Intralinks VIA® Pro for the Web

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

Monitoring Intralinks VIA® Pro user accounts

If you have been given compliance officer capabilities in Intralinks VIA Pro, you can generate and view reports that allow you to monitor the flow of information within and from your organization, as well as individual and aggregate usage information. You also will be able to view information about business group members and policies, but you cannot make changes to these areas unless you have also been given administrator privileges for your organization.

In many organizations, the compliance officer role and the administrator role may be performed by a single person. To learn more about the administrator role, see the *Intralinks VIA Pro Administrator Guide*.

Getting started

Requirements

In order to use Intralinks VIA Pro for the Web, you must have one of the following browsers:

- Google Chrome (latest version, automatically installed by Google if you use Chrome)
- Firefox (latest version)
- Safari 6.1 or later (Macintosh only)
- Microsoft Edge (latest version)

For an optimal viewing experience, we recommend that you use Chrome, Firefox or Safari.

Activating your Intralinks account

If you are a new user to Intralinks, that is, you have not activated an Intralinks account, when you are invited to VIA Pro, you will receive an email message from Intralinks with a link to activate your account.

1. In the email, click **Activate Account**.
2. Read the license agreement and click **Accept** to continue logging in.
3. Enter then reenter your password and click **Next**.
4. Set up how you want Intralinks to verify your identity by setting up one or more of the following options:
   - **Receive a code by text (SMS)** - Select the country and enter the phone number to which you want an SMS code to be sent and click Activate.
   - **Use Intralinks Authenticator** – Use your phone to scan the QR code or enter the secret key displayed in this dialog box in the Authenticator section in the Intralinks Mobile app on your phone. Click the icon at the end of the secret code to copy the code. In the **Verification code** field, enter the 6-digit code generated by the app and tap **Activate**.

     Note: This option cannot be used with Okta Verify with Push.
   - **Okta Verify with Pus** - Okta Verify with Push eliminates the need to enter a code. Instead, it sends a push verification to your phone and you must tap **Yes, it's me** to authenticate. Use your phone to select the type of account and scan the QR code in this dialog box in the Okta Verify App on your phone.

     This option requires that you phone be connected to

the internet. If your phone does not have an internet connection, you can choose to verify using a code and you will be enrolled in Okta Verify.

Note: This option cannot be used with Intralinks Authenticator.

- **Use your preferred authenticator** - Scan the QR code or enter the secret key displayed in this dialog box in the Authenticator App on your phone. Click the icon at the end of the secret code to copy the code. In the **Verification code** field, enter the 6-digit code generated by the app and tap **Activate**.

5. When you are done, click **Finish**.

Logging in after your have activated your account

1. Point your browser to: https://via.Intralinks.com.
2. Enter your email address and click **Next**.
3. Enter your password and click **Login**.
4. If you are asked to verify your identity, either enter the security code in the **Verification Code** field and click **Next**, or tap **Yes, it's me** in your Okta Verify app. The security code is sent based on the method you selected when you activated your account.

The security verification is triggered based on the result of evaluating security behavior and risk-based authentication, referred to as adaptive authentication. Security behavior detection continually tracks specific user behavior and generates a challenge when any change in the tracked history of behavior for a given user is detected, such as a new device that has never been used or a new geographic location from which the user has never logged in to Intralinks.

Risk-based authentication is an additional layer of security that evaluates risk automatically using multiple features such as IP address, device, and behaviors for each user attempting to authenticate. Risk-based authentication is done with security behavior detection.

The **Workspaces** view appears. (The Intralinks VIA Pro administrator role does not include the ability to create Workspaces. If your only responsibility with Intralinks VIA Pro is to act as administrator, no Workspaces will be displayed.)

Resetting your authentication factors after your mobile phone number has changed

If you are enrolled in SMS as one of your authentication factors, you can update your phone number and authentication factors when your mobile phone number changes. If you are not enrolled in SMS, contact Intralinks Customer Support.

1. When you are asked to verify your identity when logging in, click **Update phone number used for SMS**.
2. In the **Country Code** field, select the country code of your old phone.

3. In the **Phone Number** field, enter your old phone number.
4. Click **Validate**.

   If you enter the correct phone number, an email is sent to you with a code that you can use to reset your authentication factors. This code is good for ten minutes.

   If you enter an incorrect phone number five times, you will be locked out. Contact Intralinks Customer Support.
5. In the **Code** field, enter the code that was sent to you in an email and click Next. If you click the link in the email, you will need to reenter your email address and password.

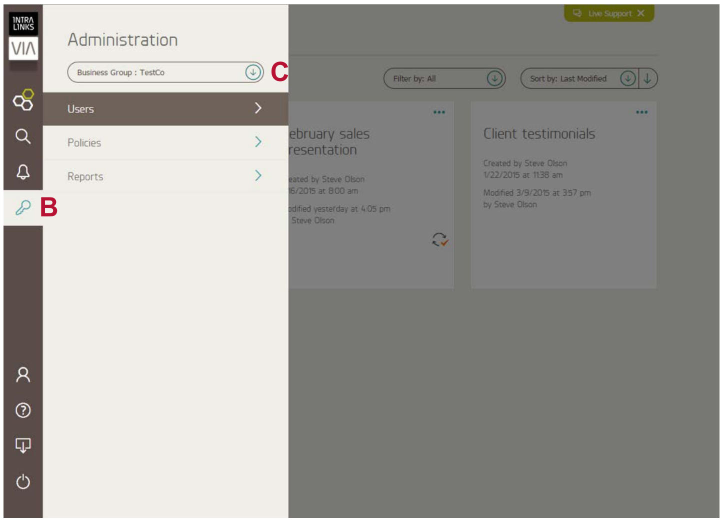
   All previously enrolled authentication factors are removed.
6. In the Account Security Setup screen, reconfigure the authentication factors that you want to use to verify your identity as described above.
7. Click **Finish**.

Displaying the administrator screens

To view the screens that Intralinks VIA Pro administrators use to manage business group member accounts, click the key icon (**B**) that appears in the navigation bar on the left side of the screen. A navigation panel slides out, showing you the options that are available to you:

- **Users** — Use the **Users** screen to view a list of business group members who have access to Intralinks VIA Pro. Administrators use this screen to create and downgrade accounts and send activation emails to group members who have not activated their accounts yet.
- **Policies** — Use the **Policies** screen to view the policies that administrators have set for this business group. Administrators use this screen to control the functions that group members can access in Intralinks VIA Pro.
- **Reports** — Use the **Reports** screen to generate and view the Workspace Activity Report, Access Snapshot Report, and Usage Report. These reports allow you to monitor Intralinks VIA Pro usage on an individual and organizational basis. The Workspace Activity and Access Snapshot reports are available only to compliance officers. The Usage report is available to both compliance officers and Intralinks VIA Pro administrators.

If you monitor multiple business groups, use the **Business Group** list (**C**) to select the group you want to view.



*The **Administration** navigation panel.*

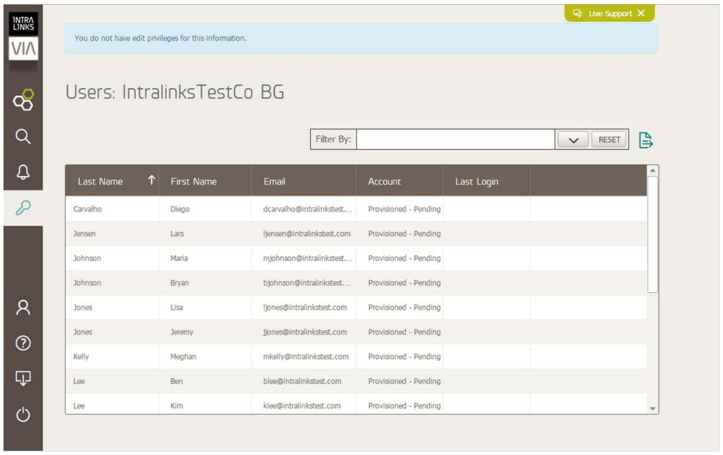
Working with the Users screen

As a compliance officer, you can use the **Users** screen to view information about the people in your business group who use Intralinks VIA Pro. If you have been given administrator privileges, you will also be able to add new accounts, send activation alerts, downgrade accounts to prevent those business group members from creating new Workspaces, and block specific members' devices from using Intralinks VIA Pro.

To display the **Users** screen, click the key icon (**B**) that appears in the navigation bar on the left side of the screen. A navigation panel slides out; click on the **Users** option.

Viewing information on the Users screen

The **Users** screen lists all the members of the selected business group who have access to Intralinks VIA Pro. The screen lists the members' names and email addresses, along with their account status and the last time each member logged into Intralinks VIA Pro.



You do not have edit privileges for this information.

Users: IntralinksTestCo BG

Filter By: RESET

Last Name ↑	First Name	Email	Account	Last Login
Carvalho	Diego	dcarvalho@intralinkstest....	Provisioned - Pending	
Jensen	Lars	ljensen@intralinkstest.com	Provisioned - Pending	
Johnson	Maria	mjohnson@intralinkstest....	Provisioned - Pending	
Johnson	Bryan	bjohnson@intralinkstest....	Provisioned - Pending	
Jones	Lisa	ljones@intralinkstest.com	Provisioned - Pending	
Jones	Jeremy	jjones@intralinkstest.com	Provisioned - Pending	
Kelly	Meghan	mkelly@intralinkstest.com	Provisioned - Pending	
Lee	Ben	blee@intralinkstest.com	Provisioned - Pending	
Lee	Kim	klee@intralinkstest.com	Provisioned - Pending	

*The **Users** screen.*

Business group members can have the following account statuses:

- **Provisioned - Pending** — The Intralinks VIA Pro administrator has created accounts for these individuals, giving them the ability to create new Workspaces, but they have not activated their accounts yet. They may have been invited by active provisioned Intralinks VIA Pro users to collaborate in their Workspaces.
- **Provisioned - Activated** — The Intralinks VIA Pro administrator has created accounts for these individuals, giving them the ability to create new Workspaces, and they have begun using their accounts. They may have been invited by other active provisioned Intralinks VIA Pro users to collaborate in their Workspaces.
- **Invited** — These individuals have been invited by an active provisioned Intralinks VIA Pro user to collaborate in a Workspace. They cannot create their own Workspaces, and they cannot use the Intralinks VIA Pro Desktop Client.

You can export information on the **Users** screen to a comma-separated value (.csv) file, allowing you to perform additional analysis and better manage user accounts. To export the information displayed on the **Users** screen, click the export icon 🗎 in the upper right corner of the screen.

Viewing the policies used to manage Intralinks VIA Pro accounts

As a compliance officer, you can use the **Policies** screen to view information about your organization's policies. You cannot make changes to these policies unless you have also been given administrator privileges. To display the **Policies** screen, click the key icon (**B**) that appears in the navigation bar on the left side of the screen. A navigation panel slides out; click on the **Policies** option.

IRM Protected

Information Rights Management (IRM) is used to protect sensitive files from being distributed without permission. Protected files remain encrypted at all times—even if they have been downloaded—and they can be viewed only by individuals who are authorized to use them. Individuals must enter their email address and Intralinks password before opening the documents. Workspace owners can unshare protected files even after they have been downloaded. When a document is unshared, previously authorized individuals will no longer have access to it. Protected files cannot be modified in any way. Only Microsoft Office and PDF files can be protected. Other types of files cannot be protected.

Require IRM protection on new and existing Workspaces – Automatically applies IRM protection to all the Workspaces created by members of their business groups, including Workspaces that were created before the policy was applied.

If this option is not marked, Workspace owners still will be able to apply IRM protection to their Workspaces or to specific folders, while leaving the contents of other folders unprotected. This can be useful if the Workspace owner wants some files to be editable during the collaboration process.

Require protected files to be downloaded for viewing – Requires people to download IRM-protected files to their computers before viewing them.

If this option is not marked, people will be able to view protected files online using a secure browser-based file viewer. Files that do not have IRM protection can always be downloaded for viewing, regardless of this policy setting.

Two-Step Verification

Require authentication on new and existing Workspaces – Requires Workspace participants to enter a security code when accessing Workspaces that are associated with the business groups managed by the Intralinks VIA Pro administrator. Codes can be sent as text messages or by email. When the **Authentication codes must be delivered by text message (SMS)** option is marked, all codes are sent by text message.

Collaboration

Enable file comments in Workspaces – Enables Workspace participants to comment on files that are uploaded to the Workspace. Comments can be an important part of the collaboration process.

If this option is not marked, participants are prevented from commenting on files in Workspaces.

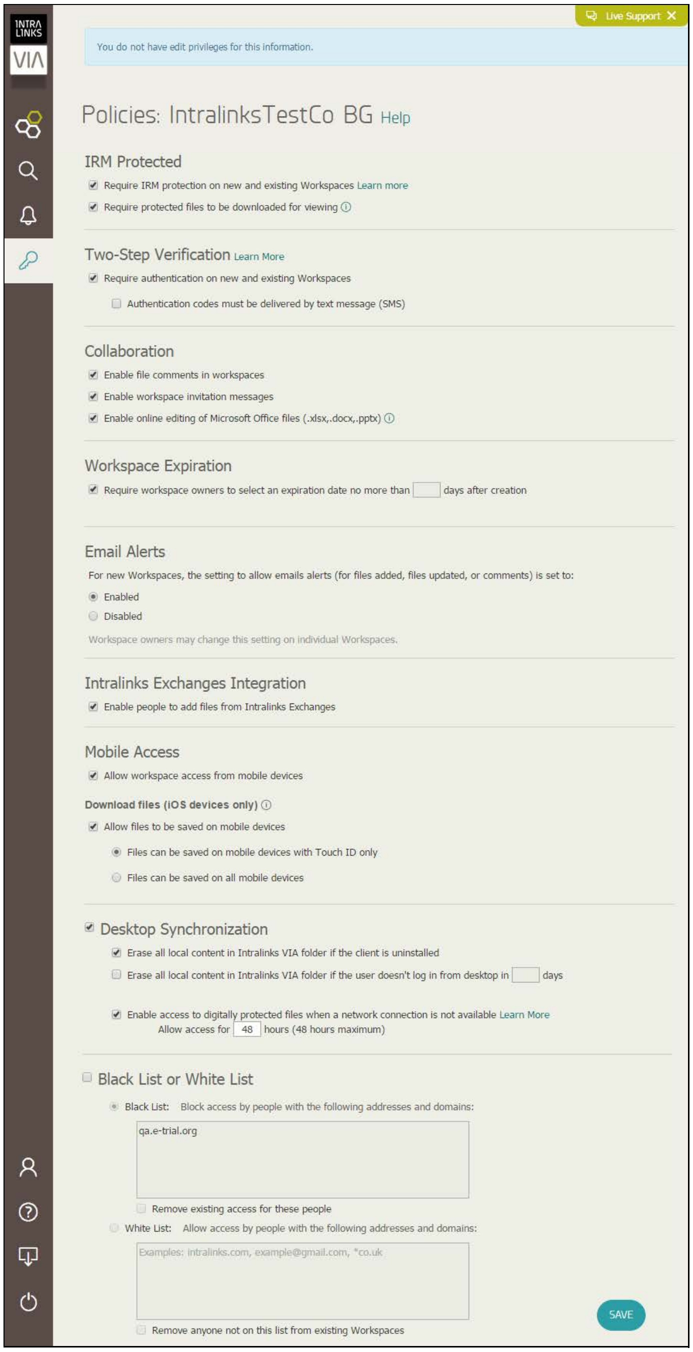
Enable Workspace invitation messages – Enables Workspace owners to add their own notes to the standard activation email that is sent to people they invite to participate in their Workspaces.

If this option is not marked, Workspace owners cannot add their own comments to activation emails.

Support Access

Disable access to workspaces by Intralinks Administrator – Prevents Intralinks administrators from viewing data within the business group's Workspaces. If this policy is enabled, Intralinks support team members who have administrative privileges will continue to have the ability to view permissions and other details associated with the storage of the data related to the business group, but Intralinks employees will not be able to access the data itself.

If this policy is not enabled, while resolving issues at a customer's request, Intralinks support specialists will be able to view all Workspace information, including the data stored in the Workspace. Note that Intralinks' operational policies prohibit Intralinks support specialists from viewing customer data other than while resolving customer issues.



You do not have edit privileges for this information.

Policies: IntralinksTestCo BG Help

IRM Protected

☑ Require IRM protection on new and existing Workspaces Learn more

☑ Require protected files to be downloaded for viewing ⓘ

Two-Step Verification Learn More

☑ Require authentication on new and existing Workspaces

☐ Authentication codes must be delivered by text message (SMS)

Collaboration

☑ Enable file comments in workspaces

☑ Enable workspace invitation messages

☑ Enable online editing of Microsoft Office files (.xlsx,.docx,.pptx) ⓘ

Workspace Expiration

☑ Require workspace owners to select an expiration date no more than ____ days after creation

Email Alerts

For new Workspaces, the setting to allow emails alerts (for files added, files updated, or comments) is set to:

● Enabled

○ Disabled

Workspace owners may change this setting on individual Workspaces.

Intralinks Exchanges Integration

☑ Enable people to add files from Intralinks Exchanges

Mobile Access

☑ Allow workspace access from mobile devices

Download files (iOS devices only) ⓘ

☑ Allow files to be saved on mobile devices

● Files can be saved on mobile devices with Touch ID only

○ Files can be saved on all mobile devices

☑ Desktop Synchronization

☑ Erase all local content in Intralinks VIA folder if the client is uninstalled

☐ Erase all local content in Intralinks VIA folder if the user doesn't log in from desktop in ____ days

☑ Enable access to digitally protected files when a network connection is not available Learn More
Allow access for 48 hours (48 hours maximum)

☐ Black List or White List

● Black List: Block access by people with the following addresses and domains:

qa.e-trial.org

☐ Remove existing access for these people

○ White List: Allow access by people with the following addresses and domains:

Examples: intralinks.com, example@gmail.com, *co.uk

☐ Remove anyone not on this list from existing Workspaces

*The **Policies** screen.*

Workspace Expiration

Require Workspace owners to select an expiration date no more than __ days after creation – Requires Workspace owners to set an expiration date (within the allowed maximum number of days) for all new Workspaces that they create. Owners of existing Workspaces will be required to enter an expiration date the next time they save a change to their Workspace(s). This option specifies the maximum length of time, in days, that Workspaces can remain active.

When Workspaces expire, viewers and editors who were invited to the Workspace lose access to them immediately. Workspace owners can continue to view the Workspace and make changes to it, however. Workspaces expire at the end of the day on their expiration date. After a Workspace has expired, it cannot be made active again.

If this option is not marked, Workspace owners will not be required to set expiration dates for their Workspaces.

Email Alerts

Workspace owners can choose to send or not send alerts when files are added, updated, or when comments are made on Workspaces within their business group. The Intralinks VIA Pro administrator can select a default setting for this business group policy by marking the **Enabled** or **Disabled** option.

If email alerts are enabled, alerts will be sent when files are added, updated, or commented on. If alerts are disabled, then no alerts will be sent when files are added, updated or when comments are made. Workspace participants can decide whether they want to receive those alerts.

Some email alerts — such as “welcome to Intralinks VIA Pro” alerts and password reset alerts — are sent regardless of the email alert setting selected by Workspace owners.

Intralinks Exchanges Integration

Enable people to add files to Intralinks Exchanges – Enables Workspace participants to copy files between the Workspaces and exchanges that they have been given permission to use. Participants can copy files only to exchanges that do not require entries for document custom fields.

If this option is not marked, individuals will not have the ability to copy files between Workspaces and exchanges.

Mobile Access

Allow Workspace access from mobile devices – Allows Workspace participants to access Intralinks VIA Pro using Intralinks mobile apps for iPad, iPhone and Android.

Participants can also be given the ability to download files to their iPhone or iPad by marking the **Allow files to be saved on mobile devices** option. For added security, this feature can be restricted to Touch ID-enabled devices only.

Downloaded files are available only within the Intralinks VIA Pro app; other apps will not be able to access them. Only files that are not IRM protected can be downloaded to mobile devices.

Desktop Synchronization

Erase all local content in Intralinks VIA folder if the client is uninstalled – Causes all files associated with Intralinks VIA Pro to be removed when the Intralinks VIA Pro Desktop Client is uninstalled from individuals' computers. This includes Workspace files that have been synced to an individual's desktop, as well as settings files used by Intralinks VIA Pro.

If this option is not marked, the files will remain on computer desktops, but they will no longer be synced.

Erase all local content in Intralinks VIA folder if the user doesn't log in from desktop in __ days – Causes all synced files and settings information to be automatically removed from members' computers unless they log into the Intralinks VIA Pro Desktop Client regularly.

When this option is marked, the number of days after which content will be removed is also specified. If a member does not log in within the specified number of days, all synced files will be removed from the Intralinks VIA Pro folder and all Intralinks VIA Pro settings files will be removed. Synced files on other devices will not be affected.

If a member logs into the Desktop Client after files have been removed from their computer, the files will be synced to their computer again.

Enable access to digitally protected files when a network connection is not available – Allows Workspace participants to view protected Microsoft Office files that have been synced to their Intralinks VIA Pro Windows desktop client without a network or Internet connection. Synced files are available for a limited amount of time (a "lease period")—up to 48 hours—as specified by the policy. During the lease period, no authentication will be required for protected files.

When enabled, this policy lets people continue working with protected files while traveling, while in a location where an active network or Internet connection is not available, or where connecting to a mobile network would result in roaming charges.

The policy applies to all Workspaces associated with the business group for which the policy is set. The ability to access files during their respective lease periods is available to all Workspace participants, including those who belong to other business groups.

This policy does not apply to protected PDF files. It also does not apply to Workspaces that require two-step verification. Synced files that are not IRM protected are not affected by this policy.

If this policy is not enabled, participants will be required to have a network connection to open protected files.

Blocked sender list or safe sender list

A blocked sender list or a safe sender list can be used to control who can be invited to participate in Workspaces. Only a blocked sender list or a safe sender list can be created, not both.

If the Intralinks VIA Pro administrator has chosen to create a blocked sender list, the email addresses and domains included in the list are blocked; Workspace owners cannot send invitations to people with these specific addresses or whose addresses are from these domains.

If a safe sender list is created, only people with the specific email addresses, or whose email addresses belong to the listed domains, can receive invitations to Workspaces.

When a blocked sender list is used, the administrator marks the **Remove existing access for these people** option if he or she wants to apply the list to existing Workspaces associated with this business group. Individuals who are on the blocked sender list are removed from all Workspaces associated with the business group. These individuals also lose access to all protected files, including those that have been downloaded.

When a safe sender list is used, the administrator marks the **Remove anyone not on this list from existing Workspaces** option if he or she wants to apply the list to existing Workspaces associated with this business group. Individuals who are not on the safe sender list are removed from all Workspaces associated with the business group.

Viewing custom fields that are used to track Workspace details

Using the **Details** screen, you can view custom fields that Intralinks VIA Pro administrators have created to enable Workspace owners in their business group to record and track details about the owners' Workspaces. These fields can be used to capture whatever information is relevant to the business.

Workspace owners can enter information in custom fields. Editors and viewers can view, but not change, these entries.

Adding and modifying custom fields

Intralinks VIA Pro administrators can use the **Details** screen to add, remove or modify custom fields. These fields appear on the **Details** tab for individual Workspaces.

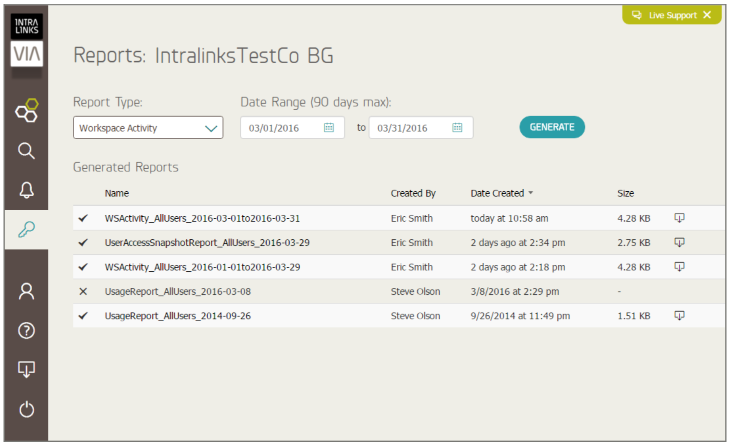
To view custom fields, display the **Details** screen: Click the key icon (**B**) that appears in the navigation bar on the left side of the screen. A navigation panel slides out; click on the **Details** option.

Intralinks VIA Pro provides four field types:

- **Single Line** – This field type allows users to enter a single line of data. Intralinks VIA Pro administrators can specify whether the field will allow alphanumeric characters, numeric-only characters, a currency amount or a percentage.
- **Date** – This field type allows users to enter or choose a date using a calendar widget. Intralinks VIA Pro administrators can add help text within the field itself; this text will be removed when users begin typing a value in the field.
- **Multi-line** – This field type allows users to enter multiple lines of alphanumeric data, up to 400 characters.
- **Drop Down** – This field type allows users to select a value from a predefined list.

Viewing reports

Intralinks VIA Pro provides three powerful reports for monitoring how VIA Pro is being used within your organization: the Workspace Activity report, the Usage report, and the User Access Snapshot report. These reports can give you insight into the flow of information within and from your organization,



Reports: IntralinksTestCo BG

Report Type: Workspace Activity

Date Range (90 days max): 03/01/2016 to 03/31/2016

Generated Reports

	Name	Created By	Date Created	Size
✓	WSActivity_AllUsers_2016-03-01to2016-03-31	Eric Smith	today at 10:58 am	4.28 KB
✓	UserAccessSnapshotReport_AllUsers_2016-03-29	Eric Smith	2 days ago at 2:34 pm	2.75 KB
✓	WSActivity_AllUsers_2016-01-01to2016-03-29	Eric Smith	2 days ago at 2:18 pm	4.28 KB
✕	UsageReport_AllUsers_2016-03-08	Steve Olson	3/8/2016 at 2:29 pm	-
✓	UsageReport_AllUsers_2014-09-26	Steve Olson	9/26/2014 at 11:49 pm	1.51 KB

*The **Reports** screen.*

and allow you to monitor Intralinks VIA Pro usage on an individual and organizational basis.

The Workspace Activity and User Access Snapshot reports are available only to compliance officers. The Usage report is available to both compliance officers and Intralinks VIA Pro administrators.

To display the **Reports** screen, click the key icon (**B**) that appears in the navigation bar on the left side of the screen. A navigation panel slides out; click on the **Reports** option.

The Workspace Activity report

The Workspace Activity report allows compliance officers to audit each person's Workspaces. If the business group members that you monitor have access to other organizations' Workspaces, you will be able to audit their activities in those Workspaces, as well.

This report can be generated for a selected date range, up to 90 days, and can be generated for all individuals.

Before you view a Workspace Activity report for the first time, a legal disclaimer will appear. The statement requires you to acknowledge that the report contains confidential information and is solely for internal compliance purposes, and to affirm that you are authorized to have access to the information contained in the report. The text of the disclaimer also appears in the header for all exported versions of the report.

This report is generated in CSV format and can be viewed as a Microsoft Excel spreadsheet. Each row in the report describes a separate event or action performed by an individual. The report includes the following columns:

- **Workspace ID** – A unique numerical identifier for the Workspace; Workspaces may be renamed, but they retain this ID.
- **Workspace Name** – The Workspace's name.
- **Folder ID** – The unique identifier assigned to the folder. If the action is associated with a file, this is the folder where the file is stored.
- **Folder Name** – The name of the folder. If the action is associated with a file, this is the folder where the file is stored.
- **File ID** – The unique identifier assigned to the file.
- **File Name** – The name of the file.
- **Action Taker** – The person who carried out the action that resulted in this event.
- **Action Taker's BG** – The business group associated with the person who carried out the action.
- **Action Taker's Role** – The role of the person who carried out the action, at the time of the action. Possible values are Owner, Editor, Viewer, Invisible Viewer and Administrator.
- **Action** – An action that affected the Workspace. The following values may appear in this column:
    - **Create Work Space** – The Workspace was created

  - **WS Expired – Manual** – The Workspace was expired by the Workspace owner
  - **Work Space auto expired** – The Workspace was expired by the system
  - **Role Change** – The Workspace owner changed the role assigned to the specified individual
  - **Work Space Protection Change** – The Workspace's protection setting was changed
  - **Work Space Expiration Date Change** – The Workspace's expiration date was changed
  - **Work Space Delete** – The Workspace was deleted
  - **Work Space Rename** – The Workspace was renamed
  - **Work Space Invite** – The organization administrator invited the specified individual to the Workspace as part of a transfer of ownership action
  - **Access Revoke** – The organization administrator removed the specified individual from the Workspace as part of a transfer of ownership action
  - **Add file** – A new file was uploaded to the Workspace
  - **Update file** – An existing file (identified in the **Previous Version Name** column) was replaced by a new file (identified in the **File Name** column)
  - **View/download File** – The specified file was downloaded or viewed; this includes files that were copied from Intralinks VIA Pro to an Intralinks Platform exchange
  - **Move File** – The specified file was moved
  - **Delete File** – The specified file was deleted
  - **Add Comment** – A comment was added to a file's comment thread
  - **Add folder** – The specified folder was created
  - **Folder Invite** – The specified individual was invited to access the folder
  - **Change the folder protection level** – The protection setting for the specified folder was changed
  - **Move Folder** – The specified folder was moved
  - **Updated Folder** – The specified folder was renamed
  - **Delete Folder** – The specified folder was deleted
  - **Folder Restored** – The specified folder was restored (undeleted)
  - **Document Restored** – The specified file was restored (undeleted)
  - **Self Revoked** – The specified individual removed himself or herself from the Workspace
- **Recipient of Action** – The email address of the person who was the target of the action.
- **Recipient's Org** – The name of the organization associated with the person who was the target of the action.
- **Recipient's Role** – The role of the person who was the target of an action, at the time of the action. Possible values are Owner, Editor, Viewer and Invisible Viewer.
- **Workspace BG** – The business group associated with the Workspace where the action was carried out.

- **Workspace Org** – The name of the organization associated with the Workspace where the action was carried out.
- **Date (MM/DD/YYYY HH:MM)** – The time the event occurred. The format used for the time stamp is indicated in the header.
- **Detail** – Provides further information about the changes made, if applicable. Details can include text added to email invitations for Workspaces and folders; the text of comments that were added; the original name of Workspaces, folders and files that were renamed; the roles of individuals who were added or removed from a Workspace or folder; the original and new dates when an expiration date is updated; and whether protections were enabled or disabled (ON or OFF) when protection settings were changed.

The Usage report

The Usage report provides a view into how each business group member uses Intralinks VIA Pro. This report is generated in CSV format and can be viewed as a Microsoft Excel spreadsheet. It includes the following columns:

- **Email Address** – The user account (email address) of the business group member.
- **First Name** – The member's first or given name.
- **Last Name** – The member's last or family name.
- **Office Phone** – The office phone number for this member.
- **Account Status** – This field has two values, *Active* and *Inactive*. Indicates whether the business group member has logged in to activate his or her account.
- **Account Creation Date (MM/DD/YYYY HH:MM)** – The date on which the Intralinks VIA Pro account was created. (The header also indicates the date format used for this column.)
- **Login Count** – The total number of logins for this individual.
- **Avg Logins per Month** – The average number of times per month the individual has logged into Intralinks VIA Pro.
- **Login Count for Last 30d** – The number of times the individual has logged in over the past 30 days.

The User Access Snapshot report

The User Access Snapshot report allows compliance officers to view a list of business group members, the Workspaces each business group member has access to, and their level of access (manager, editor or viewer) within each Workspace.

This report is generated in CSV format and can be viewed as a Microsoft Excel spreadsheet. The report includes the following columns:

- **User ID** – A unique numerical identifier for the business group member.
- **Email Address** – The user account (email address) of the business group member.
- **Workspace ID** – A unique numerical identifier for the Workspace; Workspaces may be renamed, but they retain this ID.
- **Workspace Name** – The Workspace's name.

- **Folder ID** – The unique identifier assigned to the folder.
- **Folder Path** – The folder path, if the business group member has been invited to a specific folder within a Workspace.
- **Status** – The current status of the business group member (invited, provisioned, provisioned suspended, invited suspended). Only the organization administrator can suspend and restore member accounts.
- **Level of Access** – The business group member's level of access (owner, editor, viewer, or invisible user) within the Workspace.
- **Last Access Date** – The last time the business group member accessed the Workspace.

Requesting a report

Be sure the **Reports** screen is displayed.

1. If you monitor multiple business groups, click the key icon (**B**) that appears in the navigation bar on the left side of the screen. A navigation panel slides out; then use the **Business Group** list (**C**) to select the group you want to view. Click on the **Reports** screen to hide the navigation panel.
2. Click **Generate**.

   Depending upon the size of the report being generated, the report will appear in a short time in the **Generated Reports** section of the **Reports** view. Be sure the correct business group is selected when viewing reports. Only the reports for the selected business group are displayed.
3. Click the report name to download a copy of the report in CSV format, which can be viewed using Microsoft Excel.

Using ComplianceLink

The ComplianceLink report is a daily report that allows compliance officers to see all electronic communication between individuals who use Intralinks VIA Pro, in compliance with securities regulations. This report is created for organizations that request it, and must be generated by an Intralinks Administrator. The report appears in RFC 822 and XML formats. The report includes comments, Workspace descriptions and email alerts inviting recipients to use Intralinks VIA Pro Workspaces and folders. The ComplianceLink report is not available for delivery through the Compliance Officer's user interface; contact Intralinks customer service to request assistance with ComplianceLink reporting.

Getting help with Intralinks VIA Pro

If you have a problem and need help while using Intralinks VIA Pro, you can click the **Live Support** link at the top of the screen to start a chat session with an Intralinks client support specialist. A chat window will open and you will be connected with a support specialist.

A number of other support tools are available. To view them, click the Help icon ⓘ in the navigation panel on the left side of the screen; a Help pane will appear. Select one of the following options from the pane:

Live Support Chat — This link opens the same chat window that the **Live Chat** link opens.

Support Center — This link opens the Intralinks VIA Pro Support Center. You can email a question to the Intralinks support team or start a chat session, get copies of the VIA Pro startup guides, view short video tutorials, access the Intralinks Academy resource center, and view FAQs for Intralinks VIA Pro.

Feature Tour — This link displays a video overview of Intralinks VIA Pro's key features.

What's New? — This link displays a video that shows the features added in the latest update to Intralinks VIA Pro. This link is helpful for those who have been using Intralinks VIA Pro for a while and want to get up to speed on recent enhancements.

Intralinks Academy — This link displays Intralinks Academy, Intralinks' web-based collection of video tutorials and other learning materials.

Give Feedback — This link displays a text box that you can use to send feedback about your experience with Intralinks VIA Pro. Use this link, for example, if you want to suggest improvements or new features.

Logging out of Intralinks VIA Pro

When you have finished working with Intralinks VIA Pro, click on the Logout icon at the bottom of the navigation bar on the left side of the screen.

Logging in to another Intralinks application

If you have access to other Intralinks applications, you can switch applications without the need to reenter your login credentials.

Click the **App Switcher** icon and click on the application that you want to open. Note that this menu only appears if you have access to other Intralinks applications.