions menu, select Export List. A message appears allowing you to open or save the list as a Microsoft Excel worksheet.

   The exported list includes the name of each task and any documents that have been associated with it, the task’s status, and information about the last action that was taken on the task.

Completing tasks

Use the steps below to take action when tasks are assigned to you. (Note that if you are a process owner, you also can take action on tasks that are assigned to others.)

To complete tasks

1. Display the details of the process that contains the tasks that you want to complete. For information on displaying process details, see “To view the details of a process” on page 173.

2. Locate the task that you want to complete, and select an option for it from the list in the Next Step column. The next steps available depend upon the type of task you selected and the actions that have been performed on it already. Possible next steps include:

   Download — Select this option to download the document(s) attached to a task; the status of the task will be set to Confirmed, indicating that you have received the document.

   Upload — Select this command to update documents associated with a task before action has been taken on a task with one of the following task types: Distribute Document with Reply, Request Document, Request Document from Owner, and Request Review by Owner. This command appears only for tasks that have a status of Submitted or Pending Review.

   Publish — Select this option to publish a submitted document to your exchange. The Add Document Wizard appears, allowing you to select a location for the document, set details using custom fields, set permissions and alert permissioned users that the document is available.
Exclude — Select this option if the task is complete or is no longer needed; it will no longer appear in the target group members’ Tasks lists. Excluded tasks can be reinstated; to reinstate an excluded task, select the action that appears in the Next Step column for it. (This is the first step that must be completed for the task.)

Confirm — Select this option to indicate to task owners that you have received a document that has been distributed to you.

Accept — After you have reviewed documents, select this option to indicate that the documents are ready to be published. If this task is for a document that has been distributed for eSignatures, Accept can be used to return the task in its current state to the owner’s control even if the required number of signatures has not been obtained; all previous actions are undone, but a record of the actions is retained in the task’s history.

Resubmit — Select this option to send a request for resubmission to the target group associated with this task. If you need to provide additional direction to the target group, add a comment to the task. For information on adding comments, see “Adding comments to processes and tasks” on page 176.

eSign — Select this option to electronically sign the document that you have uploaded to a task. A box appears asking you to enter a reason for your signature. Enter your reason, then click Continue. Another box appears, asking you to enter your email address and Intralinks password. Once you have entered them, click eSign Document. Note that your eSignature is the equivalent of a handwritten signature and is legally binding.

Refuse to eSign — Select this option if you cannot electronically sign the document that you have uploaded to a task. A box appears asking you to select a reason for your signing of the document. Select your reason, then click Continue. Another box appears, asking you to enter your email address and Intralinks password. Once you have entered them, click Refuse eSignature.

Restart — Select this option to return an eSignature task to its original state. If this action is selected, all previous actions are undone, but a record of the actions is retained in the task’s history.

3. To view comments that have been entered for a task, click the bubble icon for that task in the Comments column. The number of comments that have been made appears in bubble icon. To add a comment, click the Add Comment link at the top of the screen.

4. To view a list of the actions that have been performed for this task, click the clock icon for the task in the History column.

To upload documents without associating them with any task

You can upload documents related to a process and associate them with tasks later. To upload files, complete the following steps:

1. Display the details of the process with which the documents will be associated. For information on displaying process details, see “To view the details of a process” on page 173.

2. Select the Upload link. The Upload Documents screen appears.
3. Click **Choose File**. A Select file(s) dialog box appears, allowing you to select the documents that you want to upload.

   To select multiple items, press the **SHIFT** or **CTRL** key while clicking the items to highlight them.

4. Click **Open**. The documents appear on the **Upload Documents** screen.

5. Click **Save**. The documents are uploaded, and line items appear for them in the task list.

▶ To associate uploaded documents with particular tasks

If you have uploaded tasks for a process and have not associated them with any tasks, use the following steps to do so.

The task list that includes the documents should be displayed.

1. Display the details of the process that contains the documents and tasks that you want to associate. For information on displaying process details, see “To view the details of a process” on page 173.

2. Locate the document that you want to associate.

3. In the **Next Step** column, select **Task Association**. The first screen of the Task Association wizard appears.

4. Select the task with which this document should be associated.

5. Click **Next**. The **Properties** view of the wizard appears.

6. Review the properties that are displayed. You can change the document’s name if you like.

7. Click **Next**. The **Details** view of the wizard appears.

8. Enter details about the document. An entry must be made for fields that appear in red with an asterisk (*) next to them.

9. Click **Save**.

   The document is removed from the task list and is associated with the task that you selected. The task’s status is updated, as well.

Faxing in documents

Depending upon the way your exchange is set up, you may be able to fax document into the exchange for processes. In order to do this, you must print a cover sheet that will be used to direct your document to the correct exchange.

**Note:** Do not use the same cover sheet for multiple documents unless you want the documents to have the same name on your exchange.

Once the document has been faxed in, it will be associated with the process, but it will not be associated with any particular task. To information on how to do this, see “To associate uploaded documents with particular tasks” on page 175.

▶ To create a fax-in cover sheet

1. Display the details of the process with which the documents will be associated. For information on displaying process details, see “To view the details of a process” on page 173.
2. At the top of the screen (to the right of the Actions menu), locate the Fax Cover option and click it. The Choose Users view of the Create Fax Cover Sheet wizard appears.

3. In the list on the left side of the screen, highlight the user(s) who will fax in the document, and click the arrow button to move them to the list on the right.

4. Click Next. The Cover Sheet view of the wizard appears.

5. Enter the title of the document. You also can enter notes about the document if you like; these notes will appear on the document’s properties screen in the exchange.

6. Click Save. The cover sheet is created in PDF format, and a message appears asking you whether you want to open the cover sheet or save it. Either open the cover sheet and print it or save it and print it later.

Fax the document, including the cover sheet, to the phone number that appears on the cover sheet. The documents and notes are uploaded to Intralinks, and the exchange manager is alerted.

Adding comments to processes and tasks

You can add comments to multi-task processes when they are configured, and exchange members will be able to add comments when they complete tasks that are assigned to them.

You can add comments both to individual tasks in task lists and the overall process. Process comments are not associated with any particular task.

Users who are members of either a target group or a process owner group can add and view comments. The person entering the comment can send an alert manually to target members and owners of the process.

Users’ ability to view, and respond to, specific comments are affected by their exchange role. For example, reviewers cannot see comments entered by other reviewers, but they can see comments entered by an exchange manager who is visible to them and respond to those comments. Process owners and users with the Manager Plus and Hidden Manager Plus exchange roles can see and respond to all comments, regardless of who created them. (Users with the Hidden Manager Plus role should avoid posting comments, however, since this will make them visible to all users who can view the comments.)

You have the option of saving deleted comments for audit purposes; the save deleted comments must be enabled to allow this functionality.

Comments can be exported to a Microsoft Excel spreadsheet.

To add a comment to a task

1. Display the details of the process that contains the task for which you want to add a comment. For information on displaying process details, see “To view the details of a process” on page 173.

2. Highlight the task.

3. From the Actions menu, select Add Comment. The Add Comment screen appears.
4. Enter your comment in the text box. Note that the following characters cannot be used in comments:
   `/ : * " < > ?` |

5. If you want to apply the comment to a task other than the one that is selected, select the task you want from the For Specific Task list.

6. Click Save.

**To add a comment that is not associated with any task**

1. Display the details of the process for which you want to add a comment. For information on displaying process details, see “To view the details of a process” on page 173.

2. From the Actions menu, select Add Comment. The Add Comment screen appears.

3. Enter your comment in the text box. Note that the following characters cannot be used in comments:
   `/ : * " < > ?` |

4. If you want to apply the comment to a task other than the one that is selected, select the task you want from the For Specific Task list.

5. Click Save.

Your comment will appear in the Process Comments section of the task list for this process.

**To view comments that have been entered for a task**

1. Display the details for the process containing the comments that you want to view. For information on displaying process details, see “To view the details of a process” on page 173.

2. Highlight the task that has been commented upon.

3. From the Actions menu, select Comments. The Comments screen appears, displaying the comments for the selected task.

4. The first 50 characters of each comment is displayed; you can view the entire comment if you like. To view additional text, click the More>> link next to the comment. When you have finished viewing the extended text, click Back to All Comments to view all the comments entered for the task.

5. When you have finished viewing comments, click Close.

**To view all comments that have been entered for a process and its tasks**

1. Display the details for the process containing the comments that you want to view. For information on displaying process details, see “To view the details of a process” on page 173.

2. Click the See All Comments link that appears in Process Comments section of the screen. The Comments screen appears, displaying all the comments entered for the process and the tasks associated with it.

3. The first 50 characters of each comment is displayed; you can view the entire comment if you like. To view additional text, click the More>> link next to the
Changing the status of processes

You can change the status of individual processes as they are completed or no longer needed. It is important that processes’ status is correct, since this information is used to determine the number of open tasks, percentage of completion and other statistics used to monitor and manage processes.

**Important!** When processes are completed, their statuses should be changed to **Closed**, to ensure accurate reporting.

You can perform this task only if you are a process owner.

▶ **To change the status of a process**

1. Display the details for the process whose status you want to change.

   For information on displaying process details, see “To view the details of a process” on page 173.

2. From the **Status** list in the upper right corner of the screen, select one of the following options:
   - **Open** — This status is displayed by default for processes that are in progress. Select this option if you have selected another status and now wish to begin using the process again.
   - **Closed** — Select this option when a process is completed or you do not wish to continue using it for another reason. If any tasks associated with the process are open, their status will be changed to Excluded. Closed processes can be viewed by process owners, but the processes cannot be changed in any way. Closed processes can be reopened if necessary.
   - **Suspended** — Select this option when you do not want to include a process in tallies of open tasks and unread comments, but you are not ready to close the process. The status of tasks that are underway are not changed when processes are suspended, and target group members and owners can continue to make changes to the tasks and add comments. Suspended processes can be reopened.
   - **Deleted** — Select this option if you wish to stop using the process and hide its tasks from target group members. The status of individual tasks that are in progress will not be changed. Owners will be able to view tasks, but cannot take action on them. Deleted processes can be reopened if necessary.

3. An informational screen may appear informing you of the changes that will be made to the process. Review the information on the screen, then click **Continue**.
Chapter 12: Using Intralinks eForms

Intralinks eForms offer an easy and secure way to collect and manage information from business partners. eForms are created using Adobe Acrobat technology and posted to your Intralinks exchange. Any PDF form that allows all PDF capabilities can be used as an eForm.

You will work with an Intralinks support representative to create your forms. Once they have been created, you can modify the forms before distributing them. You can attach eForms to business processes; for instance, with the rules-based document distribution business process, you can require that document recipients complete an eForm and return it to your organization or team for review. Note that you can attach only one eForm to each business process task.

Requirements and prerequisites

Note that eForms cannot be used with exchanges for which watermarking or document locking and protection are enabled.

The workflow option must be enabled on the exchange. For more information about setting up business processes, see Chapter 9, Managing standard and rules-based business processes, on page 117.

Forms authors wishing to modify eForms must have the following software:

- Adobe Acrobat Professional version 7.x or later

Forms recipients must have the following software:

- Adobe Reader version 7.x or later
  - or -
  - Adobe Acrobat Professional version 8.x or later

If you are using eForms with business processes

The workflow option must be enabled on the settings screen for the exchange. You can use eForms only with the rules-based document distribution and rules-base submission business processes.

For more information about setting up business processes, see Chapter 9, Managing standard and rules-based business processes, on page 117.

Creating and modifying eForms

Creating forms is a collaborative effort between your organization and customer support specialists within Intralinks Global Enterprise Services:

1. You create a blank version of the form using Microsoft Word or another tool.
2. You send the form to Intralinks, along with information about which fields should be form fields, and which of those fields are required.

If you plan to use the form with Q&A, also note:

- The exchange to which the completed copies of the form will be posted
The title you want to use for the question created for each copy of the form

The Q&A category that will be used for the form

3. An Intralinks customer service representative converts the form to a PDF-formatted eForm and returns it to you.

4. You populate any fields that cannot be changed by the form’s recipients and mark these fields as read only.

5. You enable usage rights that allow recipients to use Adobe Reader to complete the form. (When you enable usage rights, you make the form available to recipients using Adobe Reader and you prevent recipients using Adobe Acrobat Professional from modifying the form in ways that you did not intend. Note that users of Acrobat Professional can edit the form after usage rights have been enabled by making a copy of it, but changes to the form may cause it not to work.)

6. You distribute the forms to recipients using a business process.

**To populate fields and mark them as read only**

1. Open the form using Adobe Acrobat Professional.

2. Fill in any fields that cannot be edited by users.

3. From the **Forms** menu, select **Add or Edit Fields**. The fields view of the form is displayed.

4. Right-click on the first field that you updated in step 2. A menu appears.

5. Select **Properties**. The **Properties** screen for the field appears.

6. Mark the **Read Only** option.

7. Click **Close**.

8. Repeat steps 4 through 7 for each field that you updated in step 2.

9. When you have marked all the necessary fields as read only, click **Close Form Editing** in the upper right corner of the screen. The standard view of the form is redisplayed.

**To enable the usage rights**

Usage rights allow recipients to use Adobe Reader to complete the form.

**Important!** Complete this procedure only after you have entered information that cannot be changed by users and marked those fields as read only.

1. If you are using Adobe Acrobat **version 8**: From the **Advanced** menu, select **Enable User Rights**.

   If you are using Adobe Acrobat **version 9**: From the **Advanced** menu, select **Extend Features in Adobe Reader**.

   The **Enable Usage Rights in Adobe Reader** window is displayed.

2. Click **Save Now**.
Chapter 13: Viewing, exporting and printing reports

Overview

Read this chapter for information about:

- Reports about documents
- Reports about users and groups
- Advanced access reports
- Process access reports
- Other reports

Before you begin

In order to perform the tasks in this chapter, Adobe Flash Player 9 must be installed on your computer.

When you select an Intralinks Platform exchange in the Intralinks Hub, a message will appear if Flash Player 9 is not installed. This message includes links to information about the Flash Player software and to a location on the Adobe website where you can download this free software utility. Your organization’s IT department may be required to install this software for you.

If Flash Player 9 is not installed, you can open the exchange, but you will be able to perform only basic reviewer-related tasks like reading and printing documents.

Viewing document reports

Intralinks Platform provides a number of reports that help you make the most of the time you spend in your exchange.

Intralinks provides a printer-friendly view of the Document List, which provides a detailed view of the folders and the documents on the exchange.

As a manager, you also can view the Document Access Report to learn which users have access to a selected document or documents, the number of times they have viewed, downloaded and printed the documents, the date they last looked at the documents, and the version of the documents they most recently viewed, if applicable. The report also identifies when the document was added or updated and by whom.

In addition, as manager, you can view the Permissions Overview screen, which enables you to view and change users’ permissions and security settings for selected documents in a report-like format. To learn more about using the Permissions Overview screen, see “Reviewing and modifying permissions” on page 75.
Viewing a list of folders and documents on the exchange

You can display a printer-friendly view of your exchange’s Document List, then use your browser’s Print function to print the list if you like.

▶ To display a printer-friendly view of the Document List

The Documents tab should be displayed.

1. From the More Actions menu, select Print Document List. A browser window opens displaying a list of all the folders and documents on the exchange in a format that is suitable for printing.
2. (Optional.) Select Print from the File menu to print the list.

Viewing access information for documents

As noted above, the Document Access Report provides insight into how group members are using the exchange’s documents and when they most recently viewed them.

▶ To display the Document Access Report

The Documents tab should be displayed.

1. Highlight the document whose access information you want to view.
2. From the More Actions menu, select Access Report.
3. (Optional.) To export the information that appears on the report to a Microsoft Excel spreadsheet, click the Export button.
4. When you have finished viewing the report, click Close.

Viewing history information for documents

Use the Document History Report to see an audit trail for a selected document (or documents). This report shows information about when the document was added to the exchange, changes to permissions, updates to the document itself or the document’s properties, views by users, and instances where the document was moved. If you are viewing a deleted document, the report includes information about the document’s deletion.

▶ To display the Document History Report

The Documents tab should be displayed.

1. Highlight the document whose access information you want to view.
2. From the More Actions menu, select History. A list of all actions performed on the document appears.
3. If you want to view a smaller range of information, enter a date in the Since field. To view a single type of action (such as changes to permissions), choose the action you want from the Show list.
4. To show more details about the document, click Show Details.
5. (Optional.) To export the information that appears on the report to a Microsoft Excel spreadsheet, click the Export button.
6. When you have finished viewing the report, click **Cancel** or **Save**.

**Viewing a list of deleted documents**

Use the procedure below to view a list of deleted documents on your exchange.

If the **save deleted documents** exchange setting has been enabled (on) for your exchange and you were able to modify a document before it was deleted, you can double-click the document to view it or print it. (Documents that have been protected to prevent printing cannot be printed, of course).

**To view a list of documents that have been deleted from your exchange**

The **Documents** tab should be displayed.

1. Click the **Deleted Documents** link at the bottom of the Folders list on the left side of the screen. A list of documents that have been deleted is displayed, along with the date on which they were deleted.
2. If you want to view a smaller range of information, click the **Advanced Filter** smart filter. The **Exchange Filter Criteria** window appears, allowing you to select a variety of options for limiting the information that is displayed.
3. To create a Microsoft Excel spreadsheet containing the currently displayed information, select **Export This View** from the **Export** menu. You can print the spreadsheet using Excel if you like.

**Viewing reports for users and groups**

Intralinks’ reporting capability makes it easy for you and other exchange managers to see trends in groups’ exchange usage and to evaluate their level of interest in particular issues.

At other times, you simply need to manage the exchange, and a comprehensive user list can assist you in performing management tasks efficiently.

**Exporting a list of users on the exchange**

You can export a list of all exchange users (or a subset of the entire list) to Microsoft Excel, where you can manipulate the information and print it if you like. Use the following procedure to do so.

**To export and print a list of all users on the exchange**

The **Users & Groups** tab should be displayed.

1. From the **More Actions** menu, select **Export Entire List**. A **File Download** dialog box appears.
2. Click **Open** to display the user list in Excel.
3. In Excel, from the **File** menu, select **Print**. A print dialog box appears.

**To export and print a list of the users who currently appear in the User List**

Be sure the list of users you want to export is displayed in the User List.
1. From the More Actions menu, select Export This View. A File Download dialog box appears.
2. Click Open to display the user list in Excel.
3. In Excel, from the File menu, select Print. A print dialog box appears.
4. Click OK.

Viewing users’ and groups’ overall exchange activity

Intralinks Platform provides the following reports, which show information about the documents accessed by particular users or groups:

- User Activity by Group Report
- Multi-user Coverage Report
- Group Coverage Report

Intralinks Platform also provides the following advanced reports:

- Folder Coverage
- Search Summary
- Exchange Activity Summary
- Exchange Statistics Summary

The User Activity by Group Report

The User Activity by Group report provides a comprehensive view of group and user coverage for folders and documents. The report can be created for specific groups or for all groups. Groups that do not include any members yet are not included on the report. You can choose to exclude documents for which there has been no activity.

The report is produced offline and provided to you when it is ready for viewing. Reports generally are available within one hour after a request is made. The report will be delivered as a Microsoft Excel spreadsheet. The activity for each group included on the report will be displayed on a separate worksheet.

The top section of the report provides summary information about the number of times users and each group has accessed documents on the exchange. The lower part of the report lists individual documents by folder, along with the number of documents each user has accessed in each folder and the most recent date (if any) that the user accessed each document. If the user is not allowed to view the document, No permission appears on the report.

To request the User Activity by Group report

The Reports tab should be displayed.

1. Highlight User Activity by Group and click the Open Report button. The User Activity by Group screen appears.
2. Click the New Report button. The Set Properties view of the User Activity by Group wizard appears.
3. Select the time period for the activity that you want to include in the report: since the launch of the exchange; the last day; the last seven days; last month; or a range of dates that you specify.

4. (Optional.) Mark the **Do not include on the report documents that have not been viewed** option. If you mark this option, the report likely will be shorter and take less time to create.

5. Click **Next**. The **Select Groups** view of the User Activity by Group wizard appears.

6. In the **Available groups** list, highlight each group that you wish to include on the report and click the arrow button ➔ to move the name to the **Groups included in report** list.

7. Click **Submit**.

8. When the report is ready to be viewed, you will receive an email alert. Click the link in the email message to display the report in Microsoft Excel.

   Alternatively, highlight the report in Intralinks, then select **Download** from the **Actions** menu. A dialog box appears, allowing you to open or save a copy of the report.

9. To print the report, from the **File** menu within Excel, select **Print**. A print dialog box appears.

10. Click **OK**.

**The Multi-user Coverage Report**

The Multi-user Coverage Report provides insight into the documents that selected users are viewing and printing. The report is presented in a tabular format; you can print the report for multiple users and perform side-by-side analysis of the users’ document usage.

The Multi-user Coverage Report captures information about document activities, including viewing, printing and permissions. You also can view the most recent date on which the selected user viewed particular documents.

▲ **To view, export and print the Multi-user Coverage Report**

The **Users & Groups** tab should be displayed.

1. Locate the user whose information you want to view, and highlight the user’s name. To view information for multiple users, hold down the **SHIFT** key while clicking the users’ names.

2. From the More Actions menu, select **Multi-user Coverage Report**. The Multi-user Coverage Report screen for the selected user(s) appears.

3. To view a shorter list of documents, enter information in the **Filter documents** field at the top of the screen. Note that this field is case sensitive.

4. Select the information that you want to view. From the **Show** field, select **Viewed, Permissioned, Printed** or **Last Viewed on**.

5. Click **Update**. Information for the selected users is displayed.

   If you change the report options, be sure to click **Update** again.
6. When you are ready to print the report, click the Export button in the lower right corner of the window. The report appears in table format in a Microsoft Excel spreadsheet.

7. In Excel, from the File menu, select Print. A print dialog box appears.

8. Click OK.

The Group Coverage Report
Like the User Coverage Report, the Group Coverage Report provides a view of the documents that selected groups are accessing most often. The report is presented in a tabular format; you can print the report for multiple groups and perform side-by-side analysis of the groups’ document usage.

The Group Coverage Report captures information about document activities, including viewing, printing and permissions. You also can view the most recent date on which the selected members of the selected group or groups viewed particular documents.

To view, export and print the Group Coverage Report
The Users & Groups tab should be displayed.

1. Locate the group whose information you want to view, and highlight it. To view information for multiple groups, hold down the SHIFT key while clicking the groups’ names.

2. From the More Actions menu, select Group Coverage Report. The Group Coverage Report window for the selected group(s) appears.

3. To view a shorter list of documents, enter information in the Filter documents field at the top of the screen. Note that this field is case sensitive.

4. Select the information that you want to view. From the Show field, select Viewed, Permissioned, Printed or Last Viewed on.

5. Click Update. Information for the selected groups is displayed.

If you change the report options, be sure to click Update again.

6. When you are ready to print the report, click the Export button in the lower right corner of the screen. The report appears in table format in a Microsoft Excel spreadsheet.

7. In Excel, from the File menu, select Print. A print dialog box appears.

8. Click OK.

The Folder Coverage report
The Folder Coverage report provides insight into which groups are most active and which folders they are accessing most often. It is presented in a graphical format that allows you to make a quick analysis both of group activity and the information that is most interesting to the groups’ members.

The Folder Coverage report captures information about document activities, including viewing, printing and downloading. You can view information for the groups and folders that are most, and least, active. The report is presented in the form of a “heat map”; darker colors indicate a higher level of activity, while lighter colors indicate little or no activity. If a group does not have access to any documents within a folder, the folder appears blank appears on the report. If the
group has not read any of the documents within the folder, 0% appears. If the folder is empty (no documents have been placed in it yet), n/a is shown. In addition to percentages, the actual number of accesses is displayed on the report.

If you select the **Show total coverage** option, an additional row appears at the top of the report showing aggregated totals for all folders on the exchange, not only those displayed on the report.

► **To view, export and print the Folder Coverage report**

The **Reports** tab should be displayed.

1. Highlight **Folder Coverage**.
2. Click the **Open Report** button. The **Folder Coverage** screen appears.
3. A series of options appear at the top of the window. Mark the **Total Coverage** option to see coverage information for the entire exchange, in addition to the coverage information for individual folders.
4. Click **Update**. Information for the selected number of folders and groups is displayed.
   
   If you change the report options, be sure to click **Update** again.
5. When you are ready to print the report, click the **Export** button at the bottom of the screen. The report appears in table format in a Microsoft Excel spreadsheet.
6. In Excel, from the **File** menu, select **Print**. A print dialog box appears.
7. Click **OK**.

**The Search Summary Report**

The Search Summary Report provides a view into the terms being used when users search the exchange for specific documents or folders. This information is displayed in table and bar graph format. You can add or remove individual terms from the bar graph by clicking the boxes in the **Chart** column. You can specify the timeframe and the number of terms that appear on the report.

This report is available only if the **enable document content search** setting is selected for your exchange.

Using the information in this report, you can get another view into the information that is most important to users. You also can use it to determine whether important information needs are not being met by the exchange; if a large number of users search for a term frequently, it may indicate that the information they want is missing from the exchange or that the documents they want to access are not located in the folders where they expect to find them.

► **To view, export and print the Search Summary report**

The **Reports** tab should be displayed.

1. Highlight **Search Summary**.
2. Click the **Open Report** button. The **Search Summary** screen appears.
3. Options for selecting a time period and the number of terms that will be included on the report appear at the top of the window. You also can view information for groups or individual users. Select the options you want.
4. Click **Update**. Information for the selected number of folders and groups is displayed.

   If you change the report options, be sure to click **Update** again.

5. When you are ready to print the report, click the **Export** button at the bottom of the screen. The report appears in table format in a Microsoft Excel spreadsheet.

6. In Excel, from the **File** menu, select **Print**. A print dialog box appears.

7. Click **OK**.

**The Exchange Activity Summary Report**

The Exchange Activity Summary Report provides insights into whether particular groups and their members are actively using the documents on your exchange and whether their level of activity is ongoing. The report can display information about either the most active exchange users or those who are least active.

The Exchange Activity Summary Report can be printed either for user groups or for individual users. It identifies the groups or users who are most (and least) actively viewing documents on the exchange.

The report offers two views: The Over Time view and the Total view. As their names suggest, the Over Time view enables you to see whether users’ interest is sustained over a long period of time, is increasing, or is waning. In this view, a line graph shows the percentage of all available documents that group members or individuals have viewed over the specified period of time. Viewing, printing and downloading documents all are examples of accesses that are included in this report.

The Total view offers a bar graph that shows aggregated information. It provides a quick snapshot of overall interest during the selected time period, but does not provide insight into whether users’ interest is growing, falling or steady.

You can view the number of documents viewed by each user or group using the **Unique Access** selection. (Each viewed document is counted once in this view, regardless of the number of times it has been viewed.) If you select **All Access**, the report displays the number of times the users or group members viewed documents.

Note that the Exchange Activity Summary Report is based on the documents that are available to each group or group member. Documents to which a group is not permissioned are not included in the analysis of their usage. In some cases, one buyer group may have more total accesses but a lower percentage than another group. This simply means that the first group was given access to a larger number of documents but viewed a lower percentage of them than the second group did.

**Important!** Be aware that printing of protected Microsoft Office documents is not tracked, and printing instances of Microsoft Office documents are not included in totals on the Activity Summary Report. If your organization requires this information, you can require users to view documents using Intralinks Viewer, which provides tracking of both the number of times a document is printed and the amount of time the document is viewed.
To view, export and print the Exchange Activity Summary Report for users

The Reports tab should be displayed.

2. Click the Open Report button. The Activity Summary Report screen appears.
3. A series of options appear at the top of the window. Select the options you want. Be sure that Users is selected, rather than Groups.
4. Click Update. Information for the selected users is displayed both in a graph and in a table.
   - If you change the report options, be sure to click Update again.
5. When you are ready to print the report, click the Export button at the bottom of the screen. The report appears in table format in a Microsoft Excel spreadsheet.
6. In Excel, from the File menu, select Print. A print dialog box appears.
7. Click OK.

To view, export and print the Exchange Activity Summary Report for groups

The Reports tab should be displayed.

2. Click the Open Report button. The Activity Summary Report screen appears.
3. A series of options appear at the top of the window. Select the options you want. Be sure that Groups is selected, rather than Users.
4. Click Update. Information for the selected groups is displayed both in a graph and in a table.
   - If you change the report options, be sure to click Update again.
5. When you are ready to print the report, click the Export button at the bottom of the screen. The report appears in table format in a Microsoft Excel spreadsheet.
6. In Excel, from the File menu, select Print. A print dialog box appears.
7. Click OK.

The Exchange Statistics Summary Report

The Exchange Statistics Summary Report displays high-level statistical information about exchange users, as well as for documents, in a table format.

For each user role, the number of currently active and inactive users are included, as are the total number of current users (active and inactive) and the highest number of users who had access to the exchange at a single time.

For documents, the report shows the current number of documents and pages within the documents, as well as the size of the documents. The High column
shows the largest number of documents and pages posted at any one time, along with their size.

This report provides insight into the size of your exchange, both in terms of users and in terms of content.

To view, export and print the Exchange Statistics Summary Report

The Reports tab should be displayed.

2. Click the Open Report button. The Statistics Summary screen appears.
3. When you are ready to print the report, click the Export button at the bottom of the screen. The report appears in table format in a Microsoft Excel spreadsheet.
4. In Excel, from the File menu, select Print. A print dialog box appears.
5. Click OK.

Viewing advanced access reports

You can view document access information across multiple exchanges for selected groups of documents, users or groups or working sets for documents, users, groups or exchanges. These Access Reports can be viewed in three formats: by exchange, group and user; by exchange and group; and by user.

In order to view these reports, you must be an exchange managers who belongs to a user group for which the Permission to run advanced access report custom field has been set to Yes. These reports are available only for exchanges that were created using a Life Sciences industry template.

The Access Reports include the following: Name of the document, exchange, group and user; the user’s email address, phone number and fax number; the date and exchange on which the user first accessed the document; the date and exchange on which the user last accessed it; the dates on which the document was published and permissioned to the user’s group; the date on which the user first printed the document; information about the first and last dates on which the user was sent email alerts about the document, and information if the alerts failed to be delivered (“bounced back” because of a bad email address or temporary email system outage, for example), including a suggested course of action.

You can view information for a time period up to 366 days. This date range can be based on either the date that documents were published, or that alerts were sent to users. You must enter at least one date range in order to view the report. (This limitation does not apply if you are viewing the report for documents or document working sets.)

These reports can include:

- Up to 25 exchanges
- Up to 15 documents
- Up to 15 users
- Up to 15 groups
These limitations apply to working sets as well.

Exchanges that require enhanced security (two-factor authentication) must be open at the time the report is run in order to be included. Exchanges that require public-private declarations or use Intralinks’ Access Gatekeeper functionality cannot be included.

You can filter results using the dates on which alerts were published or alerts were sent, or a combination of the two. Reports can include up to 366 days’ worth of results. If the resulting report is likely to be very large, a message will appear suggesting that you filter the report to ensure that the resulting report can be printed.

Very large reports (those containing more than 10,000 records) may take some time to be generated. When your report is complete, you will receive an email message with a link to the report. The report results will be available for 7 days.

If the selected exchange was migrated from IL5 to Intralinks Platform, the date that documents were last accessed before migration occurred also is displayed.

**Note:** Be aware that the time to generate this report will increase as you select more exchanges that contain large amounts of data and large numbers of users. If you find that the time required to generate your report is excessive, consider creating the report for a smaller range of information.

You can request audit reports that provide details about use of the Hub Access Reports, including the frequency with which they have been created for members of your organization. These reports must be created by a member of the Intralinks client services team and are available to members of the organizations for which the Hub Access Reports were created. Contact Intralinks customer assistance to request audit reports.

**To display the Access Reports**

The **Hub** tab should be displayed.

1. Locate the exchanges, users, groups, documents or working set whose access information you want to view, and highlight them.

2. From the **Actions** menu, select the type of Access Report that you want to print:
   - Access Report by Exchange/Group/User
   - Access Report by Exchange/Group
   - Access Report by User

3. A screen will appear allowing you to specify the information that you want to include on the report, and how the information will be sorted. Be sure to enter a range of dates in the **Publish Date** and/or **Alerted Date** fields. When you have made your entries, click Update. The report in displayed on the lower half of the screen.

Very large reports (those containing more than 10,000 records) may take some time to be generated. When your report is complete, you will receive an email message with a link to the report. The report results will be available for 7 days.
4. **(Optional.)** To export the information that appears on the report to a Microsoft Excel spreadsheet, click the **Export** button.

5. When you have finished viewing the report, click **Close**.

**Viewing Process Access Reports**

You can view the Process Access Reports for business processes, for specific process instances or tasks, and for the users who have accessed the processes.

The Process Access Report for business process instances lists the groups that have been assigned tasks through the selected business process instance, along with information about the users from each group who accessed the instance for the first time and most recently. You can view groups that currently have access to the instance, groups that no longer have access to the instance, and groups that have never been given access to the instance.

**Note:** The Process Access Reports include only users and groups that you are allowed to view.

The Process Access Report for groups lists processes; the target group for each process; the date each target group was given access to the process; and the dates on which group members accessed the process for the first time and most recently. You can view processes to which the groups currently have access, processes to which the groups no longer have access, and processes to which the groups have never been given access.

The Process Access Report for users lists processes; the target group for each process to which the selected user belongs; the date the target group was given access to the process; and the dates on which this user accessed the process for the first time and most recently. It also includes information about when the user was first alerted and most recently alerted about the process. If one or more alerts could not be delivered, the date of the most recent delivery failure is listed, along with the reason for the failure. This information can help you to resolve issues that arise when users’ email addresses change, for example. You can view processes to which the user currently has access, processes to which the user no longer has access, and processes to which the user has never been given access.

**To display the Process Access Report for business process instances**

You should be viewing the exchange that is associated with the business process instances.

1. Roll your mouse over the **Tasks** tab at the top of the screen. A menu appears. Select **By Process Name**. A list of business processes with tasks that have been assigned to you, or that you have initiated, is displayed.

2. From the **Actions** menu, select **Process Access Report**. The **Process Access** screen appears.

3. When you have finished viewing the report, click **Close**.

**To display the Process Access Report for Groups**

The **Users & Groups** tab should be displayed.
1. Highlight the group whose access information you want to view.
2. From the **Actions** menu, select the **Process Access**.
3. (Optional.) To export the information that appears on the report to a Microsoft Excel spreadsheet, select either **Export this page** or **Export all pages** from the **Export** list.
4. To view the tasks associated with a specific process instance, double-click the instance.
5. When you have finished viewing the report, click **OK**.

**To display the Process Access Report for Users**

The **Users & Groups** tab should be displayed.

1. Locate the user whose access information you want to view and highlight it.
2. From the **Actions** menu, select the **Process Access**.
3. (Optional.) To export the information that appears on the report to a Microsoft Excel spreadsheet, select either **Export this page** or **Export all pages** from the **Export** list.
4. To view the tasks associated with a specific process instance, double-click the instance.
5. When you have finished viewing the report, click **OK**.

**Other reports**

**The Process Definition Summary Report**

The Process Definition Summary Report provides a list of the business processes that have been created using a selected business process definition, along with a count of the business process instances in use for each process and their status (pending approval, approved, rejected, and so on). You can double-click any business process in the list to view more information about the business process instances associated with it.

**To view the Process Definition Summary Report**

The exchange whose information you want to view should be displayed.

1. In the left column, highlight **To Do & Submissions**. A list of your to dos and submissions appears, along with a **View** menu above this list.
2. From the **View** menu, select **Summary Report**. The **Process Definition Summary Report** screen appears.
3. Select the business process definition whose details you want to view from the **Process Definition** list. Details for the definition are displayed.
4. To view the business process instances created from a particular business process, double-click the process. Click the back button when you have finished viewing the information on the screen.
Appendix A: Exchange settings

Exchange settings determine many of the features that are available on your particular exchange. Other features are determined by the template used to create the exchange and may be tailored to your particular market segment.

All exchange settings also appear on the templates that are used to create exchanges.

The field labels (shown below are those that appear on the update workspace settings screen. Some labels may be different on the view workspace settings screen.

**Note:** Depending upon the industry type associated with the templates used to create your exchanges, some of the settings below may not appear on the view workspace settings and update workspace settings screens.

### General

**Enable document content search**

This setting determines whether selected user groups are able to perform only basic searches — that is, searches of document and folder names — or whether they can perform more comprehensive searches, including the contents of documents and any notes that have been entered for them in the New Documents Wizard or on the properties screen for each document.

**Allow access by Intralinks administrators**

This setting allows security-conscious managers to control Intralinks administrators’ access to exchange content. This command appears only if it was enabled on the template used to create your exchange.

- If the setting is marked (on), Intralinks administrators have the ability to see all information on exchanges created using this template.

- If the setting is unmarked (off), you have the option to block Intralinks administrators from viewing exchange content; administrators still will be able to view the exchange name and settings. You can turn the exchange setting on and off as your needs require.

Regardless of how this setting is set, Intralinks administrators are able to view your templates and business group information.

**Note:** Enabling this setting may impact Intralinks customer service representatives’ ability to respond to support issues. We do not recommend enabling this exchange setting unless your organization’s security needs require it.

**Show welcome to workspace alert screen**

This setting determines whether email alerts can be sent to exchange users when you change the exchange phase to a phase that makes the exchange visible to these users. If this setting is marked, a screen will appear when you change the exchange’s phase, allowing you to change the subject line and add a note to the alert before sending it.
• If the setting is marked (on), email alerts will be sent to users when the exchange becomes visible to them.
• If the setting is unmarked (off), no welcome alerts will be sent.

**Tags**

This setting determines whether exchange managers and publishers will be able to assign tags — words or phrases that describe the contents of documents added to the exchange — to documents using the New Document Wizard. Tags can be used to classify and organize information in ways that are meaningful to your organization.

• If the setting is marked (on), users will be able to use tags to describe documents.
• If the setting is unmarked (off), tags will not be available.

**Custom fields**

This setting determines whether custom fields are available on your exchange. Custom fields provide a structured way for managers and publishers to describe documents and other elements in greater detail. Custom fields can be used to enter specific pieces of information, such as expiration dates, internal tracking numbers, and the like.

• If the setting is marked (on), users will be able to use custom fields to describe documents.
• If the setting is unmarked (off), custom fields will not be available.

**Enable business processes**

This setting determines whether exchange users will be able to set up business processes for requesting and submitting documents for review and approval. This setting can be enabled only by an Intralinks administrator; once it has been enabled, it cannot be disabled again.

• If the setting is marked (on), users will be able to set up and use workflows.
• If the setting is unmarked (off), workflows will not be available.

When you mark this setting, you must also select one of the following options:

• **Enable process only** — If this setting is marked, standard and rules-based business processes will be available on the exchange. *This setting must be marked!*

• **Enable multi-level processes** — This setting is used only for exchanges that are used for Amendment Vote Management. *Do not select this option.*
Access Workspace Builder

This setting determines whether exchange managers will be able to access Intralinks Designer from within the exchange. Intralinks Designer is a tool that enables managers to upload and manage content and users en masse. If this setting is not marked, managers can use Intralinks Designer, but they will have to start it using selections on the Microsoft Windows Start menu.

- If the setting is marked (on), managers will be able to access Intralinks Designer from within the exchange.
- If the setting is unmarked (off), Intralinks Designer will not be available within the exchange.

Session Inactivity Timeout Setting in minutes

This setting determines the amount of time that a user may leave Intralinks Platform inactive before the user is logged out of the system automatically. By default, Intralinks Platform sessions end automatically when they have been idle for 60 minutes. Using this setting, you can specify a shorter amount of time for session timeouts. The minimum session time allowed is 20 minutes. If users have access to multiple exchanges, the shortest timeout period specified for any of those exchanges will be the one used.

Shorter timeout periods reduce the window of opportunity for a user’s session to be compromised by a computer hacker; this may be a concern, for example, if a user accesses Intralinks Platform on a public computer, or if the user has left his machine unlocked.

Enhanced security

This setting identifies the security level that has been selected for this exchange. The setting can be changed only by an Intralinks employee.

The setting determines the level of security applied to the exchange:

- **Standard**: No enhanced security measures have been applied to the exchange. Standard security measures apply. Users who log into Intralinks successfully can open the exchange without answering their challenge question or entering a one-time password.

- **Risk assessed challenge question then one time password**: A risk assessment is performed whenever a member of this exchange attempts to access it. If the risk level is low, the exchange will be displayed immediately. If the risk level exceeds an acceptable limit, the user will have to provide the answer to their challenge question. When they have successfully answered the challenge question, a one-time password will be emailed to them. They will have to enter the password in order to enter the exchange. Each password can be used only once; if the user closes the login window or enters an incorrect password, another password will be emailed to them. Once the users have successfully entered the one-time password, the exchange is displayed.

- **Risk assessed challenge question**: A risk assessment is performed whenever a member of this exchange attempts to access it. If the risk...
level is low, the exchange will be displayed immediately. If the risk level exceeds an acceptable limit, the user will have to provide the answer to their challenge question. When they have successfully answered the challenge question, the exchange is displayed.

- **Risk assessed one time password**: A risk assessment is performed whenever a member of this exchange attempts to access it. If the risk level is low, the exchange will be displayed immediately. If the risk level exceeds an acceptable limit, a one-time password will be emailed to them. They will have to enter the password in order to enter the exchange. Each password can be used only once; if the user closes the login window or enters an incorrect password, another password will be emailed to them. Once the users have successfully entered the one-time password, the exchange is displayed.

- **Always challenge question**: Members of this exchange will have to provide the answer to their challenge question every time they access the exchange, regardless of their risk level.

- **Always one time password**: Members of this exchange will be emailed a password each time the attempt to access the exchange, regardless of their risk level. They will have to enter the password in order to enter the exchange. Each password can be used only once; if the user closes the login window or enters an incorrect password, another password will be emailed to them.

- **Custom**: A custom authentication method has been created for this exchange. For example, your organization may have requested that the exchange be available only during business hours, or access may be restricted to computers that have an IP address within a specified range. Custom authentication methods are set up by Intralinks employees and should not be changed.

You can allow one-time passwords to be sent by email, by text message (SMS), or by either method. An Intralinks employee must implement your selection. If the Deliver One Time Password By Email option is marked, users can have one-time passwords sent to the email addresses they use when logging into Intralinks Platform. If the Deliver One Time Password By SMS option is marked, users can have one-time passwords sent to mobile devices that they have registered with Intralinks. If both options are marked, users will be able to select the method by which a one-time password will be sent each time a password is required.

### Password complexity

This setting determines whether exchange users will be required to create simpler or more complex passwords for their Intralinks account. If a user belongs to more than one exchange and any of those exchanges requires a complex password, the user is required to enter a complex password.

**Note**: The normal setting typically is used only by managers of Private Equity exchanges. Managers of other types of exchanges generally should choose the complex option.

**Normal**

Users whose exchanges allow normal passwords can create passwords that use the following rules:
• Contains 8 or more characters
• Does not repeat any character three times consecutively
• Does not contain quotation marks ("), semicolons (;), backslashes (\) or spaces
• Normal passwords can contain a combination of alphabetic, numeric and special characters.

Complex

Complex passwords use the following rules:

Passwords are case sensitive and must have at least 8 characters. They must contain two or more of the following types of characters:

• Lowercase letters
• Uppercase letters
• Numbers
• Special characters

They may not use the following characters:

: ";'\<>

When a user creates a complex password, he or she cannot repeat any character three times. The user also cannot reuse a password that has used within the past 365 days.

Alternatively, the user can enter a phrase of 16 to 30 characters; in this case, the user does not need to follow the rules above.

Password expiration timeframe

This setting determines when, and if, the passwords for users of this exchange will expire. Selections for this field are 90 days, 365 days and never expire.

The default setting for Private Equity templates is never expire; for all other industry types, the default setting is 90 days.

If a user belongs to multiple exchanges with varying requirements for password resets, the shortest duration will applied to the user.

You cannot change this setting yourself; it must be changed by an Intralinks employee. If you wish to change the expiration timeframe for this exchange, contact Intralinks Global Enterprise Services.

Enable E-Forms

This setting determines whether Intralinks eForms functionality is available in this exchange. eForms are PDF forms that are used to collect information from business partners and post it to your Intralinks exchange.

You cannot change this setting; it must be changed by an Intralinks employee. If you wish to use e-forms with this exchange, contact Intralinks Global Enterprise Services and request that the setting be changed for that exchange.
• If the setting is marked (on), you can use eForms to publish information in this exchange.
• If the setting is unmarked (off), eForms are not available for this exchange.

Enable custom alerts

This setting determines whether the email alerts sent from your system are standard alerts supplied by Intralinks or alerts that have been customized specifically for your organization to reflect your organization’s branding and messaging standards. (If this setting is enabled but no custom alerts have been created, Intralinks’ standard alerts will continue to be sent.)

You cannot change this setting or perform the customizations yourself; these tasks must be done by an Intralinks employee. If you wish to use custom alerts with this exchange, contact Intralinks Global Enterprise Services.

• If the setting is marked (on), custom alerts are being used for this exchange.
• If the setting is unmarked (off), Intralinks’ standard alerts are being used for this exchange.

Q&A

Q&A module

The setting determines whether Q&A functionality is available on the exchange. (Q&A functionality generally is used by the Mergers and Acquisitions market segment.)

• If the setting is marked (on), buyers will be able to ask questions and coordinators in your organization will be able to answer the question or delegate it to subject matter experts. You also will be able to create FAQ entries from questions that will be visible to all buyers.
• If the setting is unmarked (off), Q&A functions will not be available.

Question limit

This setting appears only if the Q&A module setting is marked (on). The Question limit setting provides a default entry for new buyer groups as they are created; you can choose to limit the number of questions each group can ask (using a different limit for different groups if you like) or to allow buyers to ask an unlimited number of questions. On this screen, enter a numeric value or leave it blank if there is no limit.

Enable Q&A Coordinator role

This setting appears only if the Q&A module setting is marked (on). Note that this setting enables the limited Q&A coordinator role. When this setting is enabled, the Reviewer Plus role (if it has been enabled) will be replaced with the new
coordinator role. If existing users have been assigned the Reviewer Plus role, they will lose that role.

Once this exchange setting has been enabled, it cannot be disabled again.

The limited Q&A coordinator role must be assigned to users; it is not assigned automatically. Users selected to be limited Q&A coordinators cannot be members of collaboration groups.

Users with this role can answer and delegate questions; they also can freeze and unfreeze Q&A categories. They cannot perform the following tasks:

- Create documents
- Create folders
- Update user permissions
- Select buyers to be question submitters for their buyer group
- Add, update or remove users from the exchange
- Add, update or delete groups
- Add or remove users from groups
- Set question limits

These tasks must be performed by a Q&A coordinator with the Manager Plus exchange role. (Some tasks can be performed by a user with a manager-level or publisher-level exchange role.)

M&A advisors who act as Q&A coordinators and exchange managers use the limited Q&A coordinator role to delegate some authority to their clients without providing managerial access to the exchanges that they manage. The limited Q&A coordinator role provides greater visibility into the clients’ deals than the subject matter expert (SME) role does.

### SME delegation

Q&A coordinators, who may be external to the seller organization, can delegate questions to one or more SME groups within the seller organization; these groups in turn can re-delegate those questions to the SME groups best equipped to respond to them. The groups that are allowed to re-delegate questions are referred to as the SME coordinator groups.

If this functionality is enabled, any SME group that has been delegated a question, either manually by the Q&A coordinator or through auto-delegation, can re-delegate that question to another SME group if necessary. Questions that have been re-delegated cannot be delegated again by the SME group that received the re-delegated question. The SME coordinator who re-delegates a question can set a new due date for the SME group that will receive the question. However, if the Q&A coordinator assigned a due date, the SME coordinator cannot change it. The SME coordinator also cannot retract a delegation made by the Q&A coordinator or another SME coordinator group.

If a member of an SME coordinator group re-delegates a question, the response will be delivered to the SME coordinator group, which is responsible for providing
the final response to the Q&A coordinator. Similarly, the Q&A coordinator will respond to the SME coordinator and not directly to the SME group to which a question was re-delegated.

Users and Groups

Enable workspace groups

This setting is marked by default in all exchanges and cannot be unmarked. Exchange groups are required in order for users to view documents on your exchanges.

Collaboration groups

This setting typically is used with Intralinks’ Q&A functionality. It determines whether collaboration groups are available on your exchange. Collaboration groups enable members of your organization to communicate with one another while using your exchange. They also are used to delegate buyers’ questions to subject matter experts within the organization if you are using Intralinks Platform’s Q&A function in the exchange. Once this setting is enabled for an exchange, it cannot be turned off.

- If the setting is marked (on), you will be able to create collaboration groups using the Add Group Wizard.
- If the setting is unmarked (off), you will not be able to create collaboration groups on the exchange, and you will not be able to delegate users’ questions to subject matter experts within your organization.

Buyer groups

This setting determines whether buyer groups are available on the exchange. It typically is used with Intralinks’ Q&A functionality on Mergers & Acquisitions exchanges. Members of a buyer group can view one another’s comments. Buyer group members must have an exchange role of Previewer or Reviewer; a user can be a member of only one buyer group. Once this setting is enabled for an exchange, it cannot be turned off.

- If the setting is marked (on), you will be able to create buyer groups using the Add Group Wizard.
- If the setting is unmarked (off), you will not be able to create buyer groups on the exchange.

Group member roles enabled

This setting determines whether group member roles will be used with this exchange. If this option is selected, users can be assigned a group member role that describes their position within their organization or the function they perform as a member of your exchange. Group member roles can be used to define and drive business processes and naming convention rules, as well as to organize and control access to your exchange’s contents. These roles are optional and need not be assigned to all members of a group. Group member roles are in addition to users’ exchange roles (reviewer, manager, etc.).
Group member roles must be identified on the templates used to create your exchanges. This functionality must be enabled or disabled by an Intralinks administrator, and changes to the roles must be made by Intralinks. Intralinks Global Enterprise Services team members will work with your organization to define group member roles to help expedite your business processes. If this function is enabled, a new tab appears on each user’s **Properties** screen, allowing you to select the user’s group member role.

- If the setting is marked (on), group member roles are being used for this exchange.
- If the setting is unmarked (off), group member roles are not available for this exchange.

**Enable roles**

This section displays all the exchange roles that are available for users of this exchange. This section is informational only; the roles that appear here were selected on the template that was used to create the exchange and cannot be changed once the exchange has been created.

For more information about exchange roles, see “Users’ roles within an exchange” on page 46.

**Disallow concurrent logins**

This setting determines whether exchange users can log into Intralinks more than once simultaneously.

- If the setting is marked (on), users will be able to log into only one Intralinks session at any given time. (Note, however, that Intralinks administrators can override this setting for an individual user by changing a setting on the user’s profile screen.)
- If the setting is unmarked (off), users will be able to log into Intralinks more than once simultaneously using the same user ID and password.

**Removal options**

**User self remove option**

This setting determines whether exchange users can remove themselves from the exchange.

- If the setting is marked (on), users will be able to remove themselves from the exchange if they no longer plan to participate in it.
- If the setting is unmarked (off), users will not be allowed to remove themselves from the exchange, and the **Remove Me** option will not appear on the **Actions** menu in the **Hub** when this exchange is highlighted.
Send alerts to users who are removed from the exchange

This setting determines whether email alerts will be sent to exchange members who are removed from the exchange, to alert them that they have been removed.

• If the setting is marked (on), an alert will be sent to users when they are removed from the exchange.
• If the setting is unmarked (off), no alert will be sent to users when they are removed from the exchange.

Suppress remove me alert

This setting is used only in the creation of Intralinks Courier exchanges. It does not have any effect on your exchange and cannot be changed.

Alerts inbox

This field is used to define one or more “bcc:” addresses for your exchange. These addresses can be used to capture information for audit purposes. A copy of all alerts generated by the exchange, except for those related to password changes and those used for logging into exchanges with enhanced security, will be sent to this address. Individual users will not be made aware that their alerts have been sent to the bcc: address.

The addresses displayed in this field can be viewed, added, edited and deleted only by Intralinks employees.

Documents

Save deleted documents

The setting determines whether a deleted document is removed merely from view or is removed altogether from the Intralinks system. This setting must be marked if the people using your exchange will use the Historic Filter to view information about the documents that were available in the past.

• If this setting is unmarked (off), deleted documents are removed from the system and cannot be recovered. Both current and prior versions are deleted. Information about the documents (metadata), including the documents’ names, is retained, and reports for the documents continue to be available.
• If this setting is marked (on), deleted documents are hidden from view of most users but remain in the system. In this case, deleted documents can be viewed by users who had rights to modify the documents before they were deleted, but they cannot be updated or permissioned. Once deleted, documents cannot be “undeleted,” either by exchange users or Intralinks administrators. All reports for the deleted documents will continue to be available.
Automatically version modified documents

This setting determines whether each version of a document is retained as new updates to the document are posted. This can be useful for auditing and archiving purposes. This setting must be marked if the people using your exchange will use the Historic Filter to view information about the documents that were available in the past.

- If the setting is marked (on), a copy of every version of each document will be saved. All copies will be available for viewing.
- If the setting is unmarked (off), only the current version of each document is retained. Information about each version (who changed the document, and when) is retained.

Allow bulk downloading of documents

This setting determines whether exchange users are allowed to download more than one document at a time.

- If the setting is marked (on), users are allowed to download multiple documents.
- If the setting is unmarked (off), users can download only one document at a time.

Indexing

This setting determines whether folders and documents will be indexed automatically as they are added to the exchange. For more detailed information about indexing, see “Indexing folders and documents” on page 64.

- If the setting is marked (on), folders and documents are indexed automatically.
- If the setting is unmarked (off), folders and documents will not be indexed.

Effective date

This setting determines whether managers and publishers will be able to specify an effective date for each document added to the exchange.

- If the setting is marked (on), managers and publishers can specify effective dates for documents.
- If the setting is unmarked (off), managers and publishers cannot specify effective dates.

Naming rules

This setting determines whether you are allowed to use naming convention rules to ensure that document names on this exchange conform to your organization’s standard operating procedures.
You cannot change this setting; it must be changed by an Intralinks employee. If you wish to use naming conventions with this exchange, contact Intralinks Global Enterprise Services and request that the setting be changed for that exchange.

- If the setting is marked (on), naming conventions can be used to rename documents added or updated on this exchange.
- If the setting is unmarked (off), naming conventions are not used on this exchange.

Document ownership

This setting determines whether you can identify a particular user or exchange group as the owner of a document. If you use this function, document ownership information can be used to select documents used by business processes.

You cannot change this setting; it must be changed by an Intralinks employee. If you wish to specify owners for the documents on this exchange, contact Intralinks Global Enterprise Services and request that the setting be changed for that exchange.

- If the setting is marked (on), you can specify document owners on this exchange.
- If the setting is unmarked (off), document ownership is not used on this exchange.

Save deleted comments

Comments can be added to multi-task business processes and the business process instances created from them. This setting allows you to save a copy of these comments for audit purposes if they are deleted.

- If this setting is unmarked (off), deleted comments are removed from the system and cannot be recovered.
- If this setting is marked (on), deleted comments are hidden from view of most users but remain in the system. In this case, deleted comments can be viewed by users who had rights to view or participate in the conversations before they were deleted, but comments cannot have additions comments posted to them. Once deleted, documents cannot be “undeleted,” either by exchange users or Intralinks administrators. Reports for the deleted comments will continue to be available.

OCR (Optical Character Recognition)

This setting determines whether graphic images that contain text and PDFs created from images will be scanned by an optical character reader when they are uploaded to your exchange. This function allows users to find these documents using Intralinks Platform’s search tools. If you use this function, the text is attached to the scanned documents as metadata; the contents of the files are not changed in any way.
• If the setting is marked (on), PDF documents and graphic images that contain text will be scanned when they are added to your exchange, and this text will be made available to Intralinks Platform’s search engine.

• If the setting is unmarked (off), PDF documents and graphic images will not be scanned when they are uploaded.

**UK Full Text Searching (US Index)**

This setting allows users whose data is stored in the United Kingdom (the *geo specific mount point* setting is set to *uk*) to perform full-text searches of their exchanges based on an index that resides on Intralinks servers in the United States. This setting is set by Intralinks employees at the template level and can be ignored.

**Binder enabled**

This setting determines whether users will be allowed to specify a binder when creating or updating documents. Binders allow you to organize documents in different locations either within an exchange or across multiple exchanges.

• If the setting is marked (on), users can specify binders for the documents that they add or update.

• If the setting is unmarked (off), users cannot specify binders for their documents.

**Geo specific mount point**

This setting determines whether the data on this exchange is stored in the United States or in the United Kingdom. This option was set on the template used to create the exchange, and it cannot be changed for the exchange. File processing will be performed in the United States, but apart from temporary processing, UK-based documents will not be stored in the United States.

**Expand/collapse folders**

This setting determines whether *Expand All* and *Collapse All* links will appear above the folder list for this exchange. These links can be used as toggles to show only top-level folders or top-level folders and all the subfolders within them.

• If the setting is marked (on), the *Expand All* and *Collapse All* links will be displayed above the folder list.

• If the setting is unmarked (off), the *Expand All* and *Collapse All* links will not be displayed.

**Expand folders by default**

This setting determines whether top-level folders and all their subfolders are displayed in the folder list automatically when users select the *Documents* tab.

This setting is available only if the *Expand/collapse folders* setting is marked (on).
• If the setting is marked (on), top-level folders and all their subfolders are displayed automatically.
• If the setting is unmarked (off), only top-level folders are displayed.

Permissions & protections

Bulk permissioning: Remember selections for future documents and subfolders

This setting determines whether the permissions applied to a folder’s contents apply only to the current documents and subfolders within the selected folder, or to documents and subfolders added in the future, as well. In both cases, the permissions you set can be overridden for selected documents and subfolders.

You cannot change this setting; it must be changed by an Intralinks employee. If you wish to use folder-level permissioning with an existing exchange, contact Intralinks Global Enterprise Services and request that the setting be changed for that exchange.

• If the setting is marked (on), permissions will be remembered and applied to documents and subfolders that are added in the future, as well as to all content in the folder at the time permissions are applied.
• If the setting is unmarked (off), permissions will be applied only to the documents in the folder (and any subfolders) at the time of permissioning. Documents added in the future will not be permissioned automatically.

Allow Reviewers and Previewers to add documents to selected folders

This setting determines whether managers can give reviewers and previewers the ability to add documents to selected folders when the managers set permissions for those folders. This setting can be changed only by an Intralinks administrator.

• If the setting is marked (on), managers who are setting permissions for folders will have the option to allow reviewers and previewers to add documents to the selected folders. If the Remember selections for future documents and subfolders option also is marked (on), reviewers and previewers who have permission to add documents to a folder will be able to add documents to subfolders within that folder, as well. This can be overridden for each subfolder.

When reviewers and previewers add documents, they can send an email alert to other limited publishers with permission to the folder where the new documents are stored. Alerts are sent to all limited publishers with permission to the folder. Reviewers and previewers without limited publisher permission will not receive the alert.

• If the setting is unmarked (off), reviewers and previewers will not be able to add documents to the exchange.

Allow Reviewers and Previewers to create sub folders and add documents to selected folders

This setting determines whether managers can give reviewers and previewers the ability to add folders and documents to selected folders when the managers set
permissions for those folders. This setting can be changed only by an Intralinks administrator.

- If the setting is marked (on), managers who are setting permissions for folders will have the option to allow reviewers and previewers to add folders and documents to the selected folders. If the **Remember selections for future documents and subfolders** option also is marked (on), reviewers and previewers who have permission to add documents to a folder will be able to add documents to subfolders within that folder, as well. This can be overridden for each subfolder.

  When reviewers and previewers add documents, they can send an email alert to other limited publishers with permission to the folder where the new documents are stored. Alerts are sent to all limited publishers with permission to the folder. Reviewers and previewers without limited publisher permission will not receive the alert.

  Reviewers and previewers will be able to edit the name and set custom field values for the folders that they have created.

- If the setting is unmarked (off), reviewers and previewers will not be able to add folders and documents to the exchange.

### Allow Reviewers and Previewers to edit custom fields to selected folders

This setting determines whether managers can give reviewers and previewers the ability to edit custom field values for selected folders when the managers set permissions for those folders. This setting can be changed only by an Intralinks administrator.

- If the setting is marked (on), managers who are setting permissions for folders will have the option to allow reviewers and previewers to edit custom field values for the selected folders. Reviewers and previewers will not be able to change other folder attributes, such as the folder name. If users also are granted the ability to add subfolders to the selected folder, they will be able to set the values for those folders’ custom fields.

- If the setting is unmarked (off), reviewers and previewers will not be able to edit custom field values for folders.

### Permission by

#### Users & groups and Groups only

These settings determine whether permission to view, download and print documents can be assigned to individual users, as well as exchange groups. In this version of Intralinks Platform, the **groups only** setting is marked by default and cannot be unmarked.

### Disable “all participant” permission

This setting determines whether the All Current and Future Users group will be available for this exchange. The All Current and Future Users group provides you with an easy way to give all exchange users access to documents that do not require permissions controls.
Members of the All Current and Future Users group will be able to view documents, but will have no other capabilities. If you want specific users to be able to modify documents, you will have to give them permission to control the documents separately.

You cannot change this setting; it must be changed by an Intralinks employee. If you wish to disable (or re-enable) the setting for this exchange, contact Intralinks Global Enterprise Services and request that the setting be changed.

- If the setting is marked (on), the All Current and Future Users group is disabled, and is not available for use.
- If the setting is unmarked (off), the group is available for use.

Disallow reviewers to see document creation and modification dates

This setting determines whether users can view the date and time each document was added to the exchange, as well as the date and time that it most recently was updated.

- If the setting is marked (on), reviewers and previewers will not see date and time information for documents.
- If the setting is unmarked (off), reviewers and previewers will see date and time information.

Disallow reviewers to see document creator’s and modifiers’ names

This setting determines whether users can view the name of the people who added or updated each document on the exchange.

- If the setting is marked (on), reviewers and previewers will not see the names of people who have added or updated documents.
- If the setting is unmarked (off), reviewers and previewers will be able to see these names.

Enable protection of PDF and Microsoft Office documents

This setting determines whether exchange managers or publishers who add documents to the exchange can apply various types of protection to them. This includes requiring users to enter their email address and password before viewing documents and preventing users from printing protected documents. Documents in PDF (Portable Document Format) and Microsoft Word, Excel and PowerPoint documents can be protected.

- If the setting is marked (on), document protection can be applied to PDF and Microsoft Office documents.
- If the setting is unmarked (off), document protection functions are not available on this exchange.
Disallow use of Print Screen

This setting is available only if enable protection of PDF and Microsoft Office documents is marked.

- If the setting is marked (on), users cannot use the Print Screen button while viewing this exchange.
- If the setting is unmarked (off), users are allowed to use the Print Screen button to capture images of this exchange and its contents.

Bind users’ Intralinks ID to first computer used to view protected PDFs and Office documents on this exchange

This setting is available only if enable protection of PDF and Microsoft Office documents is marked. This setting determines whether exchange users will be able to work with protected documents on more than one computer, or only on a single computer.

- If the setting is unmarked (off), users will be able to view protected documents on any computer that they may use to access this exchange.
- If the setting is marked (on), users will be able to view protected documents on only one computer — the first computer they use to access a protected document on this exchange.

Plugin-free IRM protection

This setting can be changed only by an Intralinks administrator. Once this setting is marked, it cannot be unmarked.

This setting determines whether Intralinks’ plugin-free solution will be used to protect Microsoft Office and PDF (Portable Document Format) documents.

- If the setting is unmarked (off), users will have to install a plugin before viewing protected Microsoft Office and PDF documents. Please note that the plugin-based solution will be retired on June 30, 2016, and plugin-free IRM must be used after that date if you intend to protect documents in this exchange.


- If the setting is marked (on), users will be able to view protected documents without first installing a plugin. Protected documents can be viewed on Windows and Macintosh computers. Encryption is based on Microsoft Windows’ native Rights Management technology.
Watermarking

Watermark PDFs using

This setting determines whether PDF documents that are viewed or downloaded will be stamped with a watermark containing the exchange user’s name and organization, the date and time the document was viewed, and other text, such as “Confidential” or “Final.” You can choose to apply watermarks only to protected PDF documents or to all PDFs.

- If the setting is unmarked (off), no watermarks are applied to documents.
- If the setting is marked (on) and watermarking is selected for all PDF documents, watermarks will be applied to all PDF documents on this exchange.
- If the setting is marked (on) and watermarking is selected for protected PDF documents only, watermarks will be applied to protected PDF documents on this exchange. If this setting combination is chosen, the *enable protection of PDF and Microsoft Office documents* setting must be marked, as well.

You can select the information that will appear in watermarks.

**User name**

Mark this option if you want the name of the person who viewed or printed the document to appear in the watermark.

**Host organization name**

Mark this option if you want the name of your organization to appear in the watermark.

**Download timestamp**

Mark this option if you want the time the document was downloaded to appear in the watermark. The time displayed is North American Eastern Time (ET).

**Text label**

If you want an additional text label, such as “Confidential” or “Draft,” to appear in the watermark, mark this option, then select the text label you want. If the label you want does not appear in the list, select *use typed in text* and then enter the label in the box below the text label list.

**Document title**

You can include the document name in the watermark. If the document name is too long to fit on a single line, it will be wrapped to a second line. (Any part of the name that exceeds two lines will not be included.)

**Index number**

If your exchange uses index numbers, mark this option to include the document’s index number in the watermark.
Color
You can select to display watermarks in one of the following colors: red, green, gray, blue, black, brown.

Intensity
You can select the intensity, or opaqueness, with which watermarks will be displayed on your documents. Select from five levels; Level 1 is the lightest, and Level 5 is the darkest, or most opaque.

Position
You can select to display watermarks diagonally across each page, in the header and footer of each page, in each corner of each page, or any combination of these selections.

Watermark protected Office files
This setting determines whether Microsoft Word, Excel and PowerPoint documents that are printed will be stamped with a watermark containing the exchange user’s email address and the date and time the document was printed.

- If the setting is unmarked (off), no watermarks are applied to Microsoft Office documents.
- If the setting is marked (on), watermarks will be applied to all Office documents on this exchange.

You can select the information that will appear in watermarks.

User email address
Mark this option if you want the email address for the person who printed the document to appear in the watermark.

View timestamp
Mark this option if you want the time the document was printed to appear in the watermark. The time displayed is North American Eastern Time (ET).

Position
You can select to display watermarks diagonally across each page, in the header and footer of each page, or both across the page and in the header and footer of each page.
Appendix B: Data limits

Use the tables below to determine the recommended limits for information that is stored and functions that are performed on your exchanges. These are the recommended guidelines for best performance only; you can exceed these limits (except where noted) but you may find that Intralinks Platform’s responsiveness is affected if you do.

Documents

<table>
<thead>
<tr>
<th>Item</th>
<th>Limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of documents recommended</td>
<td>20,000</td>
<td>Exceeding this limit will impact performance of advanced reports and exports, DVD archives, smart filters. Performance will degrade as the number of documents increases; users may experience failures or timeouts.</td>
</tr>
<tr>
<td>Number of documents recommended in a single folder</td>
<td>1,000</td>
<td>Performance of folder navigation will slow as the number of items in the folder increases.</td>
</tr>
<tr>
<td>File size limit recommended</td>
<td>2047 MB</td>
<td></td>
</tr>
<tr>
<td>PDF watermarking</td>
<td>200 MB</td>
<td>Watermarking PDF documents is supported for files up to 200 MB.</td>
</tr>
<tr>
<td>Protected PDF documents</td>
<td>500 MB</td>
<td>Document protection is supported for files up to 500 MB.</td>
</tr>
<tr>
<td>Protected Microsoft Office documents</td>
<td>150 MB*</td>
<td>IRM protection is supported for files up to 150 MB. *(IRM protection is supported for Excel files with the .xls extension up to 40 MB.)</td>
</tr>
<tr>
<td>Total size of documents recommended</td>
<td>40 GB</td>
<td>It is possible to have more than 40 GB of documents, but DVD archives may be impacted.</td>
</tr>
</tbody>
</table>

Folders

<table>
<thead>
<tr>
<th>Item</th>
<th>Limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of folders recommended</td>
<td>10,000</td>
<td>Advanced reports and exports will be affected if this limit is exceeded. Performance degrades as the number of documents increases; users may experience failures or timeouts.</td>
</tr>
<tr>
<td>Number of top-level folders recommended</td>
<td>200</td>
<td>The time required to open an exchange from the Hub increases as the number of top-level folders increases.</td>
</tr>
</tbody>
</table>
### Users

<table>
<thead>
<tr>
<th>Item</th>
<th>Limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of users recommended in an exchange</td>
<td>5,000</td>
<td>Performance of user-based functions (document access reports, users &amp; groups smart filters, etc) degrades as the number of users increases.</td>
</tr>
<tr>
<td>Number of users in a group</td>
<td>2,500</td>
<td></td>
</tr>
</tbody>
</table>

### Groups

<table>
<thead>
<tr>
<th>Item</th>
<th>Limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended number of groups</td>
<td>2,500</td>
<td>User of advanced reports and DVD archives will be affected if this limit is exceeded. Performance degrades as the number of groups increase.</td>
</tr>
</tbody>
</table>

### Business processes

<table>
<thead>
<tr>
<th>Item</th>
<th>Limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules-based document distribution business processes</td>
<td>500</td>
<td>No more than 500 groups can be configured as recipients for rules-based document distribution business processes.</td>
</tr>
</tbody>
</table>

### Compliance

<table>
<thead>
<tr>
<th>Item</th>
<th>Limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>7,500</td>
<td>The maximum number of users for a monitored domain is 7,500.</td>
</tr>
</tbody>
</table>

### Bulk operations

<table>
<thead>
<tr>
<th>Item</th>
<th>Limit</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Permissions | 125,000 | Setting permissions in bulk should be limited to 125,000 permission records at a time (the total number of documents multiplied by total number of groups). If this limit is exceeded, the following operations will be affected:  
  - Permission Overview  
  - Set Folder Permissions  
  - Copy Group Permissions |
Folder permissions: 100,000. We recommend that you set permissions in bulk for no more than 100,000 permission records at a time (the total number of documents multiplied by total number of groups). If this limit is exceeded, the following operations will be affected:
- Set Folder Permissions
- Copy Group Permissions

Bulk deletion of documents: 6,000.

Bulk deletion of folders: 2,000.

Copy/paste: 20,000. Total of folders and documents should be less than 20,000.

Alerts: 5,000. Alerts for 1,000 documents can be sent to 5,000 users.

**Multi-file Uploader**

<table>
<thead>
<tr>
<th>Item</th>
<th>Limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of groups in an exchange</td>
<td>100</td>
<td>This limit applies to reviewers who are allowed to add files to a folder using Multi-file Uploader. Performance improvements are planned for future releases.</td>
</tr>
<tr>
<td>File size</td>
<td>2 GB</td>
<td></td>
</tr>
</tbody>
</table>

**Download Wizard**

<table>
<thead>
<tr>
<th>Item</th>
<th>Limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of files per download (.NET/FFClickOnce version)*</td>
<td>40,000</td>
<td>Expected download rate of 1 GB/hour with good network connection</td>
</tr>
<tr>
<td>Total size of download (.NET/FFClickOnce version)*</td>
<td>6 GB</td>
<td></td>
</tr>
<tr>
<td>Total number of files per download (Silverlight version)</td>
<td>2,000</td>
<td></td>
</tr>
<tr>
<td>Total size of download (Silverlight version)*</td>
<td>500 MB</td>
<td></td>
</tr>
</tbody>
</table>
*The .NET version is used automatically if you are using Internet Explorer and the Microsoft .NET Framework. If you are using a Windows-based browser other than Internet Explorer (for example, Firefox), you may be able to install a browser plugin such as FFClickOnce that allows your browser to communicate with .NET Framework. Other users must use a version of Download Wizard that is based on Microsoft Silverlight; that version requires no plugin, but has less robust capability.

### Intralinks Viewer

<table>
<thead>
<tr>
<th>Item</th>
<th>Limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>File size limit for PDF documents</td>
<td>200MB</td>
<td></td>
</tr>
<tr>
<td>File size limit for Microsoft Excel files</td>
<td>40MB</td>
<td>Excel files that contain up to 100 worksheets and 65,000 rows can be viewed using Intralinks Viewer.</td>
</tr>
<tr>
<td>File size limit for Microsoft Word files</td>
<td>40MB</td>
<td></td>
</tr>
</tbody>
</table>
Index

A
Access Report 36
   by Exchange/Group 191
   by Exchange/Group/User 191
   by User 191
acknowledgment responses
   configuring 141
acknowledgment responses for distributed documents 168
   resubmitting 170
Activity Summary Report
   exporting and printing 189
Add Group Wizard 42
Add Users Wizard 48
Adobe
   Acrobat Professional 179
   Flash Player 41, 60, 117, 146, 161, 181
   Reader 7, 8, 179
      using Intralinks Viewer as an alternative 114
alerts
   adding notes 23
   custom
      exchange setting 199
   enabling welcome to exchange alerts 194
   exchange settings 203
   for multi-task processes 149
      Due Date Approaching alert 150
   Overdue alert 150
   preferences 14
   sending for documents 84
   sending to multiple addresses 14
alerts inbox
   exchange setting 203
All Users - Current and Future option 62, 70, 73, 83, 103
   exchange setting 208
Android
   allowing access on 39
Answer Library 18
   training videos 18
apps, mobile
   allowing access on 39
   allowing users to view protected documents 39
archive copies
   compliance 35
   data 35
   ordering 34
assignments
   viewing tasks assigned to you 162
audit controls
   capturing alerts sent by Intralinks 203
automatic logout
   exchange setting 196
autopublishing
   configuring 137, 142
   enabling for a business process 128

B
binders
   associating with a document 67
   creating 67
   exchange setting 206
browser requirements 7, 8
bulk downloading 110
   enabling 204
bulk permissioning
   enabling 207
business group 20
   creating 20
   membership levels 20
business process definitions
   defined 117
business process instances
   defined 117
   Process Access Report for business process instances 192
   renaming 171
business processes 117
   activating 143
   co-monitors 171
   copying from one exchange to another 145
   creating and configuring group-triggered document distribution 138
   creating and configuring rules-based document distribution 133
   creating and configuring rules-based submission 127
   defined 117
   deleting 143
document date trigger 118
document submission for approval 118
document submission for review 119
document submission with two-step approval 119
document submission without any approval 119
draft mode 121
enabling 195
inactivating 143
managing 173
multi-task processes 146
activating 156
configuring 147
deleting 156
inactivating 156
reactivating 156
renaming 158
updating 158
Process Definition Summary Report 193
Process Monitor 172, 173
reactivating 143
renaming 144
request for documents 119
submitting and approving documents 161
viewing 172
business processes, see also multi-task processes
buyer groups
- enabling 201

C
challenge question 12
checking out documents 86
Chrome (browser) 7, 8
collaboration groups
- analyzing exchange usage 186
- defined 42
- exchange activity report 189
- exporting a list of members 44
- exporting group history to Excel 45
- filtering 58
- finding 58
- moving users from one group to another 53
- properties
  - modifying 44
  - viewing a list of members 44
  - viewing group history 45
colleagues
- adding to your exchange 16
comments
- for tasks 176
co-monitors
- adding 171
- defined 171
compliance reporting
- maximum users per monitored domain 214
concurrent logins
- allowing 202
contact details
- editing 14
Copy Group Permissions screen 76, 98
curtain (Intralinks Viewer) 115
custom alerts
- exchange setting 199

custom fields
- activating 33
- adding 31
- adding to documents 69
- adding to folders 61
- allowing reviewers and previewers to edit 91, 208
- changing options lists 31
- defining 30
- disabling 32
- enabling 32, 195
- enabling advanced access reports 190
- field types 29
- modifying
  - restrictions 30
- publishing 33
- renaming 30
- setting default values and access rights 33
- setting up 29
- types 31
- users who are allowed to set custom fields 29
- using in naming conventions 89
- viewing 30

dashboard 12
data
- storing in the United States or Europe 206
data entry limits 213
date-triggered business processes 118
digital rights management
  - for PDF documents 209
Document Access Report 182
document distribution business processes 133, 138
Document List 182
- printing 182
document locking and protection 93
- capabilities 93
- changing protection settings 95
- defined 93
document ownership 69, 71
- exchange setting 205
document placeholders
adding 66
    replacing with a document 71
document submission business processes
127
document submission for review (business process) 119
document submission without any approval (business process) 119
document tags, see tags documents
Access Report
    by Exchange/Group 191
    by Exchange/Group/User 191
    by User 191
acknowledging
    resubmitting 170
adding 66
adding multiple 72
alerting users 70
allowing reviewers and previewers to add
    62, 63, 78, 80, 81, 82, 91, 101, 102, 207
    recommended limit 215, 216
approving 165, 167
asking for resubmission 165, 167
assigning tags 68
associating with a task 175
automatically applying permissions 79, 100
auto-versioning 204
binders
    enabling 206
changing protection settings 95
checking out and in 86
copying and pasting
    recommended data entry limits 215
    using working sets 86
deleting 85, 183
    recommended data entry limits 215
distributed, acknowledging 168
Document Access Report 182
document links (URLs) 108
document usage report (Folder Coverage) 184, 187
document usage report (Group Coverage) 186
document usage report (User Activity by Group) 184
document usage report (User Coverage) 185
downloading 110
downloading from multiple exchanges 111
downloading multiple 110
effective date 67
    enabling 204
entering custom fields 69
favorites 109
freezing and unfreezing 65
indexing 64
list of folders and documents 182
lock icon 113
locking 86
moving 83
    in a frozen exchange 65
naming 67
overriding automatically applied permissions 81, 102
ownership 69, 71
    exchange setting 205
permissioning to all users 70, 83, 103
placeholders 66
printer icon 113
printing 112
printing all 112
protected 113
protecting 93
recommended file size limit 213
recommended file size limit per exchange 213
recommended limit per exchange 213
recommended limit per folder 213
rejecting 165, 167
renaming using naming conventions 87, 204
    identifying a document's original name 88
replacing 75
replacing a document placeholder 71
reports 181
requesting 166, 171
resubmitting using Intralinks 164
reviewing and modifying permissions 75, 97
saving deleted documents 203
searching for 105
searching for across multiple exchanges 107
setting permissions 69, 97
setting properties 67
setting protections 63, 70, 74, 81, 102
smart filters 109
submitting 162
submitting and approving 161
submitting via fax 163, 175
uploading and associating with tasks 174, 175
viewing 104
viewing by effective date 107
viewing deleted 183
viewing in Intralinks Viewer 114
viewing new 105
viewing unread
  Advanced Filter 106
  watermarking 211, 212
Download Wizard 111
  recommended limits 215
downloading documents 110
  preventing 63, 70, 74, 81, 93, 102
Due Date Approaching alert (multi-task process) 150
DVD archive copies
  ordering 34

E
effective date 67
  enabling 204
  using to find documents 107
eForms 129, 136, 179
  creating 179
  exchange setting 198
  requirements and prerequisites 179
  using with business processes 179
email address (user ID) 11
email alerts
  adding notes 23
  configuring for a business process 140
  sending for documents 84
enhanced security 12
  enabling access to 196
Excel 76, 98
  exporting a list of exchange users 183
  exporting a list of removed users 55
  exporting a list of user group members 44
  exporting group history 45
exporting reports
  Exchange Activity Summary Report for groups 189
  Exchange Activity Summary Report for users 189
  Exchange Statistics Summary Report 190
Folder Coverage 184, 187
Group Coverage 186
Search Summary 187
User Activity by Group 184
User Coverage 185
protected documents 113
  performing ad hoc analysis 114
  size limit for protected documents 213
Exchange Activity Summary Report
  exporting and printing 189
exchange groups
  analyzing exchange usage 186
defined 42
  enabling 201
  exchange activity report 189
  exporting a list of members 44
  exporting group history to Excel 45
  filtering 58
  finding 58
  Group Coverage Report 186
  moving users from one group to another 53
properties
  modifying 44
  viewing a list of members 44
  viewing group history 45
exchange ID
  viewing 38
exchange roles 10
  changing 54, 55
  changing for multiple users 54
  manager roles 46
  publisher roles 47
  reviewer roles 46, 47
  roles enabled for this exchange 202
exchange settings 194
  changing 25
  session inactivity timeout setting 196
  viewing 24
Exchange Statistics Summary Report
  exporting and printing 190
exchange users
  adding 48
  adding without an email address 49
  assigning to another user group 53
  changing exchange roles 54
    for multiple exchanges 55
  definition 19
  exchange roles 46
  finding 58
  importing from another exchange 48
  removing from an exchange 45, 55
    exporting a list of removed users 55
    viewing a list of removed users 55
exchanges
  activity report 188
  changing phase 24
  copying 21
  creating 21
  creating a footer 22
  creating a splash screen 22
data
  storing in the United States or Europe 206
definition 9
deleting 34
freezing and unfreezing 65
hold phase 24
host organization
  viewing 38
life cycle 19
open phase 24
ordering archive copies 34
  phase
  viewing 38
  preparation phase 24
removing yourself 16
settings 19–37
templates 21
viewing details 38
experts (Q&A)
  SME coordinators
  enabling 200
exporting
  permissions information 76, 98
  user lists 183

F
Favorites folder 109
Favorites menu 110
fax cover sheets
  printing 163, 175
fax-in
  enabling for a business process 128
faxing documents 163, 175
field types
  for custom fields 29
fields, custom
  adding to documents 69
  adding to folders 61
filters 58, 109
  Advanced Filter 106
  Historic Filter 106
Firefox 7, 8
Folder Coverage report 184, 186, 187
folders
  allowing reviewers and previewers to add
    91, 207
  copying and pasting
    recommended data entry limits 215
  creating 60
  deleting 66
    recommended data entry limits 215
  entering custom fields 61
Folder Coverage report 184, 187
freezing and unfreezing 65
indexing 64
indexing an existing folder 64
list of folders and documents 182
moving 65
  in a frozen exchange 65
naming 61
organizing 64
permissioning to all users 62, 73
permissions, setting for documents and
  subfolders
  recommended limits 215
  recommended total number per ex-
  change 213
setting permissions for documents and
  subfolders 76, 98
smart filters 109
subfolders 61
top-level 61
User Activity by Group report 184
footer 22
  creating or modifying 22
freezing exchanges 65
FTP archive copies
  ordering 34

G
geo specific mount point 206
Global Enterprise Services 147
Global User Directory (GUD) 48
Google Chrome 7, 8
graphics
  OCR
    making graphics searchable 205
Group Coverage Report 186
group member roles 44, 48
group membership roles
  exchange setting 201
groups
  adding 42
  All Users - Current and Future option 62,
    70, 73, 83, 103
  analyzing exchange usage 183, 186
  applying one group’s permissions to an-
  other group 76, 98
  automatically applying permissions 79,
    100
collaboration groups
  defined 42
copying groups 57
  using working sets 57
enabling 201
exchange activity report 189
exchange groups
  defined 42
exporting a list of members 44
exporting group history to Excel 45
filtering 58  
finding 58  
Folder Coverage report 184, 187  
Group Coverage report 186  
moving users from one group to another 53  
overriding automatically applied permissions 81, 102  
Process Access Report for groups 192  
properties  
modifying 44  
recommended total number per exchange 214  
removing 45  
setup 41–45  
User Activity by Group report 184  
user groups  
defined 41  
viewing a list of members 44  
viewing group history 45  
group-triggered document distribution business processes 138

Intralinks Designer  
enabling access to 196  
starting 52, 87  
using to copy exchanges 21  
using to import information 51, 87  
Intralinks ID 11  
Intralinks Viewer 114  
enabling 25  
printing documents 115  
iPad  
allowing access on 39  
iPhone  
allowing access on 39  
IRM (Information Rights Management) 113  
capabilities 93  
defined 93  
performing ad hoc analysis on protected Excel documents 114

H  
help  
Answer Library (knowledgebase) 18  
training videos 18  
help system 18  
Hidden Manager Plus exchange role 46  
Historic Filter 106  
setting up 203, 204  
hold phase 24  
host organization  
viewing 38  
HTML alerts  
preference 14  
Hub  
using to add users 50  

K  
key contacts  
changing 54, 55  
definition 54  
removing 54, 55  
knowledgebase 18  

L  
limited publisher 62, 63, 78, 79, 80, 81, 82, 91, 101, 102  
limits  
for data entry 213  
lock icon on documents 113  
locking documents 86  
locking exchanges, see freezing exchanges  
logging in 10–14  
allowing concurrent logins 202  
logging in the first time 11  
logging out 16  
lost password 13  
resetting using email 14  
resetting using SMS 14  

M  
Macintosh  
system requirements 8  
Manage Exchanges wizard 55  
Manager exchange role 47  
Manager Limited exchange role 47  
Manager Plus exchange role 46  
managers 46  
exchange role 10, 46
Microsoft Excel 76, 98
exporting a list of exchange users 183
exporting a list of removed users 55
exporting a list of user group members 44
exporting group history 45
exporting reports
Exchange Activity Summary Report for groups 189
Exchange Activity Summary Report for users 189
Exchange Statistics Summary Report 190
Folder Coverage 184, 187
Group Coverage 186
Search Summary 187
User Activity by Group 184
User Coverage 185
protected documents 113
performing ad hoc analysis 114
viewing documents in Intralinks Viewer 114
Microsoft Internet Explorer 7, 8
Microsoft Office
protected documents 113
Microsoft Office documents protecting
size limit 213
Microsoft PowerPoint
protected documents 113
Microsoft Windows
system requirements 7
Microsoft Word
protected documents 113
mobile apps
allowing access on 39
allowing users to view protected documents 39
mobile phones
registering 15
Multi-file Uploader 72
recommended limits 215, 216
multi-task processes 146, 156
alerts 149
Due Date Approaching alert 150
Overdue alert 150
configuring 147
deleting 156
inactivating 156
managing 173
owners 149
Process Monitor 172, 173
reactivating 156
renaming 158
target groups 147
tasks 150
updating 158
uploading documents 174, 175
viewing 172
Multi-user Coverage Report 185
my profile screen 14

N
naming conventions
character limits 89
elements 89
exchange setting 204
using custom fields 89
naming conventions (documents) 87
activating 90
copying 90
creating 88
deactivating 90
New Document Wizard 66

O
OCR
exchange setting 205
one-time password 12
open phase 24
operating system 7, 8
optical character recognition
exchange setting 205
Overdue alert (multi-task process) 150
overriding folder-level permissions 81, 102
owners
documents
exchange setting 69, 71, 205
multi-task processes 149

P
password
changing 13
entering a one-time password 12
exchange settings
password complexity 197
requiring a password for PDF and Office documents 209
rules for creating complex passwords 198
rules for creating normal passwords 197
setting the expiration timeframe 198
resetting a lost password 13
using email 14
using SMS 14
using text messages (SMS) 15
PDF documents
   enabling PDF protection 209
OCR
   making PDFs searchable 205
   protecting
       size limit 213
   viewing in Intralinks Viewer 114
   watermarking 211, 212
       size limit 213
performance
   data entry limits 213
permissioning users to documents 69, 97
   permissions 69, 97
       applying one group’s permissions to another group 76, 98
       automatically applying to documents 79, 100
   document-level permissioning 77, 99
   enabling bulk permissioning 207
   folder-level permissioning 79, 100
       overriding 81, 102
   overriding automatically applied permissions 81, 102
   permissioning a document to all users 83, 103
   recommended data entry limits 214
   reviewing and modifying 75, 97
   setting for all the documents in a folder 76, 98
   recommended limits 215
Permissions Overview screen 75, 97
   using to set document protections 95
personalizing Intralinks 14
phases, exchange 24
placeholder users 49
plain-text alerts
   preference 14
PowerPoint
   protected documents 113
   size limit for protected documents 213
preferences
   updating 14
preparation phase 24
Previewer exchange role 47
previewers 47
   allowing previewers to add documents 62, 63, 78, 80, 81, 82, 91, 101, 102, 207
   recommended limit 215, 216
   allowing previewers to add folders 91, 207
   allowing previewers to edit custom fields for folders 91, 208
setup 209
Print Screen
   blocking use of 210
printer icon on documents 113
printing 112
   fax cover sheets 163, 175
   preventing 63, 70, 74, 81, 93, 102
Process Access Report
   for business process instances 192
   for groups 192
   for users 192
Process Definition Summary Report 193
processes, see business processes or multi-task processes
profile 11
   challenge question 11
   sharing profile information with others 12
   sharing with others 14
   updating 14
protected documents
   allowing users to view on mobile apps 39
   public (shared) working sets 37
   adding users 37
   removing users 38
Publisher exchange role 47
Publisher Plus exchange role 47
publishers 47
   exchange role 10, 46
Q
Q&A
   collaboration groups
      defined 42
   SME coordinators
      enabling 200
R
Reader (Adobe) 7, 8
   recommending other users 16, 52
registering a mobile phone 15
Remove Me command 202
   removing 202
   removing yourself from an exchange 16
reports
   Access Report by Exchange/Group 191
   Access Report by Exchange/Group/User 191
   Access Report by User 191
   Document Access Report 182
   Document List 182
   Exchange Activity Summary Report 188
   Folder Coverage 186
   for user groups 183
   Group Coverage 186
Multi-user Coverage 185
Process Access Report
  for business process instances 192
  for groups 192
  for users 192
Process Definition Summary Report 193
Search Summary Report 187
User Activity by Group 184
request for documents (business process) 119
requirements
  Macintosh 8
  Windows 7
resubmitting documents 164
Reviewer exchange role 47
Reviewer Plus exchange role 47
reviewers 47
  allowing reviewers to add documents 62, 63, 78, 80, 81, 82, 91, 101, 102, 207
  recommended limit 215, 216
  allowing reviewers to add folders 91, 207
  allowing reviewers to edit custom fields for folders 91, 208
  exchange role 10, 46
  setup 209
roles, see exchange roles and group member roles
rules-based document distribution business processes
  creating and configuring 133
  recommended recipient group limit 214

S
Safari 7
saving (downloading) documents
  preventing 63, 70, 74, 81, 93, 102
screen resolution
  Macintosh 8
  Windows 7
search
  adding tags to documents 68
  Boolean, advanced 108
Search Summary Report 187
search tool 105
  tips 108
searching documents
  enabling 194
security 9, 11
  document protection 63, 70, 74, 81, 93, 102
  exchange settings 196, 209–212
security codes
  receiving by text message (SMS) 15
session inactivity timeout
  exchange setting 196
Set Folder Permissions screen 77, 79, 99, 100
settings, exchange 194
  changing 25
  viewing 24
setup
  exchanges 19–37
  user groups 41–45
Single Sign-On (SSO) 10, 11, 12, 13
smart filters 58, 109
SME coordinators
  enabling 200
special characters
  in searches 109
splash screen 22
  creating or modifying 22
Spotlight (Intralinks Viewer) 115
SSO, see Single Sign-On (SSO)
standard operating procedures
  standardizing document names 87
statistics
  viewing for users and documents 190
subfolders
  defined 61
submitting documents 162
system requirements
  Macintosh 8
  Windows 7

T
tag sets
  deleting 28
  renaming 28
tags 27
  activating 29
  adding 28
  adding to documents 68
  deleting 28
  enabling 195
  publishing 29
  renaming 28
  viewing 27
target groups
  for multi-task processes 147
tasks
  comments 176
  for multi-task processes 150
  managing 173
  renaming 171
  viewing 172
  viewing your assignments 162
Tasks List 162
templates
creating 20
defining for exchanges 21
settings 194
time zone
selecting 14
timeout (session)
exchange setting 196
top-level folders
defined 61
training videos 18
troubleshooting
data entry limits 213
using the Answer Library 18

U
UK full text search exchange setting
searching documents
enabling for UK-based exchanges 206
unfreezing exchanges 65
URLs
for documents 108
User Activity by Group Report 184
User Activity by Group report 184
User Coverage report 185
user groups
see also buyer groups, collaboration
groups, exchange groups
adding 42
analyzing exchange usage 183
defined 41
exporting a list of members 44
exporting group history to Excel 45
Folder Coverage report 184, 187
Group Coverage Report 186
Group Coverage report 186
moving users from one group to another
53
properties
modifying 44
recommended total number per ex-
change 214
removing 45
setup 41–45
User Activity by Group report 184
viewing a list of members 44
viewing group history 45
user ID 11
user lists
exporting and printing 183
user profile 11
challenge question 11
sharing profile information with others 12
sharing with others 14
updating 14
users
accepting and rejecting requests to add
users 53
adding 48
adding from the Hub 50
adding to a public working set 37
adding without an email address 49
alerting 70
alerting removed users 203
analyzing exchange usage 184, 185,
186
assigning to another user group 53
changing exchange roles 54, 55
changing roles 54
definition 19
exchange activity report 189
exchange roles 46
finding 58
Folder Coverage report 184, 187
Group Coverage report 186
importing from another exchange 48
Process Access Report for users 192
recommended total number per ex-
change 214
recommended total number per group
214
recommending 16
removing from a public working set 38
removing from an exchange 45, 55
exporting a list of removed users 55
viewing a list of removed users 55
requesting that another manager add us-
ers 52
reviewing and modifying permissions 75,
97
User Activity by Group report 184
User Coverage report 185

V
videos
training 18
viewpoint
in archive copies 34

W
watermarking
Microsoft Office files 212
PDF documents 211
size limits for watermarked documents
213
web browser requirements 7, 8
welcome to exchange alerts
   enabling 194
wildcards
   in searches 109
Windows
   system requirements 7
Word
   protected documents 113
   size limit for protected documents 213
workflows, see business processes
working sets
   adding items to an existing set 36
   creating 36
   enabling for a business process 128
   public (shared) working sets 37
   removing 37
   using to copy documents 86
   using to copy groups 57
   using to view the access reports 191