ON SIGHT
CONNECT

ONSIGHT WORKSPACE
ADMIN GUIDE

TABLE OF CONTENTS

OVERVIEW

Onsight Workspace provides a secure, central repository for Onsight images, recordings and calls as well as external content such as manuals and schematics. Using WORKSPACE, enterprises can efficiently manage and maintain content created by and for Onsight users. With detailed permission controls, enterprises ensure that authorized users can access the content they need to perform their work.

Integrated with Onsight Connect, WORKSPACE provides tools to:

• Upload and Edit Onsight generated video and still images – Onsight Administrators can view and manage the status of the Onsight Connect generated content.
• Enable Automatic Uploads when Onsight calls end.
• Manually upload content from Onsight Connect Files.
• Monitor Upload Queue status.

Launch Workspace from Onsight Connect clients to view the repository.

• Configure User and Group Permissions – Use the Onsight Client Policies and Permissions defined in Onsight Platform Manager to control access to the WORKSPACE. Refine User and Group permissions using the WORKSPACE Administration interface.
• Share content between authorized users.
• File Management
• View images and edit telestration.
• View Onsight video recordings including telestration and shared images.
• Includes support for versioning of content for audit controls.
• Search tags, titles and Metadata.
• View Favorites, Recent Files and Recent Activity on the Dashboard.

Generate Advanced Reports – Regular review of usage statistics, including who logged in to the software, how many calls a person placed and received, and total and average duration of calls will indicate how well the technology is being adopted.

The tasks described are administration-level tasks and are not intended for end-users of Onsight Connect. Many of the tasks involve configuring Client Policy and Permissions, and affect how endpoints function.

ONSIGHT CONNECT

The Onsight Connect Service is a centrally managed subscription based cloud collaboration service. An authorized user can log in to Onsight Connect on a Windows PC, iOS or Android Smartphone, or Librestream Onsight Rugged Smart Cameras to begin collaborating.

Once logged in, an Onsight Connect user can securely view, edit and share video, images, audio, and telestration with another Onsight user. They can also share audio and video with a 3rd party video endpoint that supports Session Initiation Protocol (SIP).

When Onsight WORKSPACE is enabled, users can upload their content directly to WORKSPACE as an archival, knowledgebase and workflow repository.

Onsight Platform Manager (OPM) is the central management server for Onsight Connect users. All Onsight Connect user licenses and policies are controlled by OPM. This includes access to WORKSPACE.

Workspace Tip: Client Policy specific to the Onsight WORKSPACE is defined by Onsight Platform Manager Group Policy. WORKSPACE file and folder permissions are managed within Onsight WORKSPACE.

For more information on the full Onsight Connect capabilities, access the online training portal at https://onsight.librestream.com/.

NETWORK REQUIREMENTS

Onsight software requires HTTPS network protocol to communicate with Onsight WORKSPACE.

HTTPS	443
Browser	TLS v1.2 support.
Web Proxy	Configure as required by your Enterprise's security policy.
Wireless Network	802.11 a/b/g/n
Wired Network	A wired 10/100 Ethernet port is recommended.
Wired Network	A wired 10/100 Ethernet port is recommended.

FIREWALL CONFIGURATION

If Windows Firewall or other third-party firewall software is running on the network where you are attempting to access Onsight Workspace, you may need to add firewall exceptions for the ports listed in Table 1.

Name	Protocol	Port	Description
HTTPS	TCP	443	Required if remote endpoints will access the Web Service interface over TCP port 443. If your IIS configuration uses a port other than 443, ensure that you have allowed that port instead.

LOGGING INTO WORKSPACE

Onsight user licenses provide access to Workspace as long as a user has been granted permission by a Group Policy. Onsight Platform Managers can access Onsight Workspace regardless of Group Policy settings.

Logging in from a Browser

LOGIN VIA ONSIGHT PLATFORM MANAGER

You will receive your OPM Administration login information from Librestream via an email.

To login to OPM, open a browser and navigate to https://onsight.librestream.com. Enter the user name and password that Librestream provided to you via email in the following format:

User Name: user@domain.com
Password: Password

To avoid unauthorized access to the software, you should change this password immediately after logging in for the first time, as described in Changing the Administrator's Password section.

After successfully logging in, you will be taken to the OPM

Home page. Tap the Workspace tab, you will be directed to the Workspace Home page.

LOGIN DIRECTLY TO WORKSPACE

You may login directly to Workspace using your Onsight user account by going to the Onsight Workspace login page:
 https://workspace.librestream.com
Enter your Onsight account credentials. You will be temporarily redirected to the OPM login screen in order to authenticate your credentials.

Logging in from a Browser

LOGIN FROM AN ONSIGHT CLIENT

Using your Onsight user credentials login to Onsight Connect. Go to

FILES, and click the green Workspace *button. This will open your browser and take you to your Onsight WORKSPACE.*

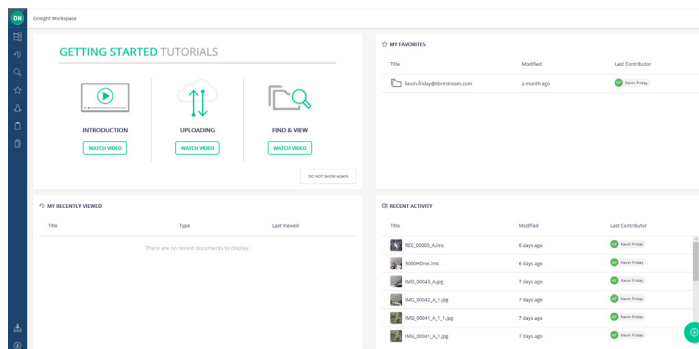*These browsers have been tested with Workspace and provide full support:*
- Google Chrome
- Safari iOS 10.2 and Mac
- Microsoft Edge

Note: *Internet Explorer is not supported. Firefox can display content but is unable to play video content.*

External Guest Users can not access Workspace.

WORKSPACE HOME PAGE

The Workspace Homepage provides a Dashboard with the following features:

For Standard Users:
- Getting Started Tutorials.
- My Favorites – Content marked as favourite. By default, users' upload folders are automatically added to their Favorites list for quick access.
- My Recently Viewed – List of recently viewed content.
- Recent Activity – A list of recent activity in the Workspace based on the user's Read permissions.
- Browse – File system explorer.
- Search – File names, tags, metadata.
- Personal Space – Stores private user content accessible only by the owner. The owner can edit permissions to share access to the personal space with other users.
- Clipboard – Copy media between folders using the clipboard.

For Administrators:
- Analytics – Provides Document Distribution and Repository Content information.
- Users & Groups – The listing here is provided for reference and the application of workspace permissions. All users and groups are managed using Onsight Platform Manager.
- About – Version, Terms of Use/EULA, Connect with Us, Copyright.
- Audit

User Settings:
- Profile
- Settings
- Sign Out

File and Folder Permissions

The following list describes the default behaviour of file and folder permissions in Onsight Workspace.

- By default, users and groups can access all files and folders in Onsight Workspace.
- Administrators define the upload folder directory structure within group client policies.
- You may restrict permissions to upload folders so that only administrators and owners may access the files and folders.

See the Advanced Permission Control section for a full description.

ADMINSTRATOR SETTINGS

The following section describes settings that are managed on the Onsight Platform Manager.

All Administrator accounts are managed by Onsight Platform Manager. The **Account Owner** is the main Administration account. The Administrator account includes an Onsight Connect endpoint license; therefore, you can log in to Onsight Connect software as a User as well as configure OPM.

When logged in to OPM, My Profile allows the Administrator to configure their personal settings like any other User Account. Once these settings are configured, the Administrator can also log in to an Onsight endpoint and use it for collaboration.

Onsight WORKSPACE access is included with the Administrator account provided the WORKSPACE service has been enabled for your enterprise's Onsight domain and access has been granted through a client policy.

Changing the Administrator's Password

- Choose Personal Settings → My Profile. This will take you to the My Profile configuration page.
- Select Common Actions → Change Password, and enter the new password into both provided fields. Your password must be different from the current password.
- Click the Change Password button to save your changes.

Changing the Administrator's User Settings

- Choose the CONTACTS tab.
- Click the Global Contacts button to search for a contact to add to your Contacts list.
- Enter a name to search and press the search button.
- Or, you may just press the search button to see a list of all users.
- To Enter a contact manually, click the New button.
- Enter the Name, Address, and Type for the contact. You may enter an optional Address 2. Note: the address must be in the SIP URI format, e.g., user@sipdomain.com.
- Click OK to save.

Adding Administrators to Workspace

As the OPM Administrator you can add additional Administrator accounts. The additional Admin accounts will not consume a call license unless you specifically assign an Onsight Client Licence to the administrator.

To add additional Administrators:

- Select the USERS tab.
- Press the New User button.
- Enter the PROFILE settings:
  - Username
  - First Name
  - Last Name
  - Email: Send Welcome Email and Generate Temporary Password are selected by default. If you choose not to send the welcome email, it is recommended to also uncheck Generate Temporary Password. You will need to notify the new admins of their usernames and passwords.
  - If Single Sign On is enabled, enter the Federated SSO ID (if required). See the SSO section for details.
- Under CLIENT SETTINGS, select Administrator for the Account Type.
- The Automatically assign a SIP account to this user is selected by default. This is required if you want your administrators to be able to log in locally on an Onsight endpoint and make calls.
- By default, the Administrator will belong to the Domain license group. You do not need to assign the administrator to a different license group.
- By default, the Administrator belongs to the Domain policy group. You do not need to assign the administrator to a different client policy group.
- It is recommended you do not set the account expiry for Administrators unless required. For example, a temporary administrator has been assigned while someone is on vacation
- You **must** grant the Administrator access to Workspace through a client policy.

USERS AND GROUPS

The following section describes settings that are managed on the Onsight Platform Manager.

Onsight administrators centrally manage Onsight user licenses, manage contacts lists and groups, and configure user group policies and permissions through the Onsight Platform Manager Web interface. Using OPM, administrators can efficiently manage and maintain groups of Onsight users.

In order to access Onsight WORKSPACE, a user must be added to the Onsight domain and assigned to a group with a client policy that grants access to WORKSPACE.

Refer to the Onsight Platform Manager Admin Guide for details on managing users and groups.

ON SIGHT
CONNECT

GROUP CLIENT POLICY

This section describes client policy settings managed on the Onsight Platform Manager.

Group Client Policy allows you to control endpoint behaviour. The policy is assigned to a Group and applied to the group members each time they log in to an Onsight Connect endpoint.

Whether users are logging in to a Windows PC, iOS or Android smartphone, or an Onsight Smart Camera their assigned client policy will be applied.

Client permissions determine authorization for user access to settings on an Onsight endpoint. For each setting, you can select either Allow, Deny or Inherit to set the permission access to the setting.

When a user is logged into Onsight Connect Software:

- Allow will let them edit the setting.
- Deny will prevent access.
- Inherit will apply the permission based on the parent of the current Client Permissions group. All Client Permissions groups will inherit from the parent Domain Defaults group.

ℹ️ Group Client Policy controls user access to Onsight Workspace.

The Onsight Platform Management Settings Template describes settings and provides best practices for Group Client Policy with respect to Onsight WORKSPACE settings.

See https://cms.librestream.com/media/Onsight-Platform-Manager-Default-Settings-400305-09_Rev_D.xlsx

Configuring Onsight Workspace Group Client Policy

- **Access** – Authorizes access to Onsight Workspace for the members of the group.
- **Upload Path** – Sets the top-level directory structure in the Workspace. All files will be placed under the upload path in a User's upload folder within a Call folder. The format is \UploadFolder\CallFolder. E.g, \b.engineering@mycompany.com\171116_111734_BobEngineering
- **Auto Upload Media** – When enabled, any files captured during an Onsight call will be automatically uploaded to the Workspace once the call has ended.
- **Maximum Upload Bit Rate (Kbps)** – When set to 0, the file upload will progress without any application controlled restrictions to bandwidth. When set to a limit, the file upload will not exceed the maximum value in Kbps.
- **Restrict Upload Folder Access to Owner** - When enabled, users can only access the upload folders they own.
- **Allow cellular/mobile data usage** – When enabled files will be uploaded using the cellular/mobile data when a wireless connection is not available. When disabled, files will be uploaded using the wireless network connection only.

Perform the following steps within Onsight Platform: Manager
1. On the SETTINGS page, select the CLIENT POLICY tab.
2. Select the Group to which you wish to apply a policy.
3. Click the Choose Settings button. You will be presented with the Choose Settings screen.
4. Select the Workspace category to include all Workspace settings in the client policy. Click OK.
5. When you are returned to the Client Policies page, set the appropriate Value for each Category:
   a. **Access** – Authorizes access to Onsight Workspace for the members of the group.
   b. **Upload Path** – Sets the top-level directory structure in the Workspace. All uploaded files will be placed under the user's upload path in a Call folder.
   c. **Auto Upload Media** – When enabled, any files captured during an Onsight call will be automatically uploaded to the Workspace once the call has ended.
   d. **Maximum Upload Bit Rate (Kbps)** – When set to 0, the file upload will progress without any application controlled restrictions to bandwidth. When set to a limit, the file upload will not exceed the maximum value in Kbps. Network bandwidth limits will still apply.
   e. **Restrict Upload Folder Access to Owner** - When enabled, users can only access upload folders they own.
   f. **Allow cellular/mobile data usage** – When enabled, files will be uploaded using the cellular/mobile data when a wireless connection is not available. When disabled, files will be uploaded using the wireless network connection only.
6. Repeat the process for each Group to which you want to apply a Workspace Client Policy.

Onsight Workspace Client Permissions
Client permissions determine whether a user can edit a setting when logged in on an Onsight client. The permissions include:
1. *Allow – let users edit the setting when logged in to an Onsight client.*
2. *Deny – do not allow users to edit the setting.*
3. *Inherit – use the setting inherited from the parent group. (Available only if the group is a child of a parent group. For example, the Domain group is the parent of all groups.)*
To set the permissions for the Workspace settings on client endpoints:
Users can only edit settings to which they granted permission. Two Workspace settings are editable on an Onsight client **Maximum Upload Bit Rate and Allow Cellular/Mobile Data Usage**. *All other Workspace settings are available to Admin only.*
1. *On the SETTINGS page, select the CLIENT PERMISSIONS tab.*
2. *Select the Group you want to manage.*
3. *For each setting below, apply the Action you want applied for the permission.*
   a. *Maximum Upload Bit Rate (Kbps) – determines if the user can edit the upload bit rate. (Allow, Deny)*
   b. *Allow Cellular/Mobile Data Usage – determines if the user can enable cellular/mobile data usage. (Allow, Deny)*
4. *Click* **Save**.

ADVANCED PERMISSION CONTROL

This section describes file and folder permission settings managed from within Onsight Workspace. As an Administrator, you may want finer control over folder and file permissions.

Permissions include:

Read – View and Download files.

ReadWrite – View, Edit and Download files.

Everything – ReadWrite and Folder creation.

To edit file and folder permissions:

1. Log in to Onsight Workspace.
2. Press the Browse button.
3. Navigate to the file or folder to which you wish to manage permissions.
4. Press the Permissions button in the upper right-hand side of the screen.
5. Press BLOCK to restrict access to the Administrators and the owner of the file or folder.

Note: by default, all users have access to all files and folders, you must block a file or folder to limit access to the owner and administrators only.

You can also restrict access by setting **Restrict Upload Folder Access to Owner** to enabled in group client policy (this is managed in Onsight Platform Manager). However, be cautious, undoing this step requires **manually** resetting permissions on all folders in Workspace.

6. To grant additional access to specific users and/or groups, press the NEW button.
7. Search for users and groups by entering text in the User/Group field. Select the Right to assign to the user or group from the drop-down list.
8. **Read**, **ReadWrite** or **Everything**.

Note: **Everything** allows a user to manage permissions as well as ReadWrite.

9. Select the Time Frame for the duration of the Right to be applied. Permanent or Date Based (if using Date Based enter the time period).
10. Press the CREATE button to apply the permissions to the file or folder.
11. The permission will be added to the PERMISSIONS DEFINED LOCALLY section.
12. To return to the default permission for a file or folder, set press the UNBLOCK button on the permissions page. Also, delete the new permissions that were added to the PERMISSIONS DEFINED LOCALLY section.

Note: As an administrator, you will always have access to all files and folders regardless of the defined permissions in the PERMISSIONS DEFINED LOCALLY section.

This process must be repeated for any file or folder on which you wish to edit permissions. Note that whenever you BLOCK a file or folder, by default, the owner of the object will maintain ReadWrite permission on the file or folder unless removed by the administrator.

AN EXAMPLE WORKSPACE

As the Administrator for your Onsight domain, you have been tasked with setting up access to Onsight Workspace for your users. Use this section as an example to plan your deployment.

MyCompany is an Onsight domain that has Onsight Workspace enabled. To grant access to the Workspace, you must perform the following steps:

1. Define your groups. MyCompany will have four groups:
   a. Customer Support
   b. Engineering
   c. Field Service
   d. Quality Assurance
2. For each group create a client policy.
   a. Group client policy must include the following Workspace settings:
      ii. Access – Enabled.
      iii. Upload Path – for each group you will define a distinct Upload Path, e.g., ~/CustomerSupport/, ~/Engineering, ~/FieldService, ~/QualityAssurance.
   b. The following are optional:
      iii. Auto Upload Media – recall that this setting will automatically upload all data captured in all Onsight calls. In this example it is Enabled.
      iv. Maximum Upload Bit Rate (Kbps) – Disabled, i.e., It is set to 0, and no restrictions are applied.
      v. Restrict Upload Folder Access to Owner – Disabled.
      vi. Allow Cellular/Mobile Data Usage – Disabled.
3. If required, assign a group administrator for each group.

Note: **Group administrators** will have Standard User rights within Onsight Workspace. They are not considered Workspace administrators.

4. Assign users to each group.
   a. New uses will automatically be synced with Workspace.
   b. If you are adding existing users to the Workspace, you must assign a Workspace account to them. Select the user and go to the More menu. Next, select Assign/Restore Workspace account.

This completes basic setup.

Restricting Access to Content

By default, all users can access all content in the Workspace. But access can be restricted. There are two main ways to restrict access to content:

- OPM Client Policy - Restrict Upload Folder Access to Owner
- Workspace - Permissions

OPM Client Policy - Restrict Upload Folder Access to Owner

When enabled, users can only access upload folders they own. By enabling this setting in a client policy, group members will only be able to access the contents of their own upload folders. They will not be able to access the upload folders owned by other group members.

However, a group which has **Restrict Upload Folder Access to Owner** enabled, can still access the upload folders of groups that do not have this feature enabled.

For example, as a member of the Customer Support group, you would be able to access your own upload folder and all other groups' upload folders based on the settings in the table below.
You would not be able to access other members' upload folders in the Customer Support group.

Example: Restrict Upload Folder Access to Owner

Group Name	Restrict Upload	User Access to Content
Customer Support	Enabled	My CS Upload folder, Eng, FS, QA
Engineering	Disabled	Eng, FS, QA
Field Service	Disabled	Eng, FS, QA
Quality Assurance	Disabled	Eng, FS, QA

Workspace Permissions

An administrator can choose to control access to content by editing permissions directly on the Workspace server. Content includes any file or folder in the Workspace.

By default, users can also edit permissions on content they own, if they choose to restrict or grant access to specific files or folders, to other users or groups.

You may wish to restrict all access by default and grant permission to content as needed amoungst groups or individual users. Or grant access by default and restrict access to specific users or groups to some content.

Workspace Upload Directory Structure
Your Workspace directory structure is based on the Upload Paths you have defined in each Group Client Policy. The MyCompany directory structure is outlined below:
- Workspace
  - CustomerSupport
  - Engineering
  - FieldService
  - QualityAssurance

When users upload to the Workspace, their files will be placed in the directory structure as defined by the Upload Path. For example, three users were added to the Engineering group:
- Bob Engineering
- Carol Design
- Jim Layout

When each user logs into Onsight Connect and participates in a call, any images and recordings they make will be automatically uploaded to Workspace (this is based on the applied Group Client Policy – Auto Upload Media: enabled).

The Engineering's Group directory structure will look like this in the Workspace:

- Workspace
    - Engineering/b.engineering@mycompany.com
        - 171119_102355_BobEngineering
            - IMG_0015.jpg
            - IMG_0016.jpg
            - IMG_0017.jpg
            - REC_00002_A.lmc
    - Engineering/c.design@mycompany.com
        - 171120_113345_CarolDesign
            - IMG_0034.jpg
    - Engineering/j.layout@mycompany.com
        - 171123_113345_JimLayout
            - REC_00010_A.lmc

As each user uploads files, their directory structure will expand as new call folders are added. The Call folder format is **date_timestamp_username**.

Note: Any offline images or recordings that are uploaded will be placed in a folder that follows the **date_username** format. Users can manually upload files at anytime when they are not in a call.

Note: All uploads will be paused when calls are in progress.

Workspace Custom Directory Structure

Administrators can manually add custom folders to the Workspace directory and control access through permissions.

For example, you may wish to restrict user access to each other's upload folders. To perform this restriction, you have set the Group Client Policy setting - Restrict Upload Folder Access to Owner – Enabled. Now when a user accesses the Workspace, they will only see their own upload folder and its contents.

To facilitate the sharing of documents, you create a new folder called Share, and grant ReadWrite permissions to all groups. They can now share files without having access to other users' upload folders. See section 7 for details on setting permissions on folders.

In this scenario, Bob Engineering would access the Workspace and see the following directory structure:

- Workspace
    - Share
        - Engineering/b.engineering@mycompany.com
            - 171119_102355_BobEngineering

Note: Custom folders are managed within your Workspace and are not synced or accessible through Onsight Platform Manager or the Onsight clients.

WORKSPACE ADMINISTRATION

This section describes Administration tasks that are performed within the Workspace. The Administration button is located on the menu.


Analytics

Workspace includes Analytics to help understand user activity and content within the Workspace. To access Analytics, select Administration on the menu located on the Administration panel. Next, select the Analytics tab.

Document Distribution

The Document Distribution is a dynamic chart that displays the number of documents, size and type within the Workspace on a per folder basis.
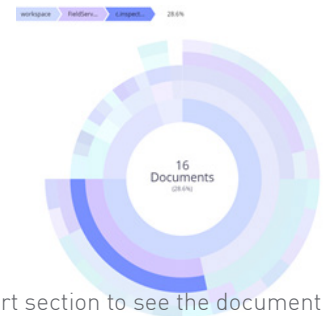
- Hover your mouse over a chart section to see the document stats.
    - The path to the folder will displayed as you hover over a folder.
- Select the type of view for the chart: folder size (MB) or document count (# of folders and files).
- Select the Options for viewing:
    - Include Hidden Documents
    - Include Deleted Documents
    - Include Versions
    - Only Folders
- The slider on the bottom refines the level of folders displayed in the chart.
    - Slide completely to the Left to see the total number of documents (files and folders) in the Workspace.
    - Slide completely to the Right to see a complete graphical representation of all folders and their contents.
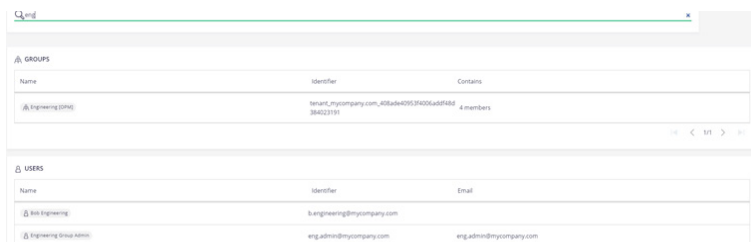
Repository Content

The Repository Content is a collection of chart and graphs that represent document types and usage statistics in the Workspace. You can filter the results based on date ranges.

Users and Groups

This page allows you to search the user and groups directories. Recall that all users and groups are managed by the Onsight Platform Manager. This is available for information purposes only.

- Type in the Search for users & groups text box to begin your search.
- Users and groups that match the search criteria will be displayed.

Recall that permissions for files and folders are applied directly from the file or folder location using the Permission button.

If a user or group is not present in the list, they must be added from within Onsight Platform Manager.

- **New users and groups are automatically synced with the Workspace.**
- **You must use Assign / Restore Workspace Account for existing users and groups that were created before Workspace was enabled within Onsight Platform Manager.**

Trash - Deleting Files and Folders

As the Administrator, you can permanently delete items that have been moved to TRASH by users. You should periodically review the files and folders users have moved to TRASH. You can also restore items from TRASH to the Workspace.

When a user moves an item to TRASH it is no longer visible to standard users within Workspace, use TRASH SEARCH to display the current contents of the TRASH repository.

- Press the TRASH search button on the menu.
- The Trash Search panel will appear.
- You can search based on Text, Modification Date, Authors, Tags or Size associated with files and folders.
- You may also just press Search to see all items in the TRASH repository.
- Check the selection boxes to select the items you wish to delete.
- The selection tool bar will be displayed at the top of your browser.
- Press the Delete button to permanently delete the items. They will not be restorable after this action is performed.
- Or you may press the RESTORE button to remove the items from TRASH and return them to the Workspace in their original location.
- Press OK or Cancel on the confirmation dialog to confirm your requested action.

END USER LICENSE AGREEMENT

This software is licensed under the terms of an End User License Agreement (EULA). The latest version of which can be found at: https://librestream.com/support-archives/termsofuse

CONTACT SUPPORT

If you need assistance, please contact **support@librestream.com** or call **1.800.849.5507** or **+1.204.487.0612.**