ONSIGHT

Onsight Platform Manager
Admin Guide

LIBRESTREAM.COM

LIBRESTREAM

Copyright

Onsight Platform Manager Guide

Doc #: 400199-24 Rev: K

February 2023 (v11.4.16)

Copyright Notice:

Patents Notice:

United States Patent # 7,221,386, together with additional patents pending in Canada, the United States, and other countries, all of which are in the name of Librestream Technologies Inc.

Trademark Notice

Librestream, the Librestream logo, Onsight, the Onsight logo, Onsight Connect, Onsight Flow, Onsight Workspace, Onsight Cube, Onsight Collaboration Hub, Onsight Smartcam, Onsight Platform Manager, and Onsight Teamlink are either registered trademarks or trademarks of Librestream Technologies Incorporated in Canada, the United States, European Union and/or other countries. All other trademarks are the property of their respective owners.

Contents

1. OVERVIEW

Onsight Platform Manager (OPM) is a secure online tool for centralized user management. System administrators can manage Onsight user licenses, contacts lists and groups, and configure user group policies and permissions. Using OPM, administrators can efficiently manage and maintain groups of Onsight users.

OPM provides tools to:

1. **Create and Manage User Accounts** — OPM Administrators can create users, policy groups, license groups and client policies and permissions.

2. **License Management** — OPM Administrators can view and manage the status of their license pools including:

    - **Connect Enterprise** — Provides Onsight Connect call services. In previous OPM versions (v9 and earlier) this was referred to as an Onsight user license. **Connect Enterprise** is equivalent to the Onsight user license.

    - **Workspace Enterprise** — Provides the user Workspace access based on administrator assigned permissions. Upload, view, share and analyze data, images, and recordings across internal teams. In previous OPM versions (v9 and earlier) this was a domain setting that was enabled to provide all users Workspace access. It is now managed by user license assignments.

    - **Workspace Contributor** — Provides the user **Workspace** access to their upload folder, access to other assets cannot be granted. Securely centralizes content from customers, suppliers, and third-party collaborators for analysis.

3. **Configure Client Policies and Permissions** — The Onsight **Client Policies** and **Permissions** are applied to an Onsight endpoint when the user logs in.

4. **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**, affect the endpoint's ability to function.

1.1. Onsight Augmented Reality Platform Architecture

The Onsight Augmented Reality platform is a centrally managed subscription-based service. An authorized user can log in to an Onsight Connect client on a Windows PC, iPhone, iPad and connect to Onsight device's such as the Cube or Hub.

Once logged in, an Onsight Connect user can securely view and share video, images, audio and telestration with another Onsight user. They can also share audio and video with a third-party video endpoint that supports Session Initiation Protocol (SIP). For more information on the full Onsight Connect capabilities, review the online documentation at www.librestream.com/support/

2. NETWORK REQUIREMENTS

Onsight software requires HTTPS network protocol to communicate with the Onsight Platform Manager.

Table 2-1 Network Requirements

HTTPS:	443
Web Proxy:	As set by your Enterprise's security policy
Wireless Network:	802.11 a/b/g/n
Wired Network:	A wired 10/100 Ethernet port is recommended.

2.1. Firewall Configuration

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

Table 2-2 Firewall Configuration

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

2.2. On Premises

Throughout this document information which applies only to on premises installations will be contained in the On Premises sections.

2.3. Login to OPM for the First-time

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

To login to OPM, open a browser and navigate to: https://onsight.librestream.com. Enter the user name and password you received in the Welcome email:

Table 2-3 Username & Password

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 *(on page 13)*.

After successfully logging in you will be taken to the Dashboard.

Note: On Premises — The URL of your OPM Server will depend on the server's URL assigned during installation. Refer to the On Premises installation guide.

3. DASHBOARD

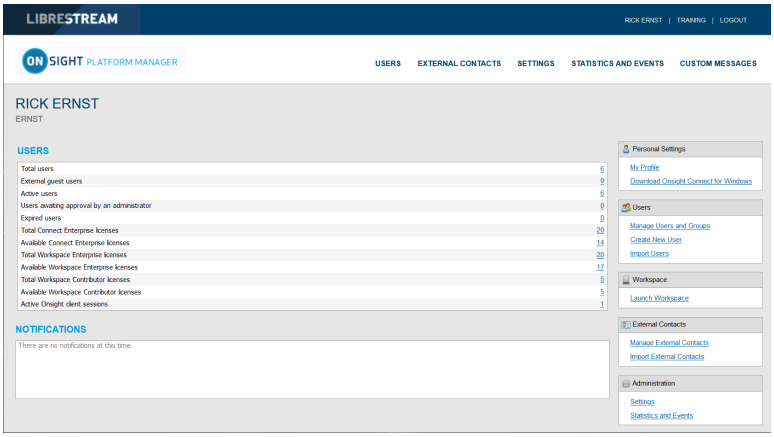


Figure 3-1 Dashboard

The dashboard page includes a **USERS** and **NOTIFICATION** section and a list of links.

USERS

The USERS section contains a table that displays user types, licenses and related information:

Total Users

The total number of all users (active and expired) in the domain.

External Guest Users

The total number of active external guest accounts.

On Premises

External guest users are not supported by on premises installations.

Active Users

The total number of active users in the domain.

Users Awaiting Approval by an administrator

The total number of self-registered users awaiting administrator approval. (See Self-Registration for details.)

Expired Users

The total number of expired users accounts.

Total and Available Licenses

A list of the total vs available licenses for each type is listed:

- **Total Connect Enterprise licenses**
- **Available Connect Enterprise licenses**
- **Total Workspace Enterprise licenses**
- **Available Workspace Enterprise licenses**
- **Total Workspace Contributor licenses**

4. ADMINISTRATOR'S SETTINGS

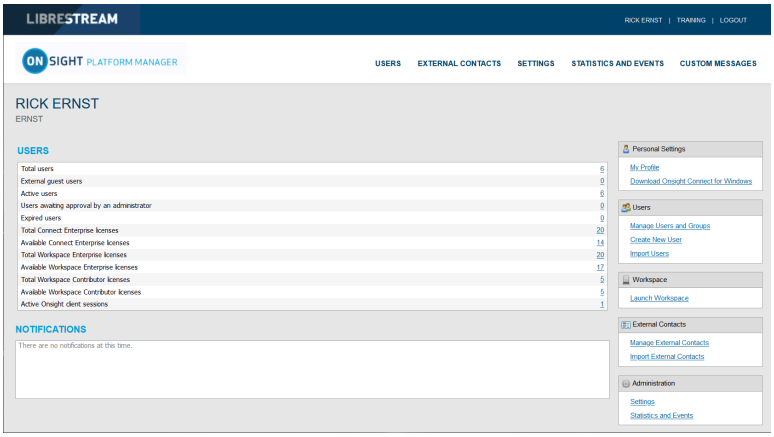


Figure 4-1 Dashboard

The Account Owner is the primary administrator. The Administrator does not consume any Onsight Connect endpoint licenses; therefore, in order to login to an Onsight Connect client as a user you must assign a client license to your Account Owner.

When logged in to OPM, locate **Personal Settings** to access **My Profile**. My Profile enables the administrator to configure their personal settings like any other user account including the assignment of licenses. Once licenses are assigned to the account, the administrator can also log in to an Onsight Connect client and use the features provided by the license type.

Administrators do not need to have licenses assigned in order to manage their OPM customer domain. You may create multiple administrator accounts.

4.1. Changing The Administrator's Password

1. Login to OPM and access your Dashboard.

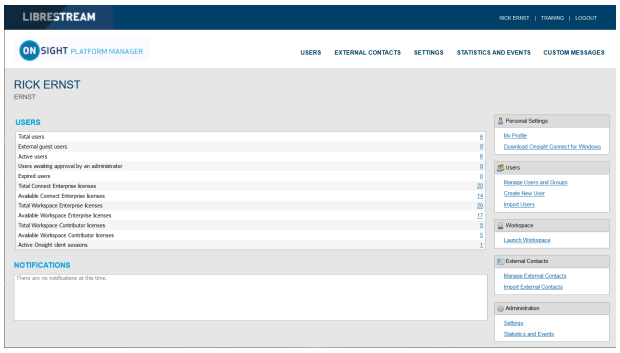


Figure 4-2 Dashboard

2. Locate **Personal Settings** on the right and select **My Profile**. This will take you to the **My Profile** configuration page.

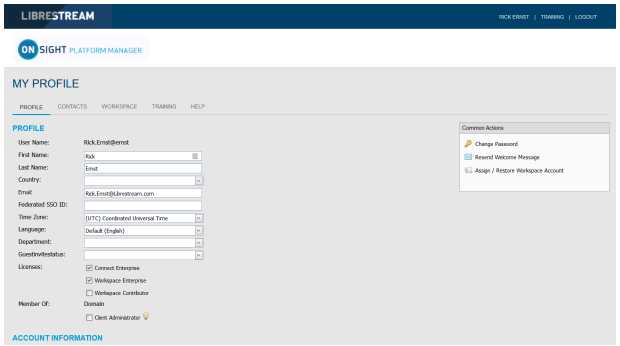


Figure 4-3 My Profile

3. Locate **Common Actions** on the right and select **Change Password**. Enter the new password into both provided fields.

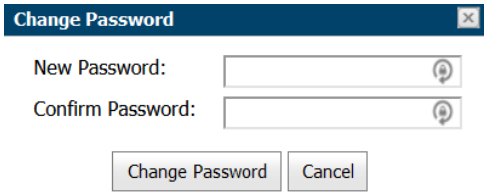


Figure 4-4 Change Password

Note: Your password must be different from the current password.

4. Click the **Change Password** button to save your changes.
This completes the procedure.

4.2. Changing The Administrator's Personal Contacts

Login to OPM.

1. Locate **Personal Settings** and select **My Profile**.

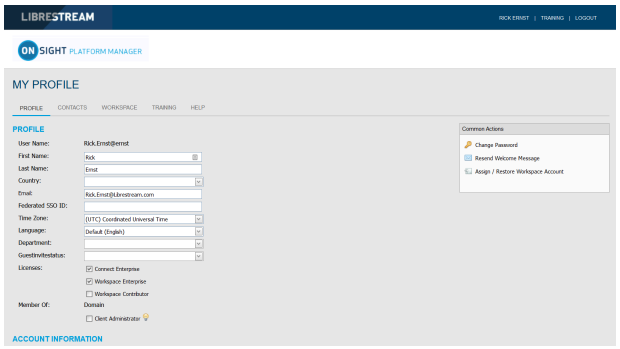


Figure 4-5 My Profile

2. Select the **CONTACTS** tab.

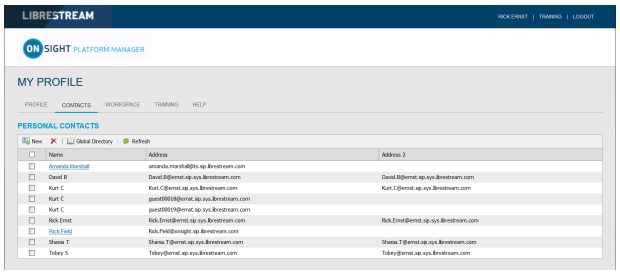


Figure 4-6 My Contacts

3. Click the **Global Directory** icon to search for a contact to add to your **Contacts** list.

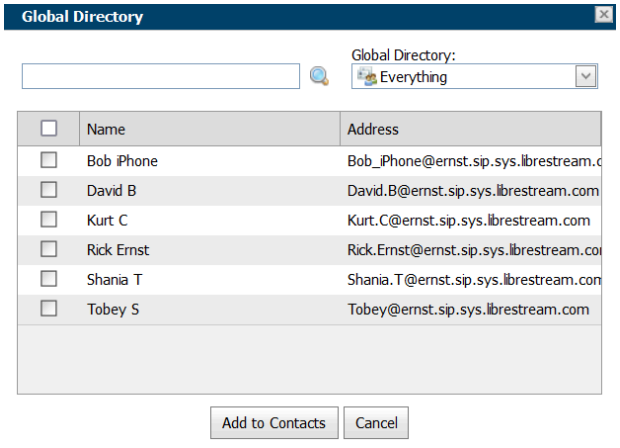


Figure 4-7 Global Directory

4. Enter a name to search and press the **Search** icon to see a list of all users.

5. Enable the check box next to the person's name and click **Add to Contacts**.

6. To manually create a contact, click the **New** icon. This is only necessary if you need to add a third-party contact.

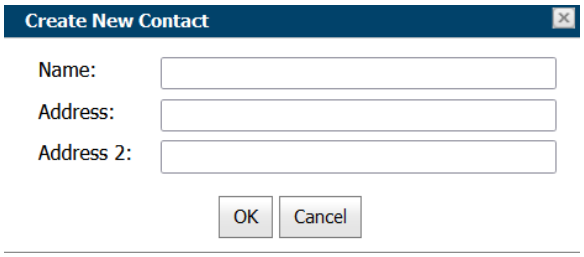


Figure 4-8 Create New Contact

7. Enter the **Name**, and Session Initiation Protocol (SIP) within the **Address** field for the contact. You can also enter an optional **Address 2**.

Note: The address must be in the `SIP URI` format, e.g., **user@sipdomain.com**.

8. Click **OK** to save.
   This completes the procedure.

4.3. Adding Administrators To OPM

You must login to OPM.

In order to add users, you will need to:

1. Select **USERS** within the main menu. The USERS page appears.

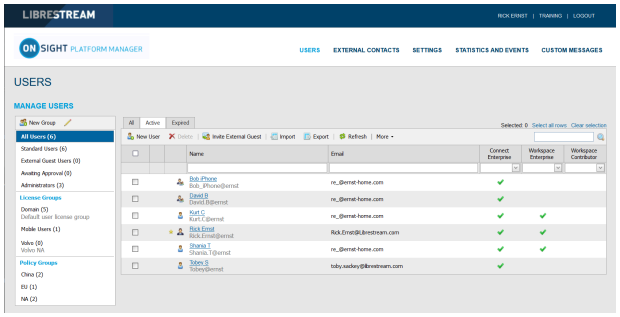


Figure 4-9 USERS

2. Click the **New User** icon. The CREATE NEW USER page appears.

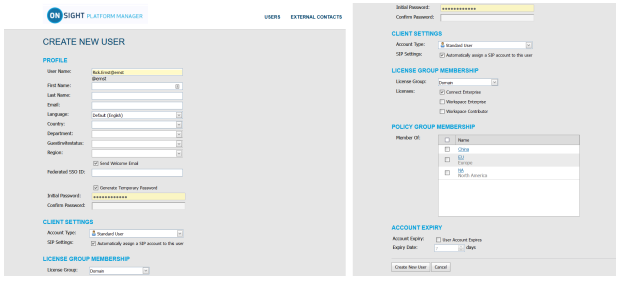


Figure 4-10 Create New User

3. Enter **PROFILE** information that includes:

   a. **User Name**

   b. **First Name**

   c. **Last Name**

d. **Email**

Note: 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 disable **Generate Temporary Password.** You will need to notify the new admins of their User Names and passwords.

e. Define **Language**, **Country**, **Department** and **Region** using the drop-down menus, as required.

f. If **Single Sign On** is enabled, enter the **Federated SSO ID** (if required). See the **SSO** section for details.

4. Under **CLIENT SETTINGS**, select **Administrator** for the **Account Type**.

5. Verify that the option to **Automatically assign a SIP account to this user** is enabled by default.

Note: This is required if you are assigning a Connect Enterprise license and want your administrators to be able to log in locally on an Onsight client and make calls.

6. By default, the **Administrator** will belong to the **domain license** group. You do not need to assign the administrator to a different license group.

7. By default, the **Administrator** belongs to the **domain policy group**. You do not need to assign the administrator to a different client policy group.

8. 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.
This completes the procedure.

5. USER LICENSES

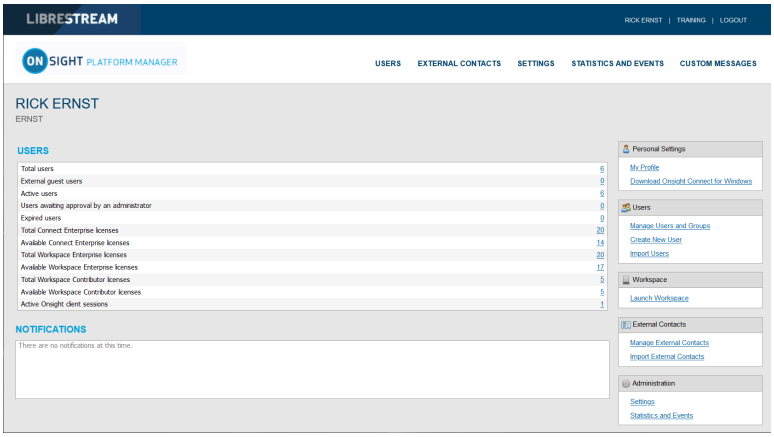


Figure 5-1 Dashboard

Onsight Platform manager supports three user license options:

- **Connect Enterprise** — Provides Onsight call services (SIP settings must be configured in the domain).
- **Workspace Enterprise** — Provides the enterprise user Workspace access based on administrator assigned permissions.
- **Workspace Contributor** — Provides the contributor user Workspace access to their upload folder and edit their content; access to other assets cannot be granted to the contributor.

Note: Workspace license types are mutually exclusive. A user cannot be assigned both Workspace license types. Each license enables features for the user within the Onsight Connect application. Users can have single or multiple licenses assigned to their account. All licenses allow the capture of content locally (images and recordings).

5.1. License Options

The following table outlines the valid license type assignment combinations:

Table 5-1 License Options

User	Connect Enterprise	Workspace Enterprise	Workspace Contributor
A	✓		
B		✓	
C			✓
D	✓	✓	
E	✓		✓

User A (Connect Enterprise):

Connect Enterprise users can log into **Onsight Connect,** make calls, capture content, and share content with other Connect Enterprise users.

User B (Workspace Enterprise):

Workspace Enterprise users can log into **Onsight Connect**, capture content, upload content to **Workspace**, and can log into Workspace to edit, manage, and collaborate on content. This includes any assets to which they have been granted permissions to access.

User C (Workspace Contributor):

Workspace Contributor users can log into **Onsight Connect**, capture content, upload content to **Workspace**, and can login to Workspace to access their upload folder content. This user cannot be granted access to content outside of their upload folder.

User D (Connect Enterprise with Workspace Enterprise):

Connect Enterprise users can log into **Onsight Connect**, make calls, capture content, and share content with other **Connect Enterprise** users. Also, with **Workspace Enterprise** users they can upload content to **Workspace**. This user can also log in to Workspace to edit, manage and collaborate on content. They may be granted permissions to access other content within Workspace outside of their upload folder.

User E (Connect Enterprise with Workspace Contributor):

Connect Enterprise users can log into **Onsight Connect**, make calls, capture content, and share content with other Connect Enterprise users. Also, with **Workspace Contributor** users, they can upload content to **Workspace**. This user can also login to **Workspace** to access their upload folder content. This user cannot be granted access to content outside of their upload folder.

5.2. Capture Mode

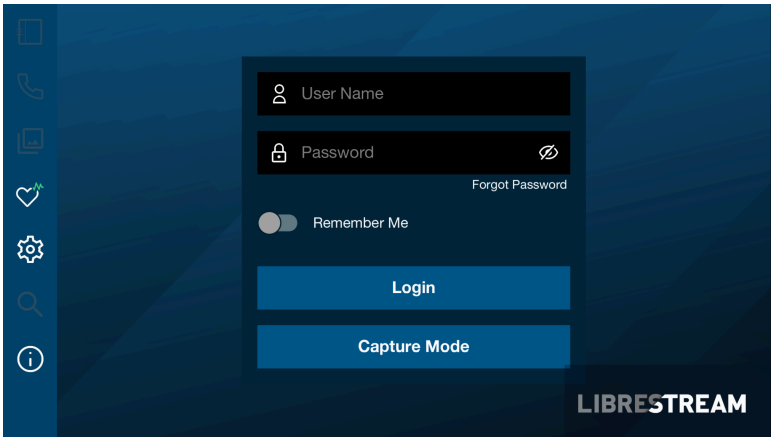


Figure 5-2 Capture Mode

Capture Mode provides offline use of Onsight Connect without requiring a login. From the login window for Onsight Connect, users can press the **Capture Mode** button to enter the **Onsight Connect Viewer**. This enables access to video sources for mobile device cameras as well as Onsight devices such as the **Cube** and **Hub** without requiring an Onsight user login.

Users who have not been assigned an Onsight account can download **Onsight Connect** and capture content immediately. All content is saved locally on their mobile device or Windows PC. Once they are assigned an account, they can login and access their previously captured images and recordings which can be shared in an Onsight call or uploaded to Workspace.

Once a user logs in to the Onsight Connect application with an Onsight user login, **Capture mode** is no longer available at the login window. An Onsight login must be used to gain access to the application from that point on.

6. MANAGE USERS & GROUPS

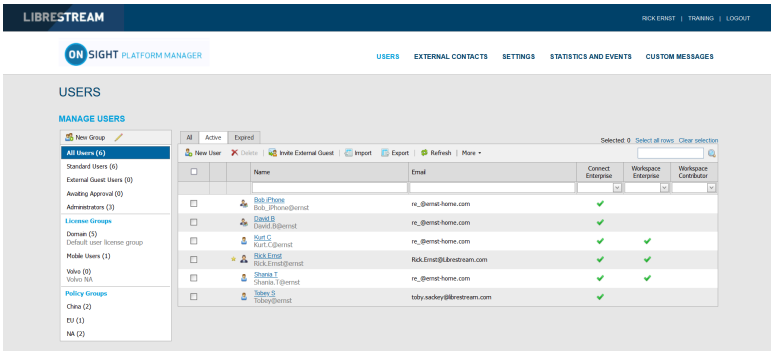


Figure 6-1 Manage User & Groups

Onsight administrators use OPM to centrally manage user licenses, contact lists, policies, and permissions. There are two main approaches to managing licenses within Onsight Platform Manager. **Select Users** from the main menu to enable you to manage:

- Domain license management
- License and Policy group management

6.1. Domain License and Policy Management

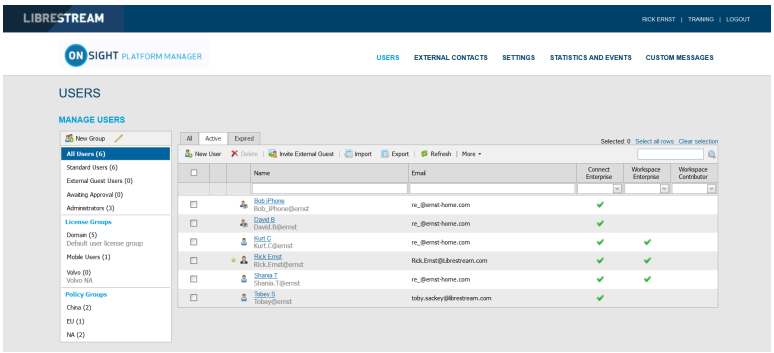


Figure 6-2 All Users/Domain License Group

The domain is the default license group. All licenses are under the domain's control, it is a single license pool from which all licenses are assigned to users. License types that are added to the domain can be assigned by an administrator to any user in the domain.

Client Policy can be set for all users by editing the **All Users** group.

Related information
Client Policy — Best Practices *(on page 117)*

6.2. License Group Management

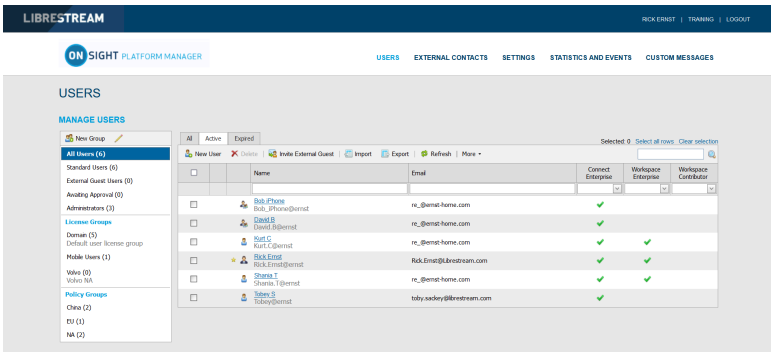


Figure 6-3 License Groups

License Group management is an optional method for managing licenses. It is enabled by request only. It enables an Onsight Administrator to create license groups and assign licenses from the domain to the license groups. Group members are added to each license group and are assigned licenses under the license groups' control.

When license groups are enabled the default domain is still active and acts as an independent license group. Licenses are transferred from the default domain to custom license groups. Once a license is transferred it is under the control of the license group.

Administrators and group administrators can create users within a license group providing that they have available licenses in the group. Users can be created without licenses, but they must be assigned a license before they become active.

Client Policy can be set independently for each license group.

Related information
Client Policy — Best Practices *(on page 117)*

6.3. License/Policy Groups & User Management

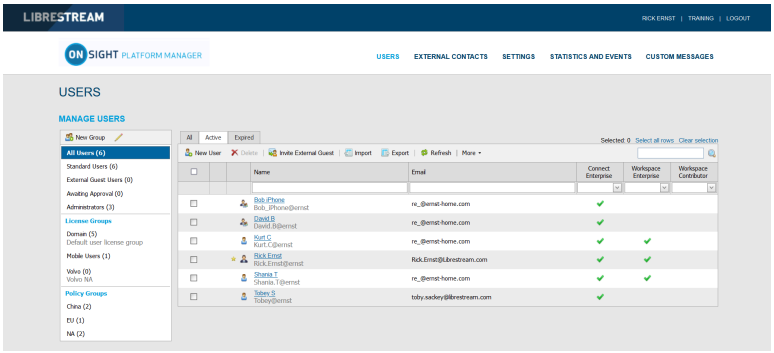


Figure 6-4 Policy and License Groups

OPM administrator can create two types of groups: **License** and **Policy**.

License Groups

License Groups are optional and can be enabled on request. They are used to apply **Client Policy** and assign licenses to group members. The administrator can assign licenses to different license groups. Administrators can be assigned to a group (Group Administrator). For example, an OPM administrator assigns 10 Connect Enterprises licenses to a **License Group**. A Group administrator can be assigned to manage and grant a maximum of 10 **Connect Enterprise** licenses to a maximum of 10 group members. If a **Connect Enterprise** user is deleted from the group; then the license becomes available for use and can be assigned to a new user. The OPM administrator can reassign licenses back to the domain or another license group.

Default groups cannot be deleted.

Policy Groups

Policy Groups are used to apply client policy to group members. Policy groups do not have license management capabilities. When using policy groups licenses are assigned to users from the domain license pool.

Administrator Override

An administrator can override group policy for a specific user by editing the user's **Client Policy** page. The user client policy settings will take precedence over any group client policy settings.

License Groups & Use

The use of **License Groups** is optional and must be enabled for your domain.

- You may leave all licenses assigned to your default domain. If you do not have a need for license management for custom groups then managing licenses from the domain pool is recommended.
- You can manage **Client Policy** using custom policy groups. If you do not need to manage client policy for custom groups, then you can set **Client Policy** for all users by editing the **Standard Users** client policy.
- If **External Guests** is enabled, you can manage client policy for them by editing the **External Guest Users** client policy.

- Domain licenses can be assigned by administrators and group administrators who have been assigned to groups.
- If license groups are not enabled for your domain, then are no restrictions on the number of users a group administrator can add to their group, providing there are available licenses in the domain.

User Management

The default options contained within the **MANAGE USERS** panel include:

- **All Users** includes everyone in the domain: Administrators, non-administrative users, and External Guest users. Includes client policy configuration. When a new user is added they are automatically a member of the All Users Group.
- **Standard Users,** by default, includes non-administrative users and Administrators (External Guest users are not included). Includes client policy configuration.
- **External Guest Users** (Optional) includes all External Guest Users and allows Client Policy configuration.
- **Awaiting Approval** indicates of the number of self-registered users awaiting Administrator approval. Client Policy is not applicable.
- **Administrators** indicates the number of administrator accounts. Client Policy is not included.
- **License Groups** (Optional) Includes custom license groups and the default Domain. Client policy is included.
- **Policy Groups** includes custom policy groups. License management is not included.

Note: Default groups cannot be deleted.

Related information
Client Policy — Best Practices *(on page 117)*

6.4. Adding a Group

Login to OPM.

To manually add a group, you will need to:

1. Select **USERS** from the main menu. The Users page appears.

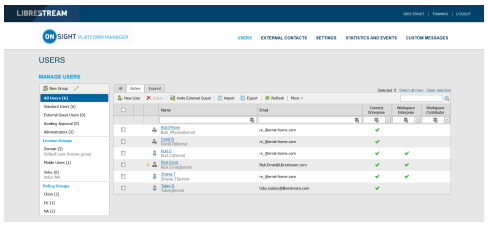


Figure 6-5 USERS

2. To add a custom group, click the **New Group** icon in the **MANAGE USERS** panel. The Create New Group window appears.

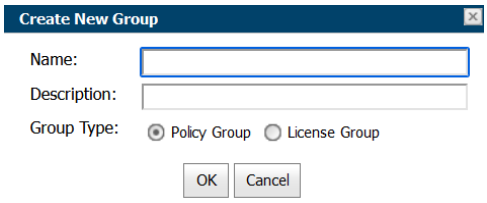


Figure 6-6 Create New Group

3. Enter information within the **Name** and **Description** fields.
4. Define **Group Type** as:
    - **Policy Group**
    - **License Group**

5. Click **OK**.

Note: License groups must have a defined number of licenses assigned to them by the administrator. Users can only be added to the license group providing there are available licenses. Both Policy and License groups have Client Policy and Permissions included with them.

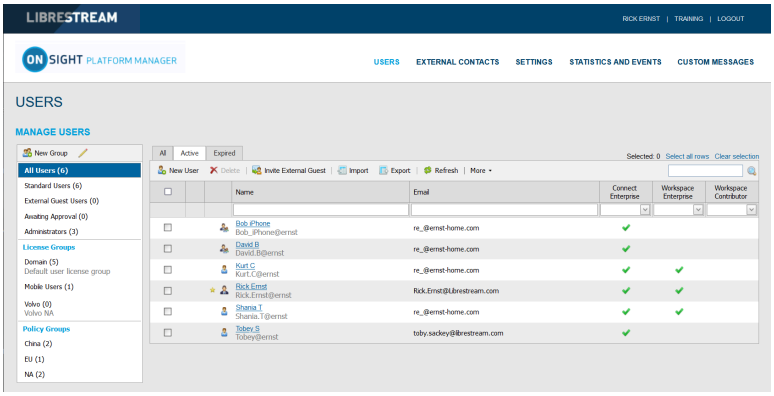
This completes the procedure.

For more information, refer to Client Policy & Permissions *(on page 73)* section.

Related information

Client Policy & Permissions *(on page 73)*
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

7. USERS AND GROUPS



There are three methods for an Administrator to add Users:

1. Manually create a new user.
2. Import users from a file (e.g., SampleUserImport.csv).
3. Self-registration using the OPM Self-registration web page.

7.1. Create New User

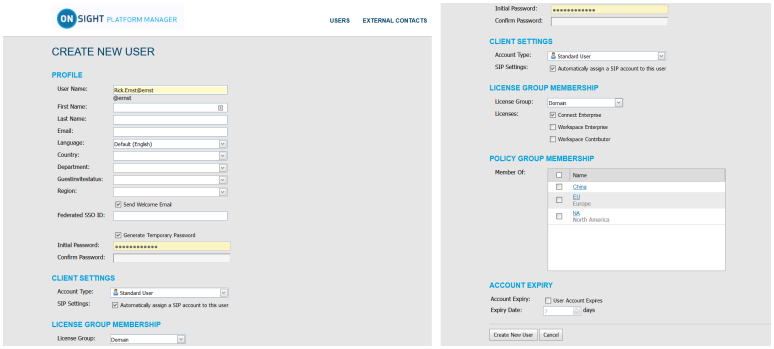


Figure 7-1 Create a New User

Select **USERS** from the main menu and click the **New User** icon to access the **CREATE NEW USER** window. To create a new user, you will need to provide details for:

- **PROFILE** — Provide user information details that include **User Name**, **First Name**, **Last Name**, **Email** and use drop-down menus to indicate: **Language**, **Country**, **Department** and **Region** etc.
- **CLIENT SETTINGS** — Define the **Account Type** using the drop-down menu as an **Administrator**, **Group Administrator**, or **Standard User**.
- **LICENSE GROUP MEMBERSHIP** — Assign the new user to a License Group as required and enable the check box to indicate the License type (**Connect Enterprise**, **Workspace Enterprise**, or **Workspace Contributor**).
- **POLICY GROUP MEMBERSHIP**— Assign the new user to a **Policy Group** as required.
- **ACCOUNT EXPIRY**— Enable the option for **User Account Expires** and provide an **Expiry Date** as required.

and click the **Create New User** button.

7.1.1. Creating a New User

Login to OPM.

To manually create a new user account, you will need to:

1. Select **USERS** from the main menu. The USERS page appears.

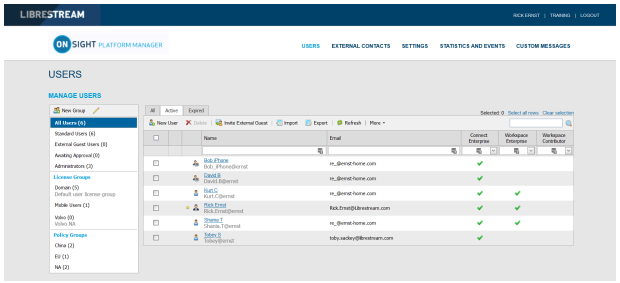


Figure 7-2 Users Page

2. Click the **New User** icon. You will be presented with the **CREATE NEW USER** window.

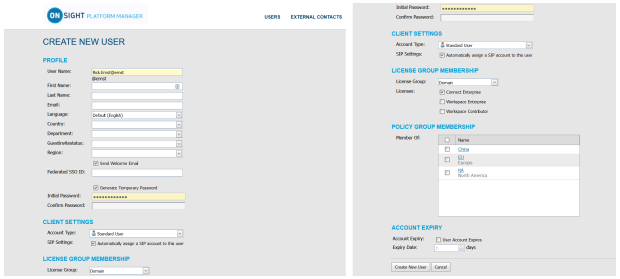


Figure 7-3 Creating a New User

Note: If the **New User** icon is missing, then you are unable to add new users. Revisit your **Client Policy** settings for **Allow New Contacts** as required.

3. Enter **PROFILE** information for the new user. By default, the **Send Welcome Email** and **Generate Temporary Password** options are selected.

4. Within **CLIENT SETTINGS**, select the Account Type: **Standard User**, **Administrator**, or **Group Administrator**.

5. The **Automatically assign a SIP account to this user** option is selected by default. See **SETTINGS > SIP** for details on configuring the **Auto-Assignment SIP Pool**.

Note: Existing Users can have their SIP Settings assigned or updated from the Auto-Assignment Pool by accessing the **Users Client Settings** page and pressing **Assign / Restore SIP Account** in the **Common Actions** section.

6. Select the **LICENSE GROUP MEMBERSHIP** for the user. By default, all users belong to the **Domain license group** if you have created licenses groups, select the group and license type(s) to which you are assigning the user. You may also want to assign the user to a **Client policy group** by selecting the **Member Of** check box to indicate which group they belong to.

Note: Both **License groups** and **Policy groups** have **Client policy** and **Permission** settings associated with them. If you have defined a **Client Policy** within the **License group**, you do not need to assign a **Policy group** to the user.

- **Optional**: You may set the **User Account Expires** check box and **Expiry date** for the user.
- To apply your changes, click the **New User** button at the bottom of the window.
- To set a user as **Client Administrator**, click on the user's name in the list on the **USERS** page. Select the **Client Administrator** check box. The user is now able to edit all settings on an endpoint.

7. Click the **Create New User** button.
   This completes the procedure.

Note: *The Client Administrator setting for user accounts is deprecated. It is recommended that users be added to policy groups to control client permissions. However, users who currently have Client Administrator enabled for their user account can be managed through the Client Administrator group policy. Also, if you are transitioning from OMS to OPM, the Client Administrator setting is the only method of granting admin rights to a user.

7.2. Welcome Email

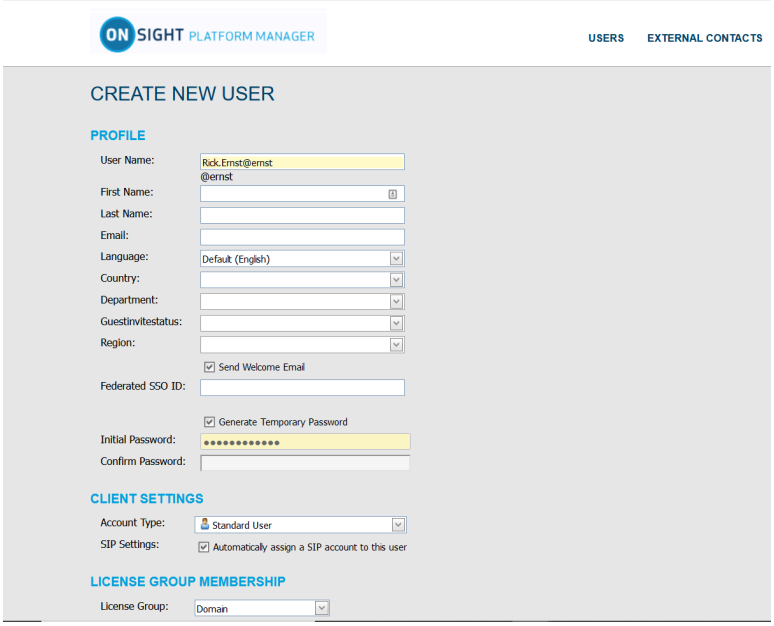


Figure 7-4 Welcome Email Option

The Welcome email notifies new users of their Onsight Connect account and provides links to **Download and install Onsight Connect** and **Login** . The Welcome email can be enabled as a check box within the **PROFILE** section when you create a new user. Thereafter, the Welcome message can be resent, if necessary. Click USERS from the main menu and select a User from the user list. Locate **Common Actions** and select **Resend Welcome Message**.

7.2.1. On-Premises Welcome Email

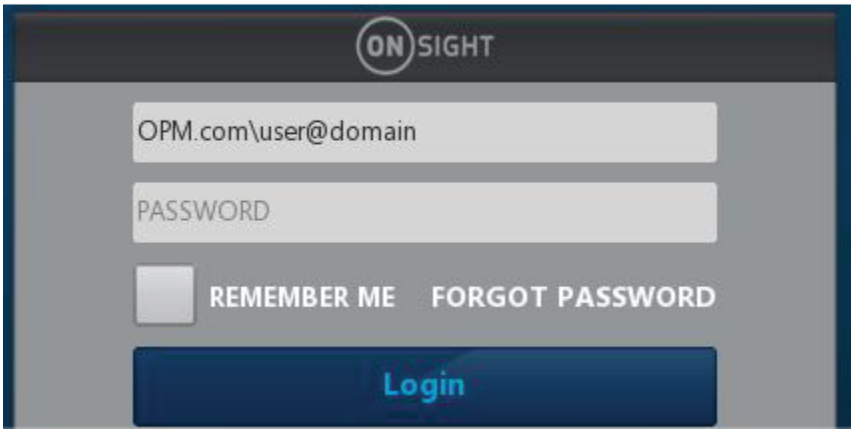


Figure 7-5 On-premises URL

On-premises Welcome emails will contain a **Login to Onsight Connect** link which will launch Onsight Connect and direct it to your Onsight Platform Manager's URL. The URL in the link must match the URL that was configured during installation your On-premises server installation.

The format must be `OPM.com\user@domain`, where OPM.com is the domain name of your server.

If using a port other than 443 for your OPM-OP installation, then the format must be `OPM.com:port\user@domain`, where OPM.com:port is the domain name of your server and the port number being used. Eg., `OPM.com:8083\user@domain`.

Once connected, they will be asked to confirm that they want to Use this Onsight Account Service from now on. The user must click **Yes** to accept the changes. Going forward, they will just enter their **User Name** and **PASSWORD** to login or enable the **REMEMBER ME** option to automate the login process.

7.2.2. On-premises-URL Formats

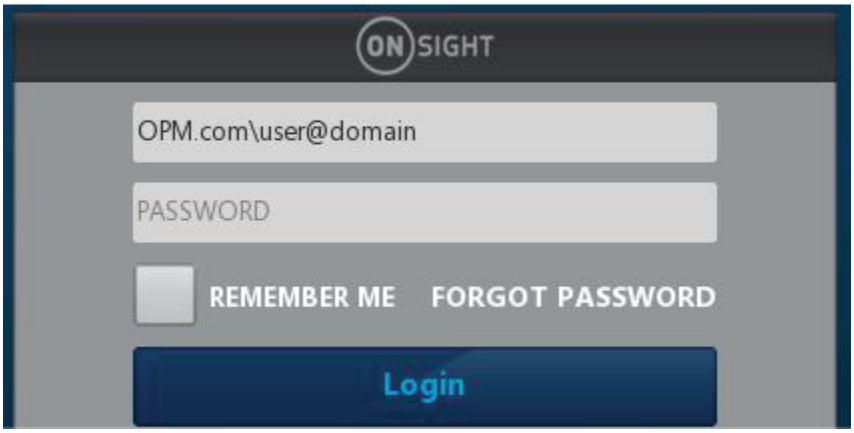


Figure 7-6 On-premises URL

When specifying the OPM path in the user name field at log in, shortened formats are accepted. Typical hard coded defaults are used in the case where elements are missing from the path.

The username field is assumed to contain an OPM path if the text entered contains a backslash '`\`': `[OPM URI]\user@domain`

The 'OPM URI' part will be parsed as a URI, so only valid relative or absolute URIs will be accepted (e.g., no spaces in host name). Acceptable formats include:

- An absolute URI: `https://[authority]/[path]\user@domain`.
- OPM host only: `[host]\user@domain`. Scheme will be set to https, path will be set to 'OamClientWebService'.
- OPM host and path: `[host]/[path]\user@domain`. Scheme will be set to https. Host and path are used as-is.
- OPM scheme and host: `https://[host]\user@domain`. Path will be set to **OamClientWebService**. Scheme and host are used as-is.
- Only https schemes are accepted.

Also, contained in the Welcome Message are links to download Onsight Connect from your Onsight Platform Manager and download links to both the **iOS App Store** and **Android Google Play** store. The user can click **Download for Windows** or **Download for iOS** or **Android**.

Once the user has installed Onsight Connect, they MUST click the **Login to Onsight Connect** button to correctly configure the software to log in to your OPM installation.

Mobile Device users must install Onsight Connect from either the **Apple Store** or **Google Play Store**.

7.3. User Email Requirement

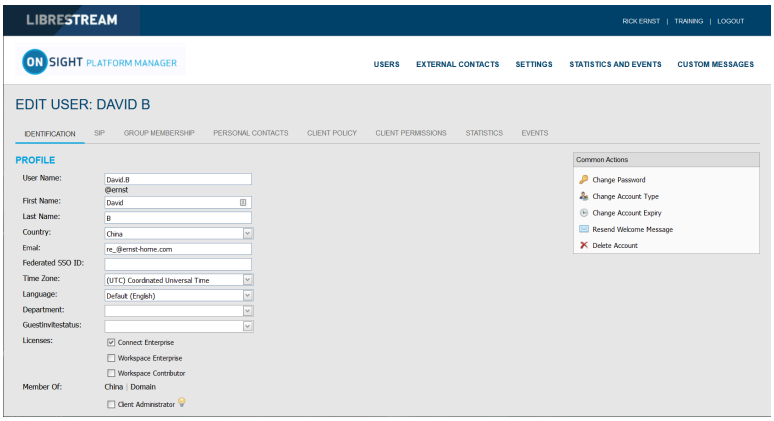


Figure 7-7 User Email Requirement

Email addresses are optional within OPM. **However, if a user does not have a configured email address, they won't get notification emails (Welcome emails, password reset emails, etc.)**. If they request a password reset, the page will say "`If a valid email is configured...`" but won't confirm whether an email is configured for their account. On the user's **PROFILE** page, within the **Common Actions** section, the **Resend Welcome Email** will be hidden if the user has no email address. Welcome emails notify users how to **download**, **install** and **login** to Onsight Connect.

Emails are required under the following conditions:

- Guest users require a valid email address or phone number to receive an invite.
- The **Account Owner** user must have a valid email address.

Email Requirements for Security & SSO Settings

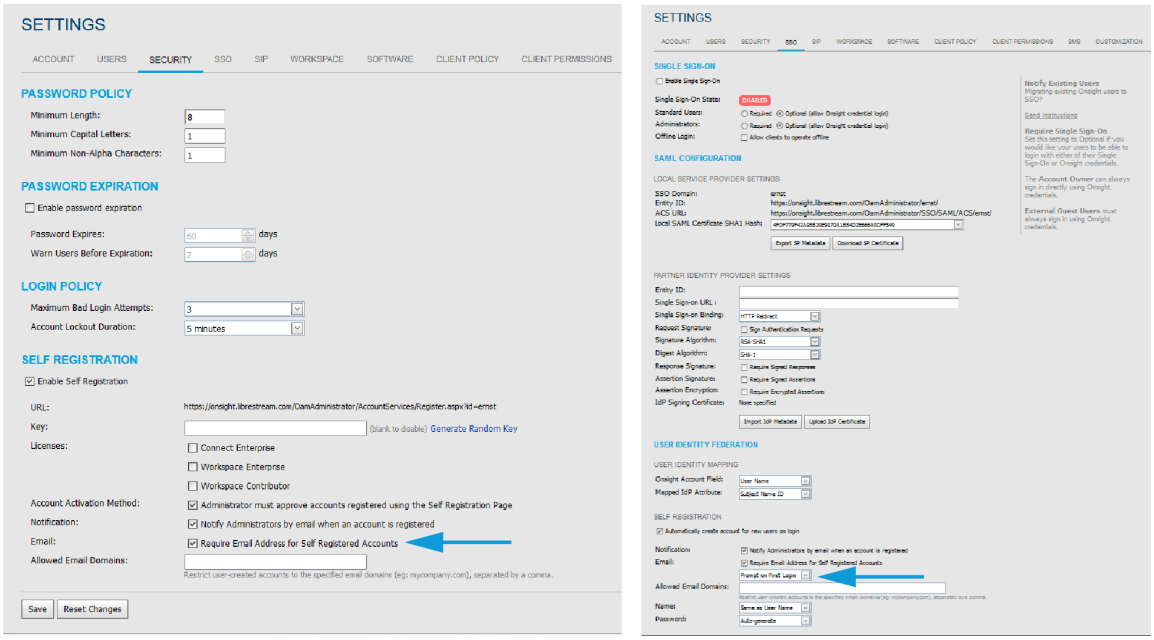


Figure 7-8 Security & SSO Settings

The email requirement for self-registered users (either through the self-registration page or provisioned through SSO), is configurable on the **SETTINGS > SECURITY** and **SETTINGS > > SSO** pages.

If set to **Required** — Users that register via the self-registration page must enter an email.

SSO Users— If the email provided as an Attribute is blank, provisioning will fail. If Email is set to **Prompt on First Login**, the user must enter an email.

Note: Require Email Address for Self-Registered Accounts cannot be unchecked.

If set to **Optional** — Users that register via the self-registration page can optionally enter an email. If not provided, email will be blank, and they won't receive a welcome email.

SSO Users — If the email provided as an Attribute is blank, provisioning proceeds with a blank email. If email is set to **Prompt**, the user can optionally enter an email.

Note: Require Email Address for Self-registered Accounts can be unchecked.

Any email provided by an SSO attribute does not require verification.

Note: Any email provided by a user during self-registration requires verification before the account can be used. Any email provided by an SSO attribute does not require verification.

7.4. User Account Types and Permissions

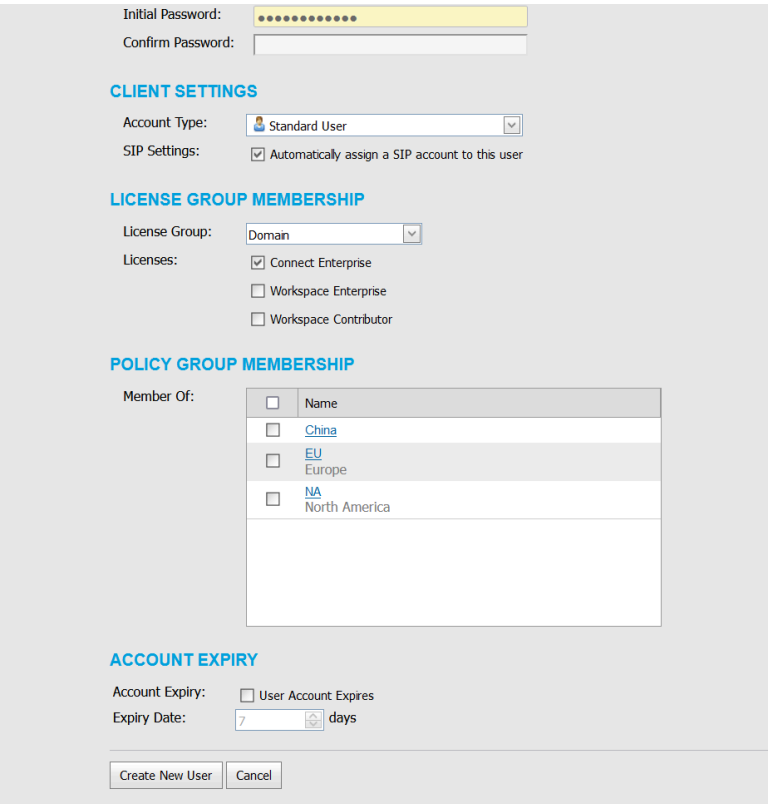


Figure 7-9 User Account Type

Within **CLIENT SETTINGS**, the **Account Type** drop-down menu indicates the level of access the User has to Onsight Platform Manager. The licenses assigned to the user determines the features the user has access to in Onsight Connect and Workspace. Client policy and client permissions dictate the users access to settings on the client apps. **Account Type** options include **Administrator**, **Group Administrator** and **Standard User**.

Administrator: Full Access to the OPM and the domain settings including user management.

Note: Only an Administrator can assign licenses to license groups. When a domain is first created for a customer the Account Owner is the only Administrator. The Account Owner must create additional administrators.

Standard User Permissions: A **Standard User** does not have administration privileges. They are subject to the group policy and permissions assigned to them through group membership by the OPM administrator. They can invite External Guests if **Allow users to invite guests** is enabled in the domain (Requires the External Guest — Master License for the domain).

Group Administrator Permissions: A Group Administrator has access to the group level settings to which they have been assigned including:

- Modify users that are in their group (change settings, passwords, etc.).
- Create and delete users within their group.
- Define **Client Policy** for the group.

For **License Groups**, group administrators will be able to add users to the group based on the number of licenses assigned to the group by the OPM Administrator.

7.5. Promoting Users and Assigning a Group Administrator

Login to OPM.

Managing group administrators is a two-step process. You must change a standard user to a group administrator and then assign them to a group.

Promoting a Standard User to an Administrator

1. To promote a user to be a **Group Administrator**, you will need to Login to OPM and select **USERS** from the main menu. The USERS page appears.

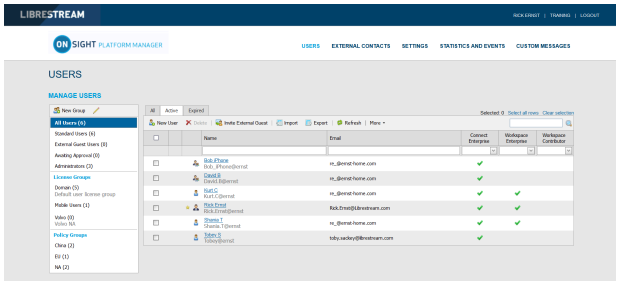


Figure 7-10 Users Page

2. Click to select a `Username` within the Users table.

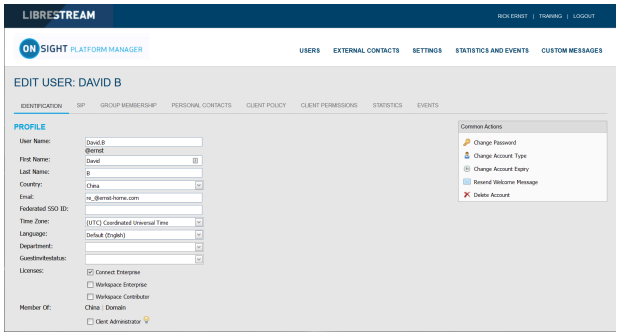


Figure 7-11 Edit User Page

3. Locate the **Common Actions** area select **Change Account Type.**
4. Select `Group Administrator` from the **Account Type** and select **Change Account Type** to apply the change. A message appears stating `Account type changed successfully.`

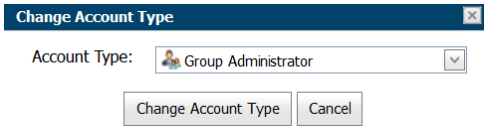


Figure 7-12 Change Account Type

5. Click **OK**.

Assigning an Administrator to a Group

To assign a group administrator to a Group, you will need to:

6. Select **Users** from the main menu and select the group to assign a group administrator.

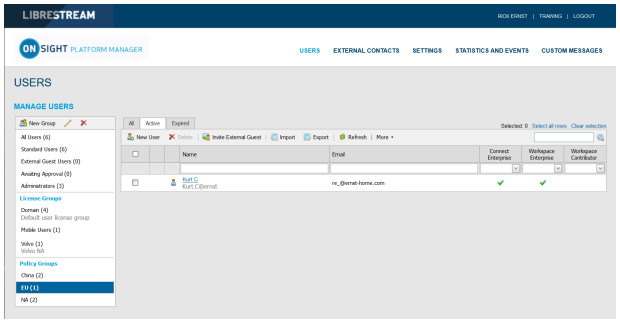


Figure 7-13 Selecting a Group

7. Click the **Modify Group** icon to edit. The EDIT GROUP page appears.

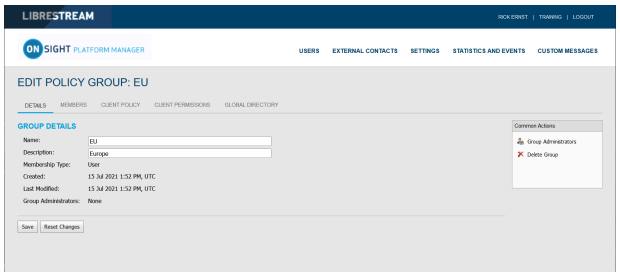


Figure 7-14 Edit Policy Group

8. In the **Common Actions** section, click **New Group**.

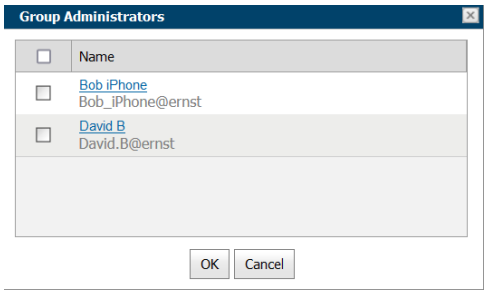


Figure 7-15 Group Administrators

9. Enable the check box next to one or more `Group Administrator(s)` from the list; and click **OK**. The Group Administrators section updates accordingly.

10. Click **Save**.
    This completes the procedure.

7.6. Edit Groups

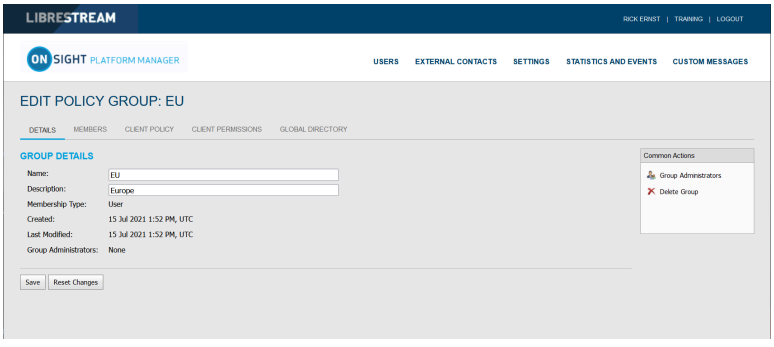


Figure 7-16 Edit a Group

To edit a group, select **USERS** from the main menu and select a group within the **MANAGE USERS** panel. Click the **Modify Group** (Pencil) icon to open the **GROUP DETAILS** page. The **GROUP DETAILS** page includes:

- **Name**
- **Description**
- **Membership Type**
- **Created date**
- **Last Modified**
- **License totals**
- **Group Administrators**

Additional tabs are available for editing the group that include **MEMBERS**, **CLIENT POLICY**, **CLIENT PERMISSIONS** and **GLOBAL DIRECTORY**.

The **Common Actions** section enables you to modify **Group Administrator** and **Delete Groups**.

Related information
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

7.6.1. Adding/Removing Group Members

Login to OPM and select **USERS** from the main menu and select a group within the **MANAGE USERS** panel and click the **Modify Group** (Pencil) icon to open the **EDIT GROUP** page.

To assign members to a group you can:

1. Select the **Members** tab and click the **Add Members** icon to add users to the group.

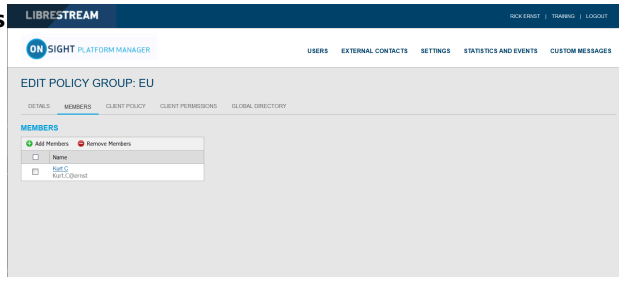


Figure 7-17 Edit Policy Group

2. Enable the check boxes for the users you want to add and press the **Add Selected Members** button.

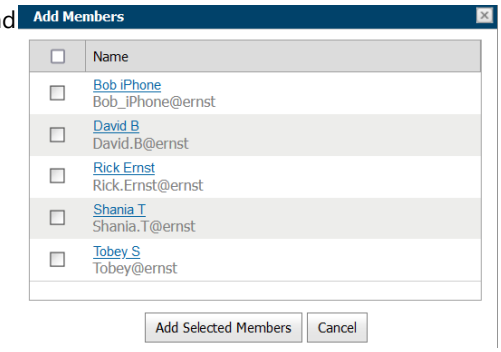


Figure 7-18 Add members

3. To remove members, enable the check box next to User's name list and press the **Remove Members** icon.

   This completes the procedure.

7.6.2. Assigning Group Administrators

Select **USERS** from the main menu and select a group within the **MANAGE USERS** panel and click the **Modify Group** (Pencil) icon to open the **EDIT GROUP** page.

To assign a group administrator you will need to:

1. Select **USERS** from the main menu and select a group.
2. Click the **Modify Group** (Pencil) icon to edit the group within the DETAILS page .

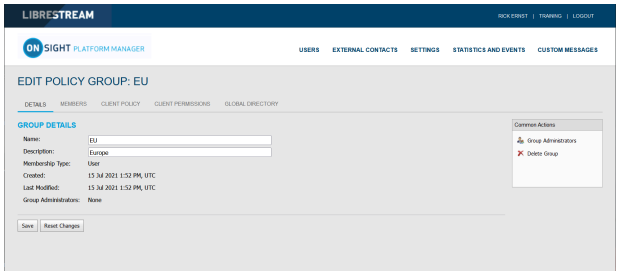


Figure 7-19 Group Details

3. Locate the **Common Actions** section and click **New Group**. A list of users with group administrator privileges is displayed.

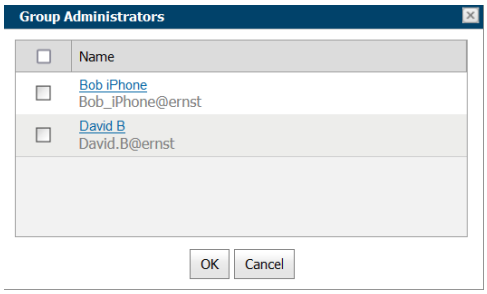


Figure 7-20 Group Administrators

4. Enable the check box next to one or more `Group Administrator(s)` from the list; and click **OK**.
5. Click **Save** to finalize your changes.
   This completes the procedure.

7.6.3. Edit Client Policy and Permissions

Login to OPM and select **USERS** from the main menu and select a group within the **MANAGE USERS** panel and click the **Modify Group** (Pencil) icon to open the **EDIT GROUP** page.

To modify Client Policy and Permissions for a group, you will need to:

1. Select the **CLIENT POLICY** tab to configure endpoint settings.

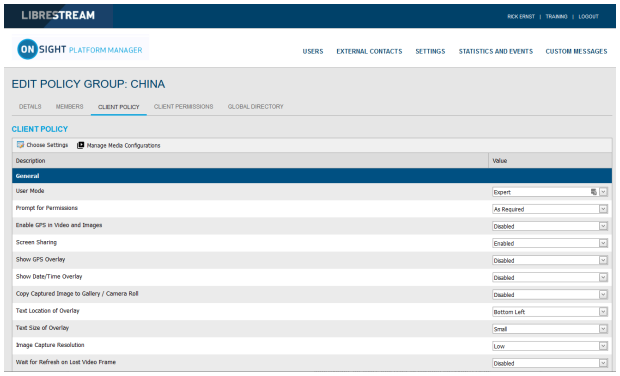


Figure 7-21 Edit Policy Group

2. Click **Choose Settings** to add the settings you want to control. Enable the categories and click **OK**.

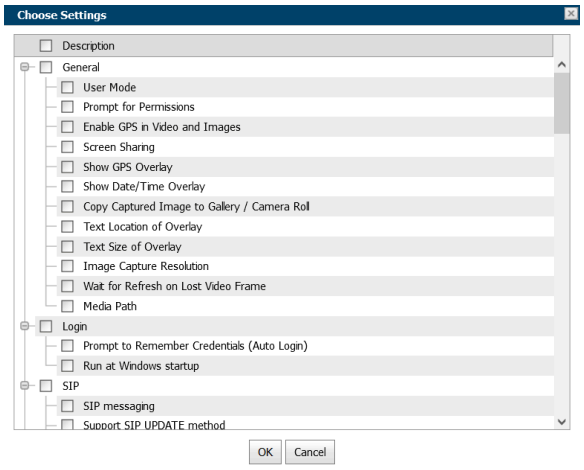


Figure 7-22 Choose Settings

3. Set the **Value** for each category and press **Save**.

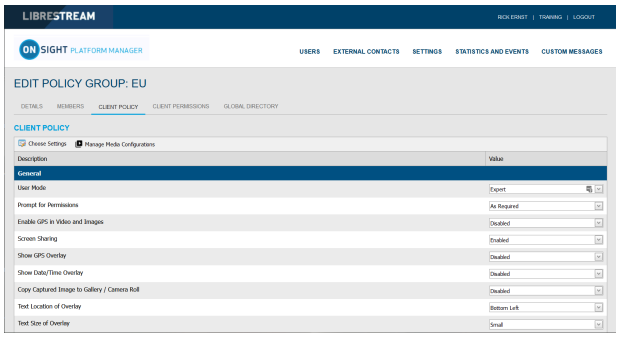


Figure 7-23 Client Policy

4. Select the **CLIENT PERMISSIONS** tab.

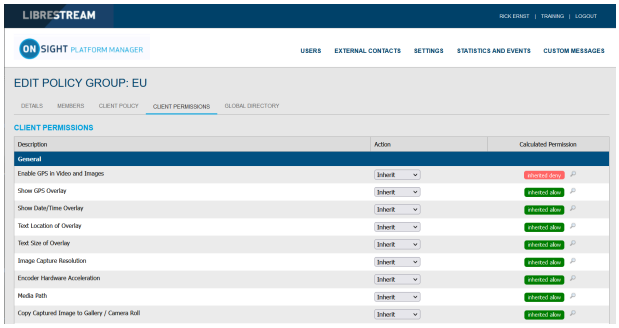


Figure 7-24 Client Permissions

5. Set the action as **Inherit**, **Allow**, or **Deny** for each setting.

Note: Inherit is the default permission, the client will inherit settings from any group to which the user is a member if the setting is not included in the current policy. Deny will not allow the user to edit settings in the Onsight Connect application. Allow will let the user edit settings in the Onsight Connect application.

This completes the procedure.

Refer to Client Policy & Permissions *(on page 73)* for a more detailed description of the actions.

The **Onsight Platform Management Settings Template** describes and provides best practices for each available policy setting and permission.

Related information

Client Policy & Permissions *(on page 73)*
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

7.6.4. Global Directory

7.6.4.1. Global Directory Availability

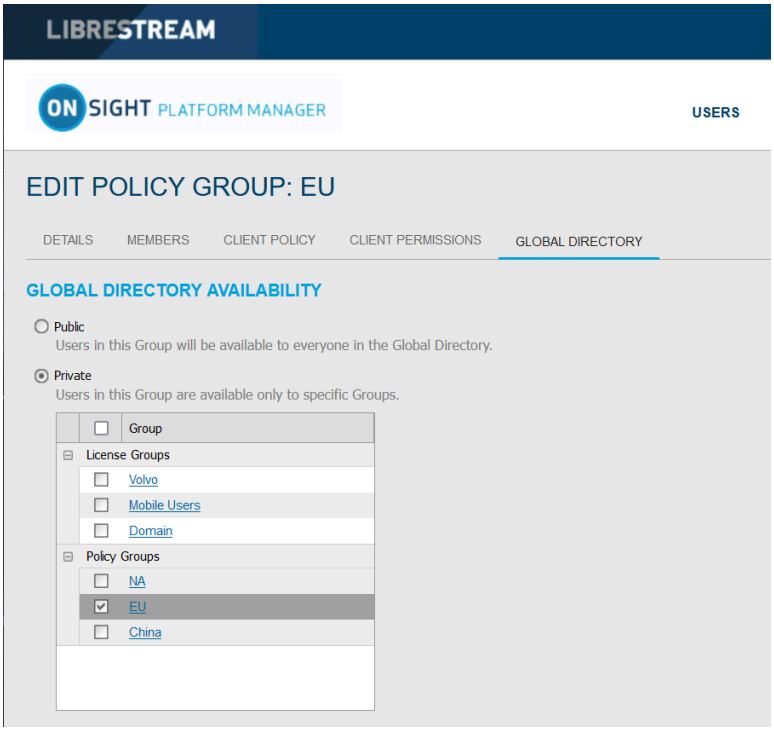


Figure 7-25 Edit Policy Group

To edit the Global Directory, select **USERS** from the main menu and select a group within the **MANAGE USERS** panel. Click the **Modify Group** (Pencil) icon and select the **GLOBAL DIRECTORY** tab. **GLOBAL DIRECTORY AVAILABILITY** filters control whether the current group is visible in the Global Directory.

- Select **Public** to make the members of the group visible to all groups in the Global Directory.
- Select **Private** to make this group visible to select groups in the Global Directory. Select the groups to which you want to be visible. E.g., you may only want the Field Service group to be visible to the Repair Depot group members.

Tip: Think of this as, who can search for me?

7.6.4.2. Global Directory Filter

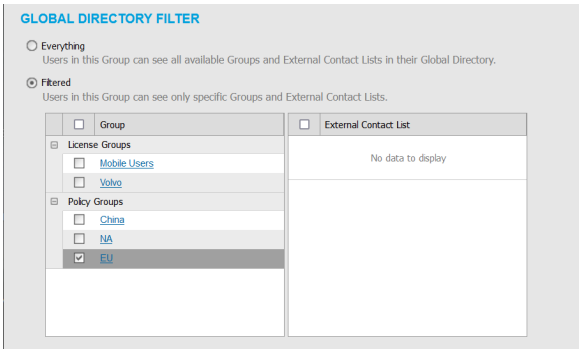


Figure 7-26 GLOBAL DIRECTORY FILTER

Global Directory Filter controls **who is visible to the current group** in the **Global Directory**.

1. Enable the **Everything** check box if you want the group to be able to view all groups and contacts in the Global Directory.
2. Enable the **Filtered** option to limit search visibility to the current group. Enable the check boxes for groups and contact lists you want to make available to the current Group. E.g., you may only want the **Field Service** group to be able to search for the **Repair Depot** group members.

7.6.4.3. Default Contacts

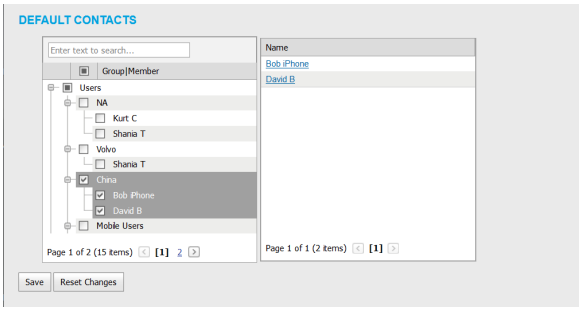


Figure 7-27 Default Contacts

DEFAULT CONTACTS control which contacts are automatically included in a group member's contact list when they log into the Onsight Connect application.

1. Enable the check box for the group or individual members of the group you want to add to the default contact list for the current group. Deselect and save to remove contacts.
2. Press **Save** to keep your changes.

Note: External Contact lists must be created on the **EXTERNAL CONTACTS** tab and assigned to groups before they are available in the **Global Directory Filter** for selection.

7.7. Import/Export Users

An OPM Administrator can import users using a Comma Separated Value File (CSV) created from the import template. This is the recommended method when creating new users and assigning licenses.

Best Practices for Importing Contacts

For most situations, including the first time you import users, you will need to include the following column headings in your import file:

- **UserName**
- **FirstName**
- **LastName**
- **EmailAddress** (Optional but is required when you want to use system notifications and features such as password change.)
- **GroupMembership** (Optional)

Importing users with this minimum information is sufficient to have all users configured correctly with the default settings in your domain.

SIP Settings can be automatically configured by selecting **Automatically assign SIP accounts to new users** during the import step. This is the best way to ensure your SIP accounts are configured correctly for each user.

Special cases where you need to include more than the basic user information include:

- **Single Sign On (SSO)**
- **Private SIP Server settings**
- **Passwords** (Use when not relying on the system to generate temporary passwords for users.)

7.7.1. Creating a Users Import Template

Login to OPM and select **USERS** from the main menu.

To manually create a users Import Template, you will need to:

1. Click the **Import** icon.

Figure 7-28 Import from File

2. Click the **Download Import Template** link.
3. Once downloaded, open the `SampleUserImport.csv` within your spreadsheet application. For example, Microsoft Excel, OpenOffice Calc, etc.
4. Follow the formatting conventions outlined in the **CSV Import Instructions** and enter information as required.

Importing a Users Import Template

5. Locate the **File to Import** field and click the **Browse...** button. A **File Upload** window appears.

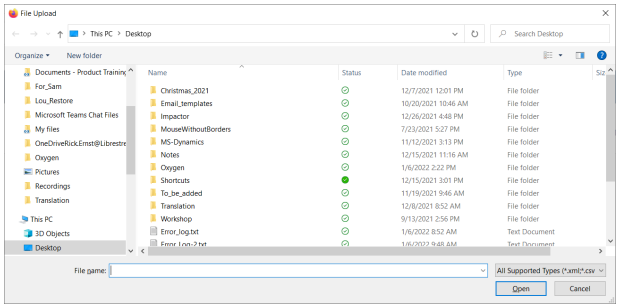


Figure 7-29 File Upload

6. Navigate to and select your `Users Import template` and click **Open**.

7. Click **Upload**.
   This completes the procedure.

7.7.2. Importing Users

Login to OPM and select **USERS** from the main menu. You must have previously downloaded and modified an Import Template as a CSV file. Refer to Creating a Users Import Template.

To import users using a template, you will need to:

1. Click the **Import** icon.

2. Select **Users** from the **Import Mode** drop down menu.

Tip: Setting External Contacts as the Import Mode will import the external contacts listed in a `contacts.csv` or `contacts.xml` file. Refer to the **CSV Import Instructions** for details on the EXTERNAL CONTACTS format. The external contacts file must be a separate file from the users import file.

Note: On the **EXTERNAL CONTACTS** page, you can select the **More > Export** option to download a contact's file template.

3. Locate the **File to Import** field and click the **Browse...** button. A **File Upload** window appears.

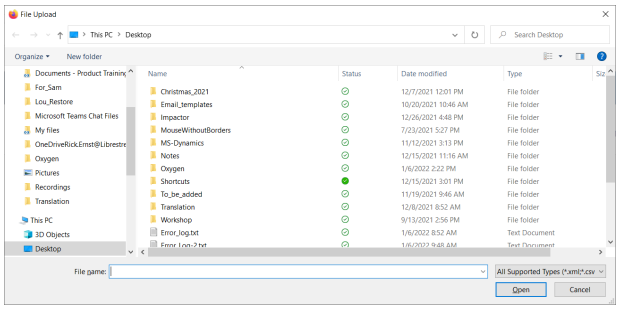


Figure 7-30 File Upload

4. Navigate to and select your `Users Import template` and click **Open**.

5. Click **Upload**. The Import Users window appears.

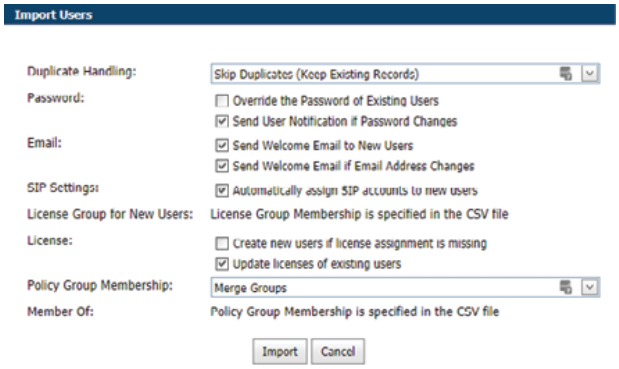


Figure 7-31 Import Users

6. Determine how you would like to handle duplicates:
    - **Skip Duplicates**(Keep Existing Records) or
    - **Update existing records**.
7. In the **Password** section, determine how you would like to import passwords:
    - **Override the Password of Existing Users**.
    - **Send User Notification if Password Changes**.
8. In the **Email** section, select the relevant options:
    - **Send Welcome Email to New Users**.
    - **Send Welcome Email if Email Address Changes**.
9. **SIP Settings** — Enable the **Automatically assign SIP accounts to new users** check box. This is an important step in configuring users accounts to ensure they are ready to make Onsight Calls.
10. The License Group for New Users is specified within the CSV file.
11. Licenses — Enable the appropriate options:
    a. **Create new users if license assignment is missing**.
    b. Update licenses of existing users as:
        i. **Connect Enterprise**
        ii. **Workspace Enterprise**
        iii. **Workspace Contributor**

    Note: The license types you are assigning to each user must be available in the chosen license group.
12. In the **Policy Group Membership** section, determine how you would like to assign group membership to the existing users. In this case, you are importing an Onsight User's file to reconfigure the existing users accounts. Select from:
    a. **Merge Groups** — Enables users to be members of multiple groups
    b. **Overwrite Groups** — Modifies the assigned groups.

13. In the **Member Of** section, it states that Policy Group membership is specified in the CSV file.

14. Select **Import** to continue. The **Import Results** window appears.

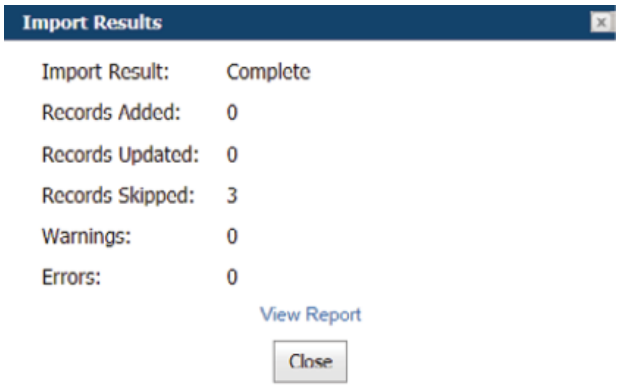


Figure 7-32 Import Results

This completes the procedure.

Note: You must use the **License Group for New Users** field to assign license group membership when importing users and assigning licenses. This means only members of the same License Group can be imported by the specified user file. The GroupMembership field of SampleUserImport.csv file cannot be used to specify license group membership.

When importing users into a License group there must be enough available licenses for each type being assigned to each user.

SSO — If you are using SSO and are using the **Federated SSO ID** to provide identity mapping between your enterprise users and the Onsight User Accounts, you must populate the Federated SSO ID field for each user in the UserImport.csv file. The Federated SSO ID must match the Mapped IdP Attribute you have configured on the SSO Settings page.

7.8. Export Users

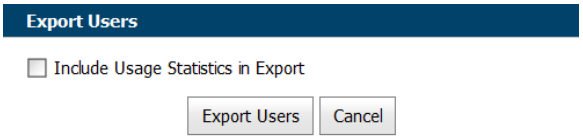


Figure 7-33 Export Users

Click **USERS** from the main menu and click on **Export** to download a CSV file containing a list of all users in the domain. You can choose to include **Usage Statistics** in the report as necessary.

7.9. Self-Register Users

The Onsight Administrator can enable self-registration for Onsight accounts. The administrator distributes the link to the self-registration page with instructions to the Onsight account candidates.

Users who are directed to self-register will be asked to provide the following information on the **REGISTER FOR AN ACCOUNT** page.

- **User Name**
- **Initial Password**
- **First Name**
- **Last Name**
- **Email**
- **Self-Registration Key** (If required)
- **Challenge code** (CAPTCHA)

Depending on how the administrator has configured self-registration, the user will receive an email to **Verify your Email Address**. They will be directed to the Email verification confirmation page. Once the email has been verified and the account has been approved, the user will receive an approval confirmation email and can begin using Onsight Connect.

If accounts are not required to be approved by the administrator, the new user will receive a **Welcome to Onsight** email immediately upon registration.

Related information

Security — Best Practices *(on page 115)*

8. EXTERNAL CONTACTS

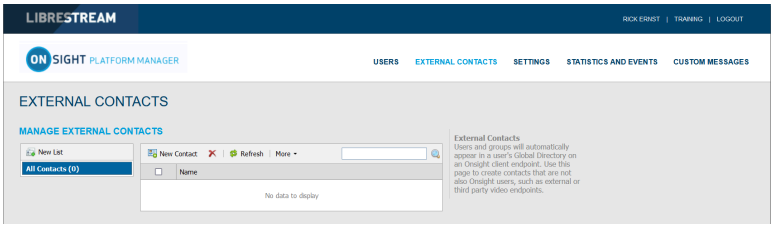
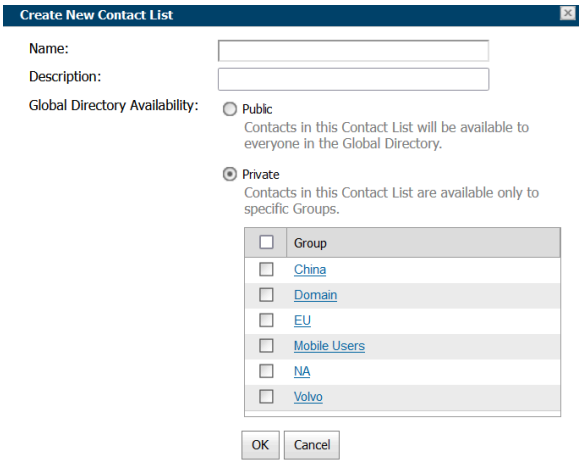


Figure 8-1 External Contacts

Click **EXTERNAL CONTACTS** from the main menu to view all external contacts. External contacts are third-party video SIP endpoints such as video conference rooms or any other SIP capable device that is not an Onsight Connect user in your Onsight domain.

By default, any user added to OPM is automatically added to the **Global Directory**.

External Contact List



You can also use the  **New List** icon create a new list of external contacts that can be shared across your domain, license and policy groups.

Export External Contacts

You can export your external contacts as a CSV template file that can be modified to include your organization's contacts and can then be reimported into Onsight Platform Manager. To export an External Contacts list, click **More > Export** to download a `ExportContacts.csv` template.

Note: The addresses you enter must be in the SIP URI format, e.g., videoroom@sipdomain.com.

The CSV file can then be modified providing you follow the conventions for column names and populate all required fields.

Tip: Click **More > Import** to access the **CSV Import instructions** link within the **Supported file formats** section, as necessary.

8.1. Manually Adding an External Contact to the Global Directory

Login to OPM and select **EXTERNAL CONTACTS** from the main menu.

To manually add an external contact to the Global Directory, you will need to:

1. Click the **New** icon.

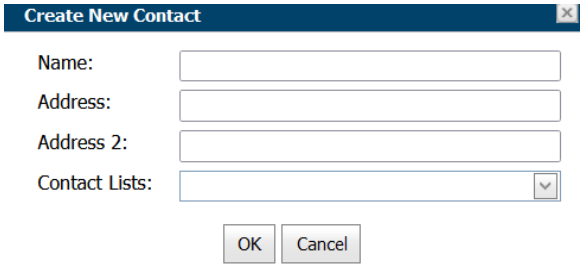


Figure 8-2 Create New Contact

2. Enter the **Name** and **Address** (Address 2, if necessary).

Note: The addresses you enter must be in the SIP URI format, e.g., videoroom@sipdomain.com.

3. Select the **Contacts Lists** drop-down menu to add the external contact to.

4. Click **OK**. You will now be able to see the External Contact when searching the Global Directory from an Onsight endpoint.
This completes the procedure.

8.2. Importing An External Contacts List

Login to OPM and select **EXTERNAL CONTACTS** from the main menu. You must have previously created and modified an `ExternalContacts.CSV` file using the **More > Import > Download Import Template** operation.

To import a revised External Contacts List as a file, you must:

1. Click **More > Import**. The **IMPORT FROM FILE** window appears.

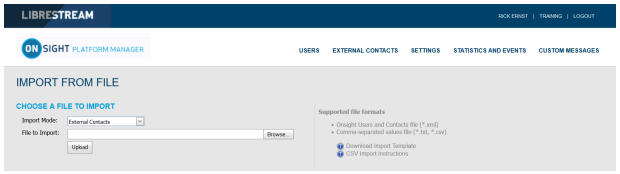


Figure 8-3 Import from File

2. Navigate and select the `ExternalContacts.CSV` to import by clicking the **Browse** button.

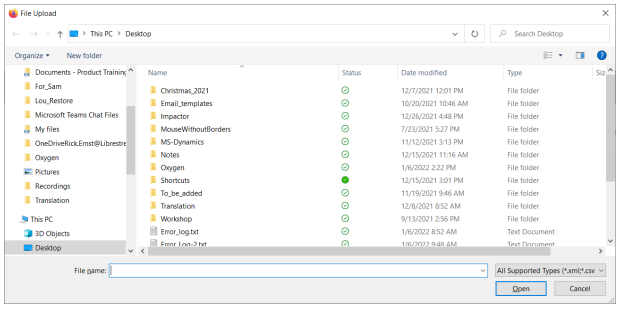


Figure 8-4 File Upload

3. Click **Open**.

4. Press **Upload**. You will be presented with the **Import Users** window.

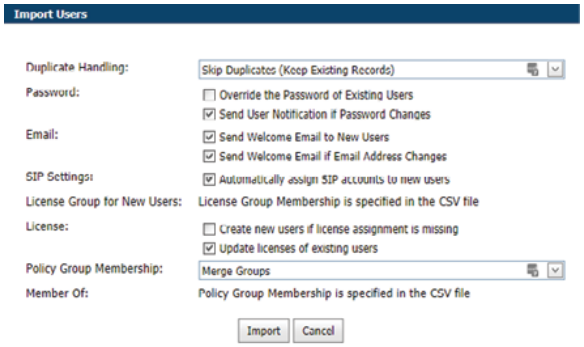


Figure 8-5 Import Users Window

5. Select the **Duplicate Handling** option that is ideal for your situation:
    - **Skip Duplicates** (Keep Existing Records)
    - **Update Existing Records**
    - **Create a Duplicate**
6. Click **Import**. When the import is complete you will be presented with the **Import Results** window.
7. Click **View Report** to review the details.
8. Press **Close**.
9. Return to the **EXTERNAL CONTACTS** page to view the imported contacts.
   This completes the procedure.

8.3. Adding an External Contacts List

Login to OPM and select **EXTERNAL CONTACTS** from the main menu.

To manually create an external contacts list, you will need to:

1. Locate and select the **New List** icon below the MANAGE EXTERNAL CONTACTS title.

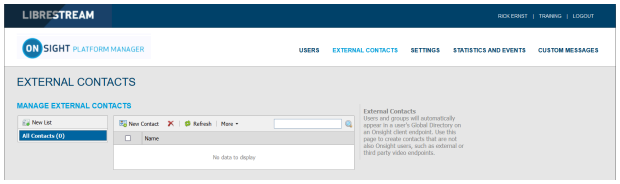


Figure 8-6 Manage External Contacts

2. The **Create New Contact List** window appears.

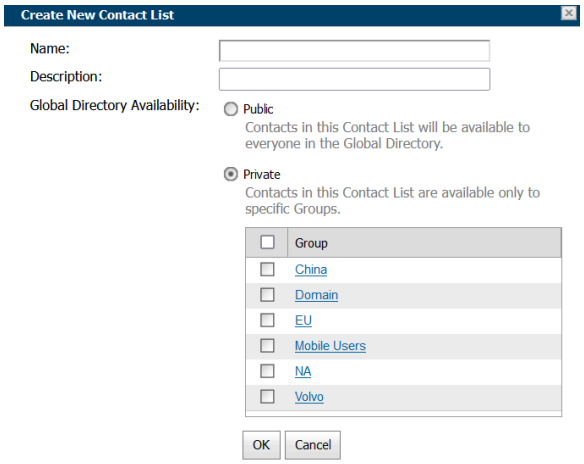


Figure 8-7 Create New Contact List

3. Enter a **Name** for the list and a Description.
4. Select **Public** or **Private** to set the accessibility level for the list.

Note: If selecting Private, select the Groups that will have access to the list.

5. The new list appears below **All Contacts** under **MANAGE EXTERNAL CONTACTS**.

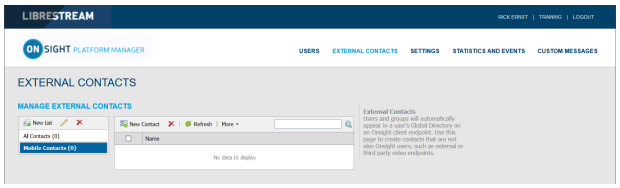


Figure 8-8 New List Appears

This completes the procedure.

8.4. Adding/Removing External Contacts from Lists

Login to OPM.

To modify contacts within your External Contacts list, you will need to:

1. Select the **EXTERNAL CONTACTS** from the main menu.

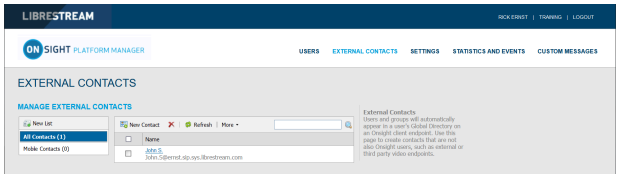


Figure 8-9 Manage External Contacts

2. Select the list to which you want the contacts to be added.

3. Enable the check box next to the `External Contact(s)` you want to add to the list.

4. Click **More > Add to List.**

5. Select the list where the contacts will be added.

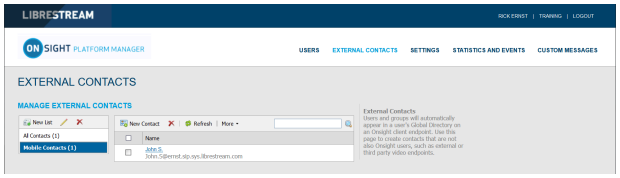


Figure 8-10 Contact Name Appears within the List

6. Verify that the contact's name appears within the list.

Tip: You can remove a contacts name from a list by selecting the list, enabling the check box next to the contact's name(s) and clicking **More > Remove from List**.

This completes the procedure.

9. SETTINGS

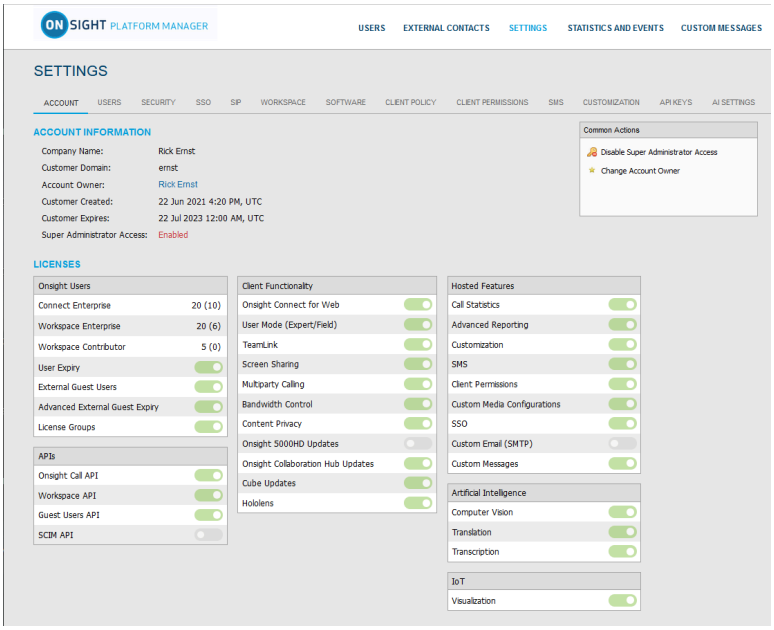


Figure 9-1 Settings

Click **SETTINGS** from the main menu to configure settings for each Onsight endpoint to comply with your policies. Settings are applied to the endpoint when a user logs in to Onsight Connect. **External Guest Users** can be enabled within **LICENSES** so that any active Onsight Connect User can invite an External Guest for a period of time as defined by the Administrator. External Guest User permissions can be restricted but have full access to the Onsight collaboration experience.

Additional tabs are accessible within **SETTINGS** that include:

- **SIP** settings are assigned from the Auto-Assignment Pool.
- **Software** settings control which Onsight Connect version settings can be selected and installed for Windows operating systems.
- **Client Policy** settings are selected for each endpoint, e.g., Encryption mode.
- **Security** settings are assigned that include Password Policy, Login Policy, and User Account Creation method.

All Settings are applied to Onsight endpoints after an Onsight user has been authenticated and authorized during the login process.

When applying changes to a settings page, you must **Save** to commit the changes. Click **Reset Changes** to return to prior saved settings for the page.

9.1. Authentication Time-out

To allow access to content and call services in the event that there is a loss of network connectivity — Users remain locally authenticated for 30 days on the client after their initial online authentication occurs. Clients must re-authenticate to the online service at least once every 30 days.

9.2. Account

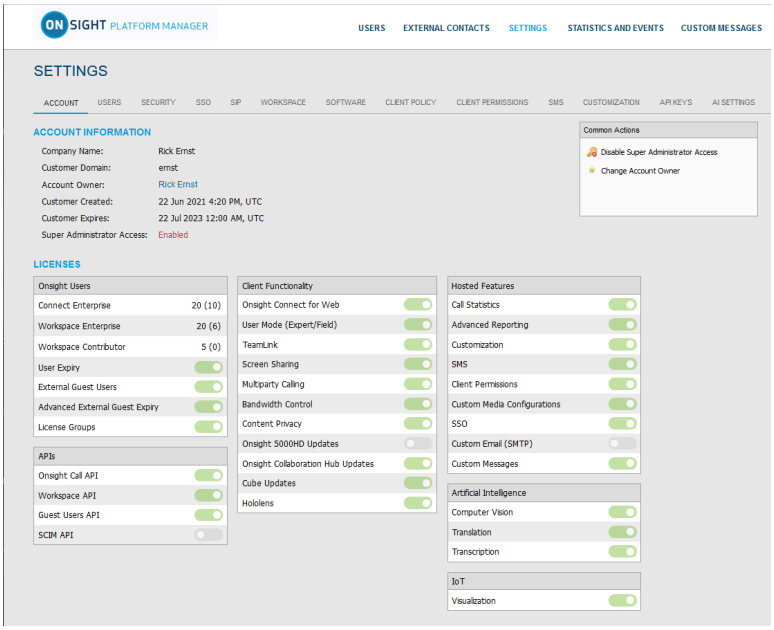


Figure 9-2 Settings

Click **SETTINGS** from the main menu to enable you to access your company's OPM account information, within the **ACCOUNT** tab. The ACCOUNT tab includes the following sections: Account Information, Common Actions and Licenses.

Account Information

Includes your **Company Name**, **Customer Domain**, **Account Owner**, **Customer Created** date, **Customer Expiry** date and **Super Administrator Access** status.

Common Actions

Within the **Common Actions** panel on the right, you can access additional functions that include Enable/Disable **Disable Super Administrator Access** and **Change Account Owner**.

Licenses

The licenses enabled in your Onsight domain are listed in the **LICENSES** section.

Related information
Account — Best Practices *(on page 112)*

9.2.1. Super Administrator Access

Within the **Common Actions** panel, you can Enable or Disable **Super Administrator Access** to Librestream Support. This enables you to specify the number of hours you would like to grant **Librestream Support** access to your domain. Granting access allows Librestream Support to assist with setup or troubleshooting. Super Administrator Access can be disabled at any time by pressing **Deny Super Administrator Access**; otherwise, it will expire after the set time limit.

ON PREMISES

When managing an on-premises server, Super Administrator Access is not applicable. CONTACT SUPPORT *(on page 103)* if assistance is required.

Related information
Account — Best Practices *(on page 112)*
CONTACT SUPPORT *(on page 103)*

9.2.2. Change Account Owner

Within the **Common Actions** section, you can use **Change Account Owner** to specify the primary **OPM Administrator** for your Onsight Account Domain. **Change Account Owner** enables an Onsight Platform Manager Administrator to assign another user as the **Account Owner**.

Tip: The user must have Onsight Platform Manager Administrator privileges before they can be assigned as the Account Owner.

Related information
Account — Best Practices *(on page 112)*

9.2.3. Licenses

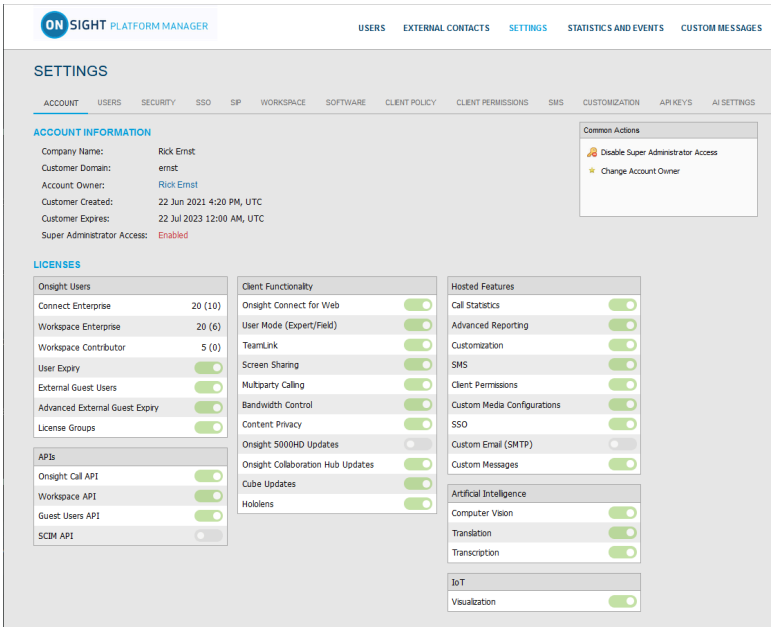


Figure 9-3 Settings

The licenses enabled for your Onsight domain are listed within the **LICENSES** section. They are divided into four main categories:

1. **Onsight Users**
2. **Client Functionality**
3. **APIs**
4. **Hosted Features**

Related information
Account — Best Practices *(on page 112)*

9.2.3.1. Onsight Users

The Onsight Users section lists the number of licenses per type and the license features. Each license type enables functionality within the client apps. User license types include:

- **Connect Enterprise**
- **Workspace Enterprise**
- **Workspace Contributor**

Each license feature enables functionality related to user license management. License features include:

- **User Expiry** — Enables user accounts to expire
- **External Guest Users** — Enables guest invites
- **Advanced External Guest Expiry — Enables guest invites to expire.**
- **License Groups** — Enables license pool management on a per group basis

9.2.3.2. Application Programming Interfaces

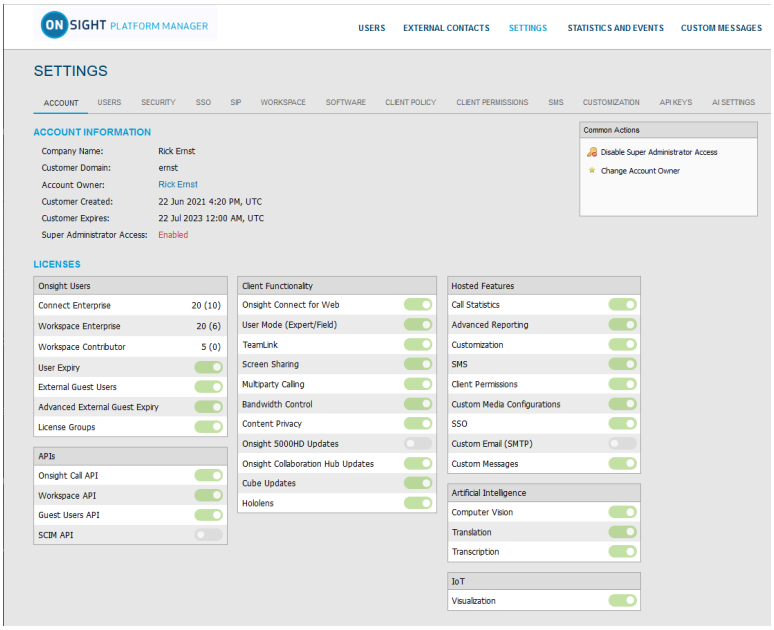


Figure 9-4 Settings

Onsight Platform manager can be enabled to work with several Application Programming Interfaces (APIs). Click **SETTINGS** from the main menu and locate APIs within the **LICENSES** section. The APIs include:

- **Onsight Call API** — Enables access to the **Onsight Call REST API** and **API Key Management**.
- **Workspace API** — Enables access to the **Workspace REST API** and **API Key Management**.
- **Guest Users API** — Enables the capability to invite external guests.
- **SCIM API** — Automates user and group management.

9.2.3.3. Client Functionality

You can access **Client Functionality** by clicking **SETTINGS** from the main menu and locating it within the **LICENSES** section. Client Functionality can be enabled or disabled for:

- **Onsight Connect for Web** — Enables the capability to access the web app.
- **User Mode (Expert/Field)** — Enables the capability to define user accounts as **Expert** or **Field** mode. **Expert Mode** provides all features to users. **Field Mode** is a simplified user interface with a subset of features available to the user. When using **Field Mode**, it is expected they will be calling Experts who will control the call remotely.
- **TeamLink** — Enables TeamLink firewall traversal capabilities for the domain. TeamLink enables HTTPS tunneling of data through a firewall that does not allow SIP or Media traffic.

Note: By enabling **TeamLink Registration**, you are automatically turning on **TeamLink** for each endpoint. By enabling the **Always use TeamLink** option, you are telling the endpoint to use TeamLink even if the SIP ports on the Firewall are open, i.e., Always tunnel SIP through HTTP/S.

Tip: Librestream recommends that **Always use TeamLink** be **Disabled** and only be used on a per endpoint basis for troubleshooting purposes.

- **Screen Sharing** — Enables the ability to share any window with participants on the call.
- **Multiparty Calling** — Enables the capability to set Windows PCs and Android devices as conference hosts. When enabled, the device can host a conference call with multiple participants. The limitation on the number of participants depends on the hardware and network resources available to the device.

Tip: The maximum number of call participants can be controlled by **Client Policy**.

- **Bandwidth Control** — Enables the ability to set the **Maximum Video Bit Rate** allowed for **Media Configurations**.
- **Content Privacy** — Enables the ability to control recording and still image capture on endpoints using **Client Policy**.
- **Onsight 5000HD Updates** — Enables updates for the 5000 HD rugged smart camera.
- **Onsight Collaboration Hub Updates** — Enables the ability to deploy software updates to Onsight Collaboration Hubs via either iOS or Android clients.
- **Cube Updates** — Enables updates for the Onsight Cube.
- **Hololens** — Enables Hololens accessibility to Onsight Connect Functionality.

On Premises — TeamLink

TeamLink is currently not supported when using on premises installations, public Internet access is required to communicate with TeamLink servers.

9.2.3.4. Hosted Features

Hosted Features are options for a customer's domain, as defined by the contract, that are enabled/disabled by Librestream's technical support team. These options may include:

- **Call Statistics** — Enables the capability to capture Call Statistics from Onsight endpoints.
- **Advanced Reporting** — Enables the capability to generate and export Advanced Call Statistic reports.
- **Customization** — Enables the capability to customize Onsight Platform Manager messages sent to Onsight users. Messages are text and HTML based.
- **Client Permissions** — Enables end users to modify their own permission settings.
- **SMS** — Enables the capability to send External Guest Invites via SMS. Client Permissions: enables the capability to control user access to endpoint settings.
- **Custom Media Configurations** — Enables the capability to deploy custom media configurations via Client Policy.
- **SSO** — Enables Single Sign On support for your domain. See the SSO section for setup details.
- **Custom Email (SMTP)** — Enables customers to use their own domain email for all notifications instead of using Librestream's domain.
- **Custom Messages** — Enables customers to customize the format of messages received by their Onsight Connect users.

9.2.3.5. Artificial Intelligence

Artificial Intelligence (AI) features can be enabled or disabled for:

- **Computer Vision** (CV) — Enables access to the CV features including OCR, barcodes and QR codes, Object classification and location, and auto-tagging.
- **Natural Language Processing** (NLP) — Enables access to the NLP feature for accessing **Onsight Translator**.
- **Transcription** — Enables access to Transcription functions for all calls.

9.2.3.6. Internet of Things

Internet of Things (IoT) features can be enabled or disabled for **Visualization**. This enables access to IoT services, instrument visualization and auto-tagging.

9.2.4. Data Anonymization

Data Anonymization: Can be enabled by request, for your domain to support General Data Protection Regulation (GDPR) for Europe, and related legislation that includes data privacy compliance and the Right to be Forgotten (RTBF).

When enabled, deleted users will automatically have their **Personal Identifiable Information** (PII) anonymized. The username, email address, and events will no longer be available for display in Onsight Platform Manager (OPM) reports and call statistics. An anonymized pseudonym will be inserted in its place to prevent identification of the user.

Note: Call statistics, reports and events will still contain the anonymized data to support analytics and reporting.

Data Anonymization of PII occurs when:

- a user account is deleted
- a guest user is deleted and/or their account expires

Note: Onsight Workspace content is the property and responsibility of the customer. When an Onsight user is deleted, their Workspace account is also automatically deleted, Their content remains intact. The Workspace Administrator can delete the user's content when required.

Additionally, upon request, Librestream can:

- **Anonymize previously deleted users from your domain** — Previously deleted users will not appear within your user lists, but their data will still be available for reporting if they are not anonymized.
- **Anonymize active user data** — When enabled, data will no longer be associated with the active user. Data will still show usage within the given time period.

9.2.5. Scheduled Anonymization

Scheduled Anonymization can be enabled by request, for your domain to automatically convert active personal data to anonymous data as defined by a **Data Retention Period** (DRP). On your next cycle, data will be anonymized. This eliminates the need for manual processing for customers.

Note: Scheduled Anonymization is disabled by default. **Once data is anonymized — It is not reversible.**

9.3. Users

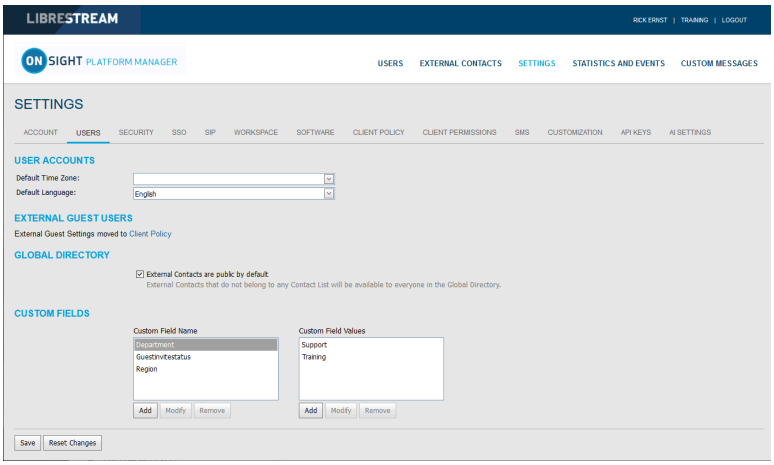


Figure 9-5 Users Page

Click **SETTINGS** from the main menu and click the **USERS** tab. The **USERS** page enables you to set the user and external guest global settings for the domain. The **USERS** page includes the following sections: **USER ACCOUNTS**, **EXTERNAL GUEST USERS**, **GLOBAL DIRECTORY** and **CUSTOM FIELDS**.

Related information

Users — Best Practices *(on page 114)*

9.3.1. User Accounts

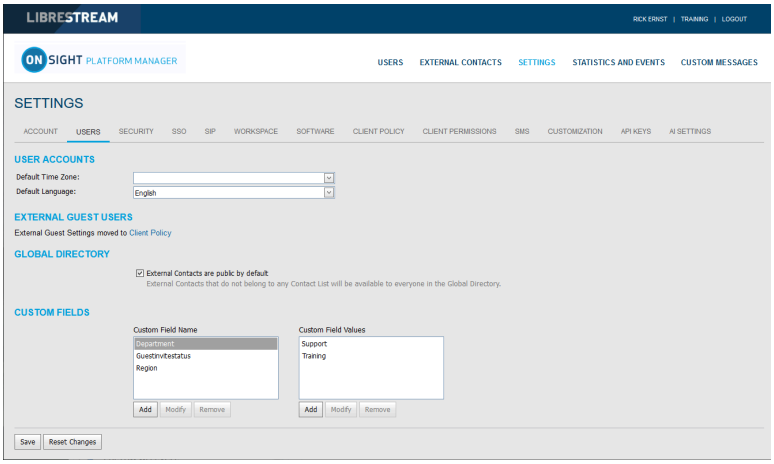


Figure 9-6 Users Page

Click **SETTINGS** from the main menu and click the **USERS** tab. The **USERS** page enables you to modify **USER ACCOUNT** settings for:

- **Default Time Zone** — Select the desired Time zone for all user accounts from the drop-down menu. All data reported by Onsight clients to OPM is based on Universal Time Coordinated (UTC) however, the Default Time Zone setting will adjust the time stamp data within OPM for display purposes only.
- **Default Language** — Set the default Language from the drop-down menu.

Note: Onsight devices must have the accurate date and time set to use the Onsight Connect Service. HTTPS relies on time/date accuracy to perform authentication.

Related information

Users — Best Practices *(on page 114)*

9.3.2. External Guest Users

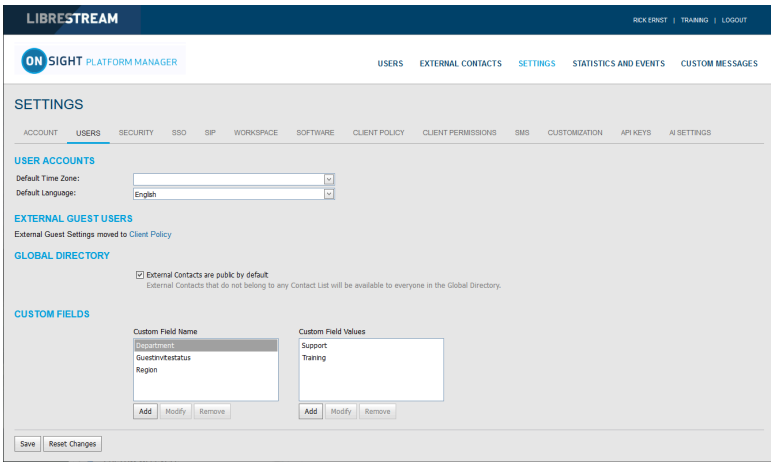


Figure 9-7 Users Page

Click **SETTINGS** from the main menu and click the **USERS** tab. The **USERS** page contains an **EXTERNAL GUEST USERS** section that enables you to click the **Client Policy** shortcut to modify these settings.

Note: All External Guest Settings are moved to **Client Policy**.

Related information

Users — Best Practices *(on page 114)*
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

9.3.3. Global Directory

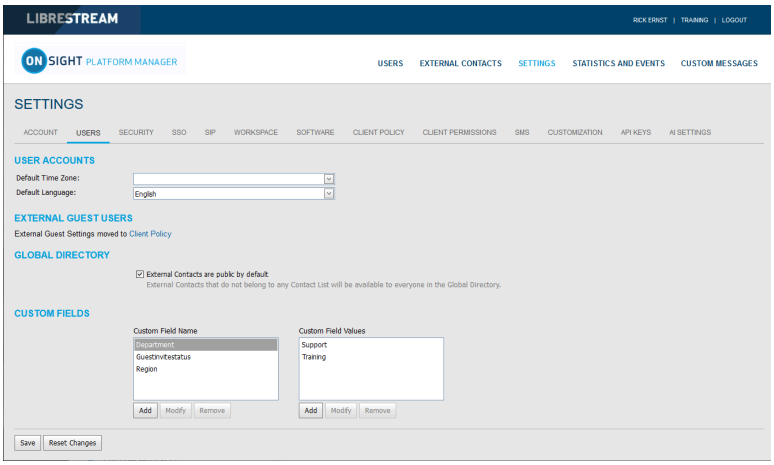


Figure 9-8 Users Page

Click **SETTINGS** from the main menu and click the **USERS** tab. The **USERS** page contains a **GLOBAL DIRECTORY** section that controls how External Contacts are displayed within the Global Directory. Users and groups will automatically appear in the Global Directory on an Onsight client. External Contacts are created contacts that are not Onsight users — They include external or third-party video endpoints.

Enable the **External Contacts are public by default** check box to control whether external contacts that do not belong to any Contact List will be available to everyone in the Global Directory.

Note: This behaves independently from the **External Guest Users** setting that can disable global directory access. This setting controls standard user access to **External Contacts** in the global directory.

Related information

Users — Best Practices *(on page 114)*

9.3.4. Custom Fields

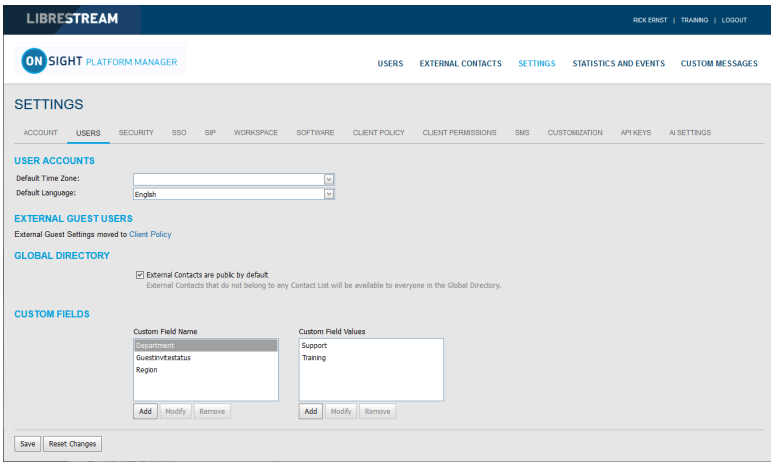


Figure 9-9 Users Page

Click **SETTINGS** from the main menu and click the **USERS** tab. The **USERS** page contains a **CUSTOM FIELDS** section. You can create custom fields to learn more about your guests and improve reporting data. Custom Fields can appear on a user's **PROFILE** page. **Custom Fields** require a:

- **Custom Field Name**: Add, Modify or Remove the name for the custom field.
- **Custom Field Value**: Add, Modify or Remove values for the **Custom Field Value** field. Custom Field Values are included within an exported user report.

Note: Custom fields will be included in an exported user report.

Related information

Users — Best Practices *(on page 114)*

9.4. Security

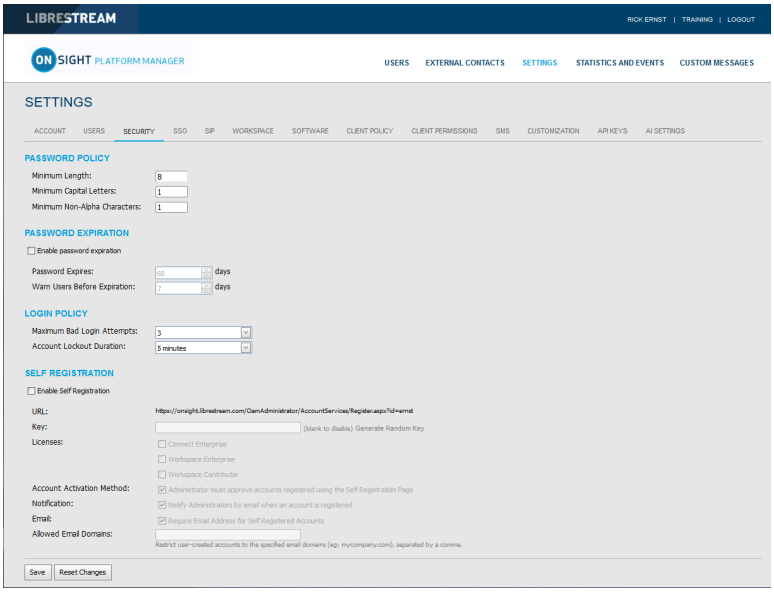


Figure 9-10 Security

Click **SETTINGS** from the main menu and click the **SECURITY** tab. The **SECURITY** page appears and enables you to modify your password and login policies. The following sections are available: **PASSWORD POLICY**, **PASSWORD EXPIRATION**, **LOGIN POLICY** and **SELF REGISTRATION**.

Related information
Security — Best Practices *(on page 115)*

9.4.1. Password Policy

Click **SETTINGS** from the main menu and click the **SECURITY** tab. The **SECURITY** page appears. Locate the **PASSWORD POLICY** section where you can set domain and client policy for passwords that include:

- **Minimum Length** (Characters) — Enter a numeric value.
- **Minimum Capital Letters** — Enter a numeric value.
- **Minimum Non-Alpha Characters** — Enter a numeric value.

Related information
Security — Best Practices *(on page 115)*

9.4.2. Password Expiration

Click **SETTINGS** from the main menu and click the **SECURITY** tab. The **SECURITY** page appears. Locate the **PASSWORD EXPIRATION** section and modify the following parameters:

- **Enable password Expiration** check box — Enable this option to force the password to expire.
- **Minimum** — Enter a value in days. For example, Minimum: 1 day, Maximum: 365 days.
- **Warn Users Before Expiration**: Set the length in days as **Minimum**: 0 day, or **Maximum**: 365 days.

Related information
Security — Best Practices *(on page 115)*

9.4.3. Login Policy

Click **SETTINGS** from the main menu and click the **SECURITY** tab. Locate the **LOGIN POLICY** section where you can modify your Login policy for:

- **Maximum Bad Login Attempts** — Set the number of allowed attempts before the user is locked out.
- **Account Lockout Duration** — Set the duration of the lockout period as: **5**, **15**, **30** minutes, or **Forever** as necessary.

Note: The **Forever** option requires that the administrator unlock the account in order to grant access.

Related information
Security — Best Practices *(on page 115)*

9.4.4. Self Registration

Click **SETTINGS** from the main menu and click the **SECURITY** tab. The **SECURITY** page appears. Locate the **SELF REGISTRATION** section. These settings enable users to self-register for an account by navigating to a self registration URL. The URL must be distributed by the administrator and may be protected by a self registration key. The following parameters are available:

- **Enable Self Registration** check box — Enables a user to enter their own account information including username, initial password, first name, last name, email, and the self-registration key (if required).
- **URL** — The system generated self registration URL. This must be distributed to users wishing to self-register.
- **Key** — Enter a registration key to protect you from unauthorized access to these user accounts. This key must be distributed to users wishing to self-register.
- **Licenses** — Select the licenses that each self-registered user will be assigned. There must be available licenses for the registration to be successful.

- **Account Activation Method** — When enabled, the administrator must approve accounts registered using the Self Registration Page.
- **Notification** — Enable the **Administrator must approve accounts register using the Self Registration Page** check box to ensure that the Admin is notified by email when an account is registered.
- **Email** — Enable to **Require Email Address for Self-registered Accounts**.
- **Allowed Email Domains** — Enter a comma separated value list of allowed email domains for self-registered users. Use this option in combination with the **Required Email** setting to restrict access to self-registered accounts.

Related information

Security — Best Practices *(on page 115)*

9.5. Single Sign On

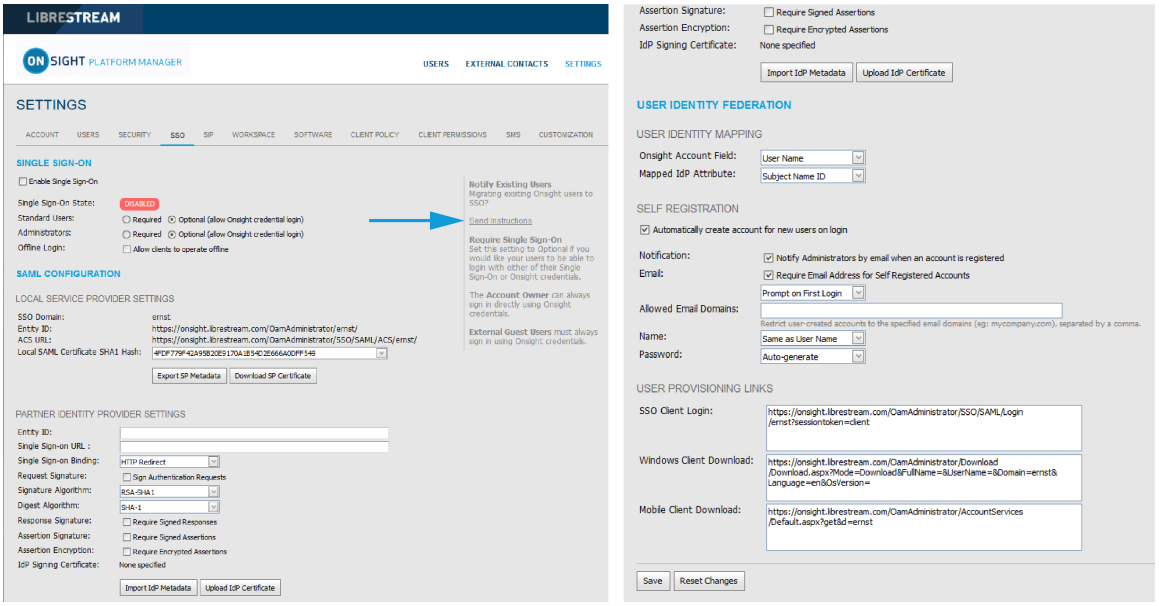


Figure 9-11 SSO Settings

Click **SETTINGS** from the main menu and click the **SSO** tab. The **SSO** page appears and enables you to modify your sign on parameters. The following sections are available: **SINGLE SIGN-ON**, **SAML CONFIGURATION**, and **USER IDENTITY FEDERATION**.

Onsight Platform Manager supports Single Sign-On (SSO) using Security Assertion Markup Language (SAML v2.0). SAML is a licensed add-on for Enterprise customers and is an open standard for exchanging authentication and authorization data between two parties: A Service Provider (SP) and the Identity Provider (IdP). In this case, OPM acts as the SP to your SSO IdP.

If you are migrating existing Onsight users to SSO, you can press the **Send Instructions** link on the right, to select which users to send instructions. You can select individual users or groups. They will receive an email with the login instructions.

Note: External Guest Users must always sign in using Onsight credentials, i.e., username and password. External Guest Users can login using the login link included in the Invite email or SMS message they have received. The username and password are also included in the invite email.

Tip: Please contact mailto:support@librestream.com to setup SSO.

9.5.1. Single Sign ON

Click **SETTINGS** from the main menu and click the **SSO** tab. The **SSO** page appears. Locate the **SINGLE SIGN-ON** section.

Tip: Please contact mailto:support@librestream.com for help with setting up SSO.

For **Standard Users** and **Administrators**:

- Choose **Required** or **Optional** to select whether you would like users to only login with SSO (Required) or have the option of signing in with their Onsight Username and Password (Optional).

  Note: The Account Owner can always log in with their Onsight Account credentials regardless of which option has been set.

- **Offline Login**: Enable **Allow clients to operate offline** if you would like users to be able to login to Onsight clients when network access is not available. In this scenario if a user cannot reach the Identity Provider (IdP), they would still be able to log in to Onsight Connect.

9.5.2. Security Assertion Markup Language Configuration

Security Assertion Markup Language (SAML) is a licensed add-on for Enterprise customers and is an open standard for exchanging authentication and authorization data between two parties.

9.5.2.1. Local Service Provider

Click **SETTINGS** from the main menu and click the **SSO** tab. The **SSO** page appears. Locate **LOCAL SERVICE PROVIDER SETTINGS** within the **SAML CONFIGURATION** section.

These settings identify Onsight Platform Manager as the **Service Provider** (SP) to your **Identity Provider** (IdP).

- **SSO Domain** — Provides the name of the SSO domain that will be used by Onsight. This value is equal to the Onsight domain name.
- **Entity ID** — Provides the Entity ID of OPM for the IdP.
- **ACS URL** — Provides the ACS URL of OPM for the IdP.

9.5.2.2. Configuring Your IdP Settings

Login to OPM and select **SETTINGS** from the main menu and click the **SSO** tab. The **SSO** page appears. Locate **PARTNER IDENTITY PROVIDER SETTINGS** within the **SAML CONFIGURATION** section.

To manually configure your IdP Settings, you will need to:

1. Press the **Export SP Metadata** button to export the Service Provider (SP) metadata file: `SPMetadata.xml`.
2. Upload the `SPMetadata.xml` file to your **SSO Identity Provider** (IdP).

   Note: If you require encrypted communication between OPM and your IdP, you will need to import the OPM SP Certificate into your IdP using the next two steps.

3. Press the **Download SP Certificate** button to download the **Service Provider** (SP) public certificate file.
4. Upload the SP `Certificate` file to your **SSO Identity Provider** (IdP).
5. Download the IdP metadata file from your IdP. This completes the procedure.

9.5.2.3. Partner Identity Provider

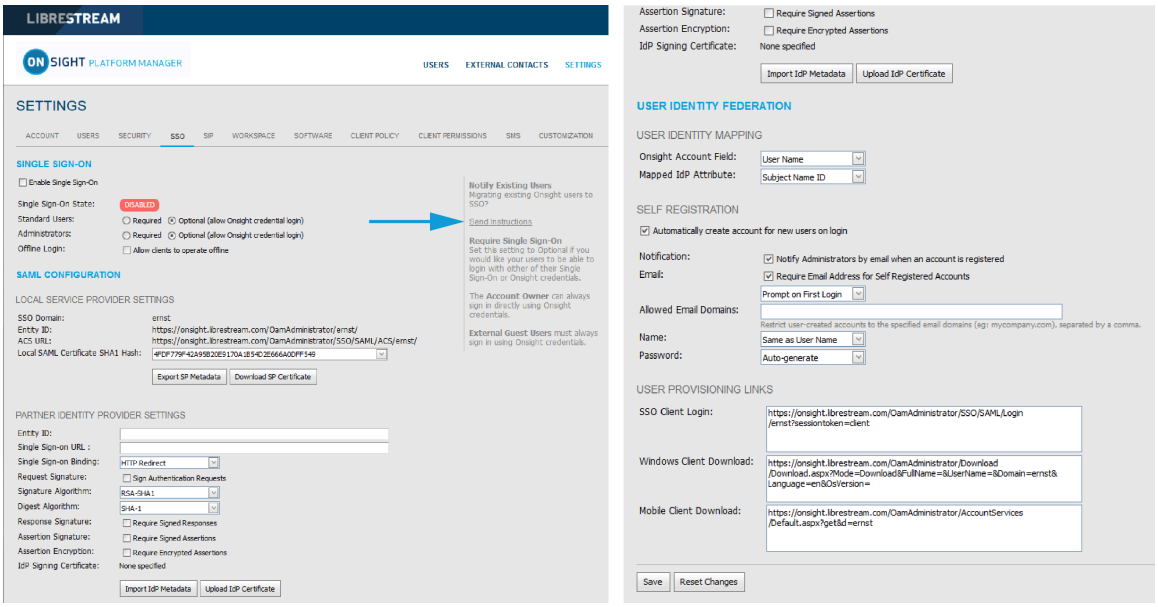


Figure 9-12 SSO Settings

Click **SETTINGS** from the main menu and click the **SSO** tab. The **SSO** page appears. Locate **PARTNER IDENTITY PROVIDER SETTINGS** within the **SAML CONFIGURATION** section.

Partner Service Provider settings inform OPM on how to communicate with the **SSO Identity Provider** (IdP). In most cases, you can use the Import **IdP Metadata** and **Upload IdP Certificate** buttons to configure OPM with your Partner Identify Providers settings.

Importing the metadata will provide the following:

- **Entity ID**
- **SSO URL**
- **SSO binding**
- **Signature Algorithm**
- **Digest Algorithm**

You will need to configure the following options to match your IdP's settings:

- **Sign Authentication Requests**
- **Require Signed Responses**
- **Required Signed Assertions**
- **Require Encrypted Assertions**

Click **Import IdP Metadata** to import the **IdP metadata** file that you downloaded from your Identity Provider.

Click **Upload IdP Certificate** to upload the **IdP Certificate** (Public). This option is provided in the event you need to upload the IdP Certificate manually. In most cases, the IdP Certificate will be provided in the metadata file obtained from your IdP.

9.5.2.4. Manually Configure Your IdP Settings

Login to OPM and select **SETTINGS** from the main menu and click the **SSO** tab. The **SSO** page appears. Locate **PARTNER IDENTITY PROVIDER SETTINGS** within the **SAML CONFIGURATION** section.

To manually configure your IdP settings:

1. Enter the **Entity ID** or your IdP.
2. Enter the **Single Sign-on URL** of your IdP.
3. Enter the **Sign-on Binding type** (HTTP Post or Redirect).
4. If required, under Request Signature, enable **Sign Authentication Requests**.
5. If required, select the **Signature Algorithm** used by your IdP.
6. If required, select the **Digest Algorithm** used by your IdP.
7. If required, enable **Require Signed Responses.**
8. If required, enable **Require Signed Assertions**.
9. If required, enable **Require Encrypted Assertions**.

9.5.3. User Identity Federation

Click **SETTINGS** from the main menu and click the **SSO** tab. The **SSO** page appears. Locate **USER IDENTY FEDERATION** within the **SAML CONFIGURATION** section.

User Identity Federation settings define how SSO enterprise users map to Onsight user accounts.

9.5.3.1. User Identity Mapping

Click **SETTINGS** from the main menu and click the **SSO** tab. The **SSO** page appears. Locate **USER IDENTITY FEDERATION** within the **SAML CONFIGURATION** section.

Identity mapping provides the link between the user information sent via the SAML assertion and the corresponding Onsight Account Fields.

The mapping tells OPM which Onsight user account is being authenticated by SSO. The mapped attributes must be of equal value, e.g., the SAML assertion's **NameID** must equal the Onsight User's **Username** if these two attributes are mapped. The attribute name and values are case sensitive.

Choose one of the following mapping methods:

- **Username Mapping**
- **Email Mapping**
- **Federated SSO ID mapping**

9.5.3.2. Username Mapping

Login to OPM and select **SETTINGS** from the main menu and click the **SSO** tab. The **SSO** page appears. Locate **USER IDENTITY MAPPING** within the **USER IDENTITY FEDERATION** section.

To apply Username mapping, you will need to:

1. Select the **Onsight Account Field** drop-down menu to compare its values to the **Mapped IdP Attribute**:
    - **User Name** — Onsight Account User name
    - **Email Address** — Onsight Account Email Address
    - **Federated SSO Id** — Onsight user's associated Federated SSO Id. This is defined by the Onsight Administrator and can be included as part of the Imported User list. This may be mapped to either the Subject Name Id or an Attribute of the SAML Assertion.

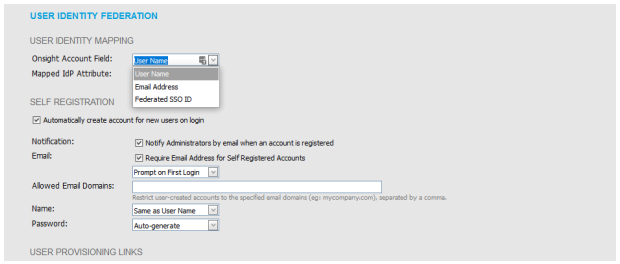


Figure 9-13 Onsight Account Field

2. Select the **Mapped IdP Attribute** drop-down menu to compare its values with the **Onsight Account Field**:
    - **Subject Name ID**
    - **Attribute** — Set the Attribute Name of the Attribute to be compared to the Onsight Account Field

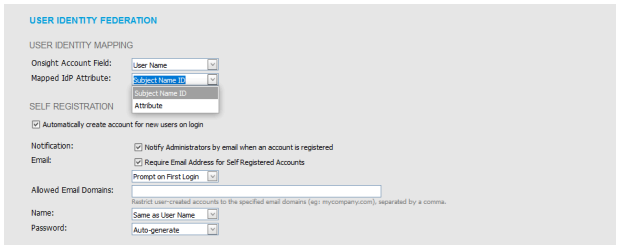


Figure 9-14 Mapped IdP Attribute

Note: User Import: If you are using the **Federated SSO ID** to provide identity mapping between your enterprise users and the Onsight User Accounts, you must populate the **Federated SSO ID** field for each user listed in the UserImport.csv file.

This completes the procedure.

9.5.3.3. Email Mapping

Login to OPM and select **SETTINGS** from the main menu and click the **SSO** tab. The **SSO** page appears. Locate **USER IDENTITY MAPPING** within the **USER IDENTITY FEDERATION** section.

To apply Email mapping, you will need to:

1. Select **Email Address** within the **Onsight Account Field** drop-down menu.

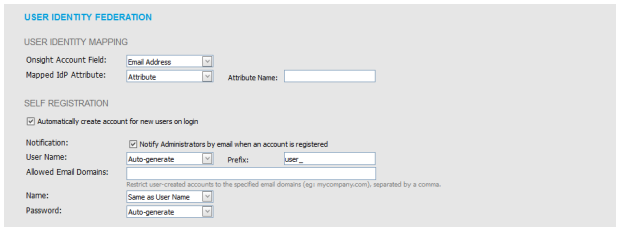


Figure 9-15 Email Address

2. Select **Attribute** from the **Mapped IdP Attribute** drop-down menu.
3. Enter the name of the Attribute within the **Attribute Name** field e.g., **Email**.
   This completes the procedure.

9.5.3.4. Federated SSO ID Mapping

Login to OPM and select **SETTINGS** from the main menu and click the **SSO** tab. The **SSO** page appears. Locate **USER IDENTITY MAPPING** within the **USER IDENTITY FEDERATION** section.

To modify your Federated SSO ID mapping settings, you will need to:

1. Select **Federated SSO ID** from the **Onsight Account Field** drop-down menu.

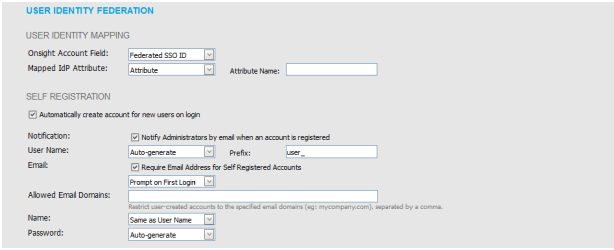


Figure 9-16 Federated SSO ID

2. Select **Attribute** from the **Mapped IdP Attribute** drop-down menu.

3. Enter the name for the Attribute within the **Attribute Name** field. e.g., OPMUSER. (You may define which ever attribute name you want).
   This completes the procedure.

9.5.4. SSO Self Registration

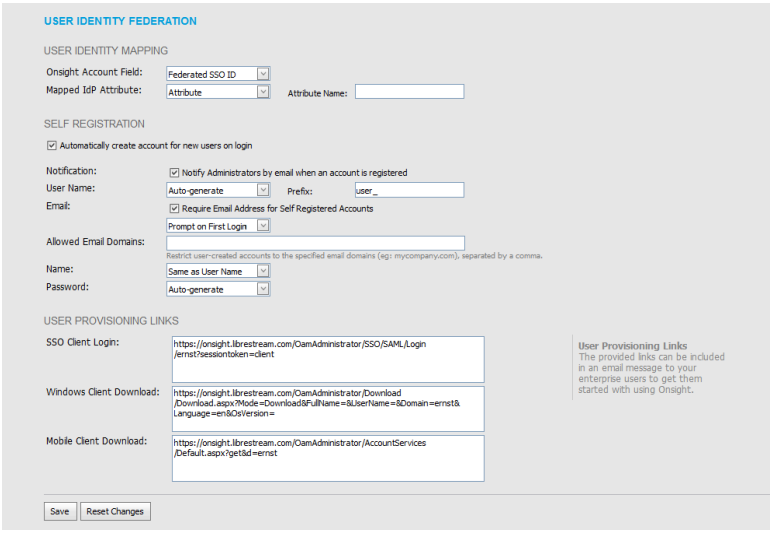


Figure 9-17 SSO Self Registration

Click **SETTINGS** from the main menu and click the **SSO** tab. The **SSO** page appears. Locate **SELF REGISTRATION** within the **USER IDENTITY FEDERATION** section.

To enable Self-Registration, enable the **Automatically create account for new users on login** check box.

Note: By default, if a user is logging in using SSO for the first time and they do not already exist as an Onsight user, an Onsight account will automatically be created for them.

SSO Self Registration Overview

To enable SSO self registration:

1. Set your **Notification** and **Email** preferences:
   - **Notification** — Enable the **Notify Administrators by email when an account is registered** check box.
   - **Email** — Enable the **Require Email Address for Self-Registered Accounts** check box.
2. Define the method to use for **User Name** creation:
   - **Attribute** — Uses the mapped attribute as the Onsight username.
     - **Attribute Name** — Sets the attribute name that will be used as the Onsight username.

- **Auto-generate** — Creates the Onsight username.
  - **Prefix** — Sets the prefix for auto-generated Onsight usernames.
- **Prompt on First Login** — Prompts the user to enter an Onsight username.

3. Set the **Email** method to use for setting the user's email address:
   - Select **Attribute** and the **Attribute Name** to use for the email address of the user.
   - Select **Prompt on First Login**, which will require the user to enter their email address the first time they log in to Onsight Connect.

   Note: Your security settings dictate whether an email address is required for self-registered users.

4. Set the personal Name of the user:
   - Same as **User Name**.
   - **Attribute** — Enter the **First Name** and **Last Name** attributes that will be mapped to the Name.
   - **Prompt on First Login** — Prompts the user to enter the First and Last names.

5. Set the **Password** creation option:
   - **Auto-generate** — The user will not need to know their Onsight User account password. This option should only be used when SSO login is set to Required and is the supported login method.
   - **Prompt on First Login** — This option should be selected if the Optional (allow Onsight credential login) has been selected. Users will be able to log in to Onsight Connect directly without using their SSO credentials.

9.5.5. User Provisioning Links

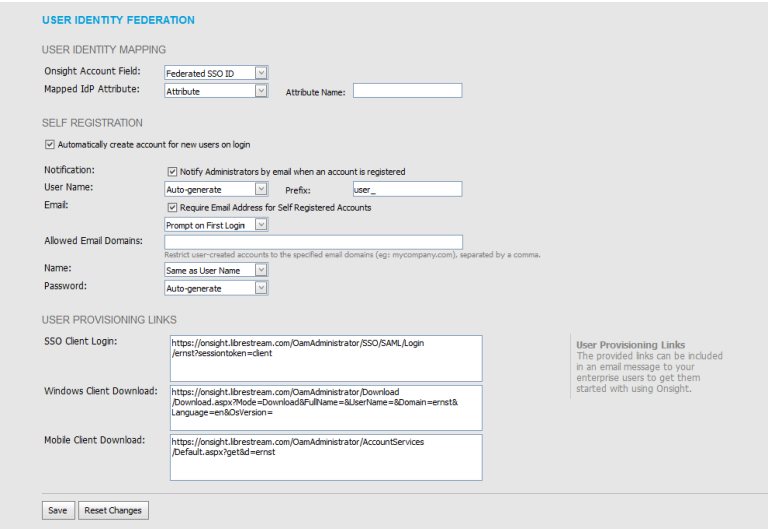


Figure 9-18 User Provisioning Links

Click **SETTINGS** from the main menu and click the **SSO** tab. The **SSO** page appears. Locate **USER PROVISIONING LINKS** within the **USER IDENTITY FEDERATION** section.

The following links are provided for reference. You can include these links in your Onsight account deployment instructions email to your users:

- **SSO Client Login** — The link to the SSO login page.
- **Windows Client Download** — The download link for Onsight Connect for Windows.
- **Mobile Client Link** — The link to the Onsight Connect for mobile devices download page.

9.5.6. Notify Existing Users

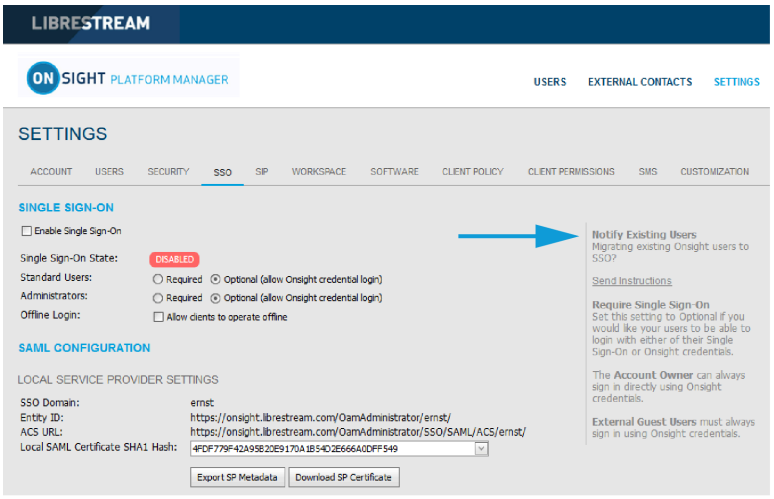


Figure 9-19 Notify Existing Users

Click **SETTINGS** from the main menu and click the **SSO** tab. The **SSO** page appears. Locate the **Notify Existing Users** section on the right.

Once you have completed the SSO setup, you can send instructions to your existing users via email.

1. Press the **Send Instructions** link in the **Notify Existing Users** section.

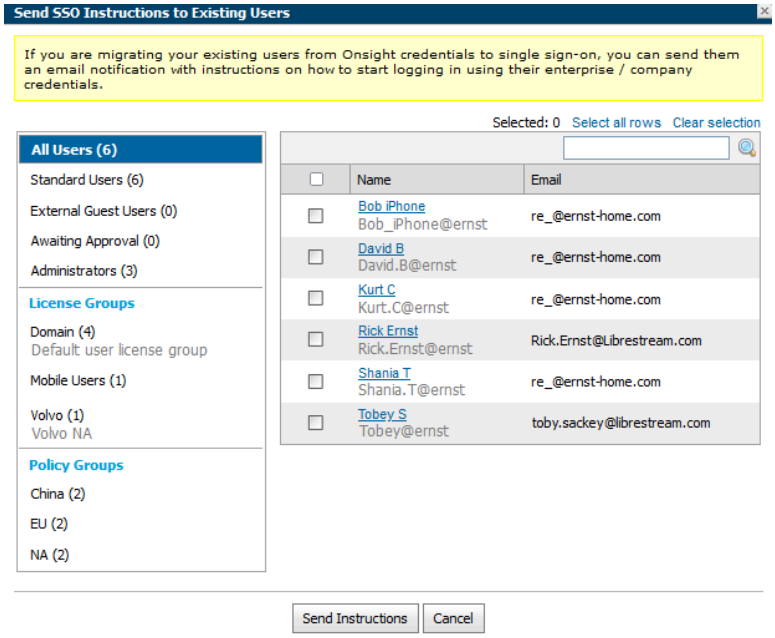


Figure 9-20 Send SSO Instructions to Existing Users

2. Select the users you want to notify and press the **Send Instructions** button. You can press the **Select all rows** link to select all users or you may also sort based on the Groups listed in the left-hand column.

9.5.7. On-premises — SSO Certificate Setup

For OPM On Premises, the server hosting OPM must have a certificate installed suitable for SAML encryption and signing. The SSO certificate must have the **Digital Signature** and **Key encipherment** key usage extensions and have the **Extended key usage set** to critical.

1. To configure OPM to use the SSO certificate go to **Site Administration > Server Settings > General**.

2. In the SSO section, paste the certificate's SHA1 thumbprint in the Local Service Provider Certificate SHA1 Hash text box.

3. To verify the certificate, go to **Customer Portal > Settings > SSO**.
4. Verify the certificate is available for use by OPM. Click the **Download SP Certificate** button.
5. The certificate should be downloaded successfully.

Refer to the Onsight Platform Manager On Premises — Installation Guide for details on deploying server certificates.

9.6. Session Initiation Protocol

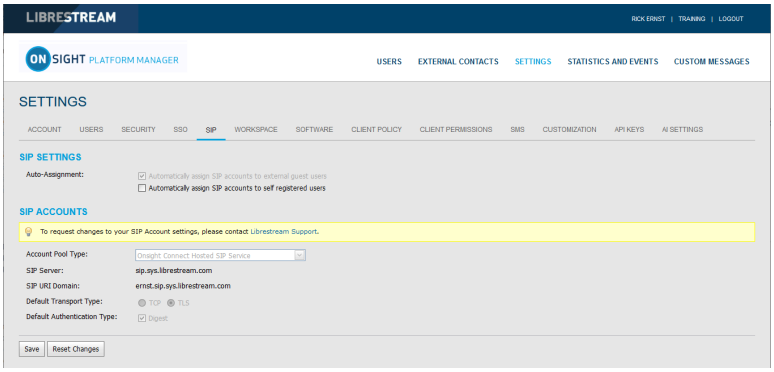


Figure 9-21 SIP Settings

Click **SETTINGS** from the main menu and click the **SIP** tab. The **SIP** page includes **SIP SETTINGS**, and **SIP ACCOUNTS** sections.

Session Initiation Protocol (SIP) is the underlying call control protocol that connects all Onsight Connect sessions. Each Onsight Connect user will have a SIP account automatically assigned to them. This section describes the SIP Settings for all users.

Tip: To request changes to your SIP Account settings, please contact mailto:support@librestream.com to setup SSO.

9.6.1. SIP Settings

Self-Registration Auto-Assignment

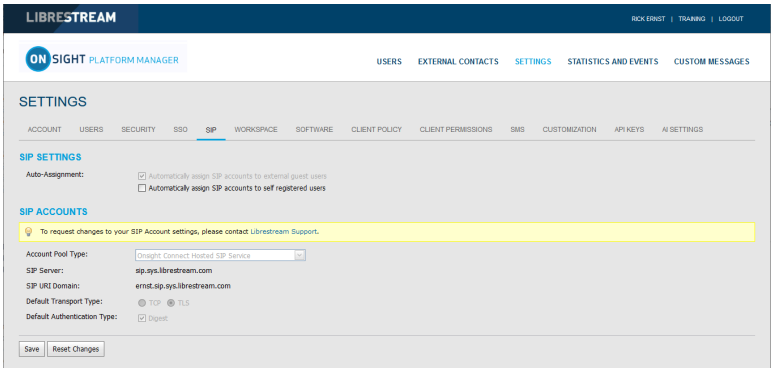


Figure 9-22 Auto-Assignment

Click **SETTINGS** from the main menu and click the **SIP** tab. The **SIP** page appears. Locate the **SIP SETTINGS** section.

When enabled, **Automatically assign SIP Accounts to self-registered users** will link a newly registered user to a SIP account. This should be enabled when using Self-Registration.

9.6.2. SIP Account

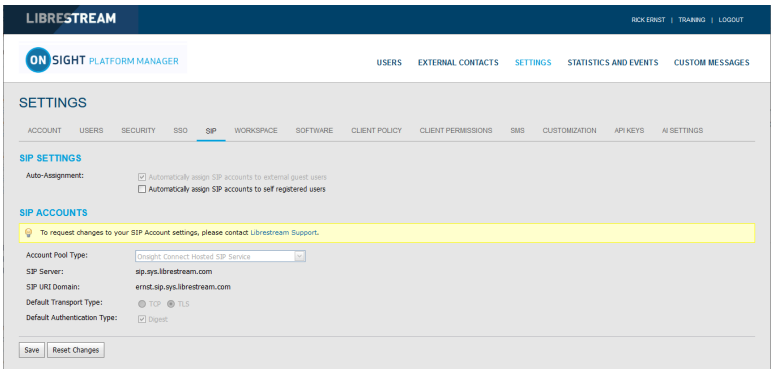


Figure 9-23 SIP Account

There are three SIP Server set up options accessible from the **Account Pool Type** drop-down menu:

1. **Onsight Connect Hosted SIP Service**
2. **Shared Account** (Enterprise SIP Server)
3. **Multiple Accounts** (Enterprise SIP Server)

When a Customer is hosting an Enterprise SIP Server, SIP Accounts are entered into the Auto-assignment Pool using either Multiple Accounts or a Shared Account.

When using a Shared Account, the SIP Server must support wildcard usernames. The SIP URI (SIP address) is automatically generated from the SIP URI domain and the user name associated with the Onsight User account.

The Transport selected (TCP or TLS) must match the configuration of the SIP Server to which you are registering. TLS is recommended for security. Accurate date and time on the endpoint is a requirement for TLS.

Each User can be assigned two SIP accounts: One Public, and one Private. This is to allow SIP registration depending on network location. If a user is internal to the Firewall, they will register to the Private Server. If they are external to the Firewall, they will register to the Public Server, e.g., Cisco VCS expressway and control.

Users that only register to a single SIP Server (Public or Private) need only provide SIP settings for the single server. Use the Public SIP settings as the primary SIP account.

9.6.2.1. Onsight Connect Hosted SIP Service

Onsight Connect Hosted SIP Service is the default SIP service used when you have subscribed to Librestream's Onsight Hosted Service.

The settings are read-only since SIP account information is automatically managed by Onsight Platform Manager in your domain. SIP Accounts are automatically assigned to each user when a user account is created by the OPM Administrator.

SIP settings include:

- **SIP Server** — Lists the Librestream SIP Server assigned to your domain.
- **SIP URI Domain** — Lists the SIP URI domain and appears as the domain portion for a user's SIP address, e.g., user@sipuridomain.com.
- **Default Transport Type** — TCP or TLS, the default is TLS. This provides encrypted communication for the SIP protocol.
- **Default Authentication Type** — Digest provided as read-only reference.

9.6.2.2. Multiple Accounts

Multiple Accounts are used when you are hosting your own Enterprise SIP server and have a fixed number of SIP Accounts available for use with Onsight Connect. Each SIP Account is created on your Enterprise SIP server with a unique authentication name, password and URI. It is then added manually to the OPM SIP Pool for use as Onsight Connect Users are added.

9.6.2.2.1. Creating Multiple Accounts

Login to OPM and select **SETTINGS** from the main menu and click the **SIP** tab.

To create multiple SIP Accounts, you will need to:

1. Acquire your Enterprise SIP account information from the SIP Server Administrator. The SIP Account information must include the SIP Server Address (Public and/or Private), Authentication name, Password, Username and SIP Domain (Username and SIP Domain are combined to create the SIP URI).

2. In the **SIP Settings** section, select **Automatically assign SIP accounts to self-registered users**.

3. Set the **Account Pool Type** to **Multiple Accounts**.

4. Set the **Public Server** to the public server address provided by your SIP Server Administrator.

5. Select **TCP** or **TLS** as the transport type. TLS is recommended.

6. Add the SIP Accounts information for each user by clicking the **New** button.

    - On the Public tab, enter the SIP URI (SIP URI = username & sip domain, e.g., `user@sip.librestream.com`), Authentication Name, and Authentication Password.

7. Repeat steps 4 to 6 for the Private Server if required.

8. **Save** the changes.
   This completes the procedure.

9.6.2.3. Shared Account

Shared Accounts are used when you have wild card SIP Accounts available for use with Onsight Connect. The wildcard SIP Account is first created on the SIP Server then added manually to the OPM SIP Pool for use as Onsight Connect Users are added. Each SIP account shares the same Authentication Name and Authentication Password but has a unique SIP URI. The SIP URI is created automatically by combining the Onsight user name and the SIP domain, e.g., jdoe@sipdomain.com.

9.6.2.3.1. Creating a Shared Account

Login to OPM and select **SETTINGS** from the main menu and click the **SIP** tab.

1. Acquire your SIP account information from your SIP server administrator. The SIP account information must include the **Server Address**, **SIP URI Domain**, **Authentication Name**, and **Authentication Password**.

2. In the SIP Settings section, select **Automatically assign SIP accounts to self-registered users**.

3. Set the **Account Pool Type** to **Shared Account**.

4. On the **Public Server** tab, set the **Server Address** to the address provided by your SIP server administrator.

5. Select **TCP** or **TLS** as the transport. TLS is recommended.

6. Set the **SIP URI Domain** to the domain provided by the SIP administrator.

7. Enter the **Authentication User Name**, and the **Authentication Password**.

8. Repeat steps 3 to 7 on the **Private Server** tab if required.

9. Click **Save**.
   This completes the procedure.

9.6.2.4. Manually Assigning SIP Accounts to Users

SIP Accounts are assigned when a new User Account is created. The **Automatically assign a SIP account to this user** check box is enabled by default.

SIP Accounts can also be assigned on the User and Groups tab by selecting an existing user (by checking the box beside their name) and then selecting **Assign/Restore SIP Account** from the **More** drop-down menu.

Once the SIP settings have been assigned/restored, the user's SIP Account settings will be available for use as soon as the new settings are received by the Onsight account. This will happen on next login or if already logged in, during next update from the server (within 60 seconds).

9.7. Onsight Workspace

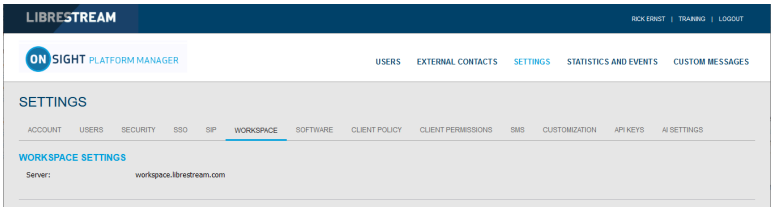


Figure 9-24 Onsight Workspace

When Onsight Workspace is enabled for your domain the Workspace server is displayed for reference on the settings page. As an administrator you must assign yourself a Workspace Enterprise license in order to configure Workspace settings.

Using Onsight Workspace, authorized users can upload, view, share, and manage Onsight data, images, and recordings as well as external content such as product manuals and schematics. With detailed permission controls, enterprises can ensure that only authorized teams and individuals can access specific content.

Workspace integrates with the full Onsight platform by providing a practical solution to aid in knowledge management and audit trail requirements. Workspace key features include:

- Automatic or manual upload of data, images, or recordings from Onsight
- Optional upload controls to manage field situations such as cellular data consumption
- Quick add option to store product manuals, schematics, or other files
- Content tagging for quick search and retrieval
- Automatic versioning of content with built-in audit capabilities
- Secure architecture and detailed permission controls
- Advanced reports to audit content and use across the enterprise
- Access content and data in your back-office systems with the Workspace API
- Select Enterprise or Contributor license types to control and extend Workspace data collection

Related information
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

9.7.1. Enabling Workspace Access for Users

Login to OPM.

To enable Workspace access for your users, you will need to:

1. Access the **Users** page and select the users you want to have Workspace access.

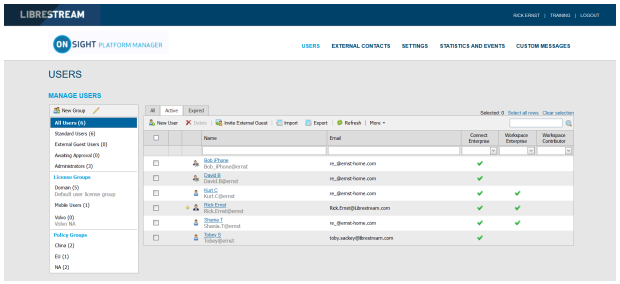


Figure 9-25 Users

2. Then select **More > Assign/Restore Workspace Account**.

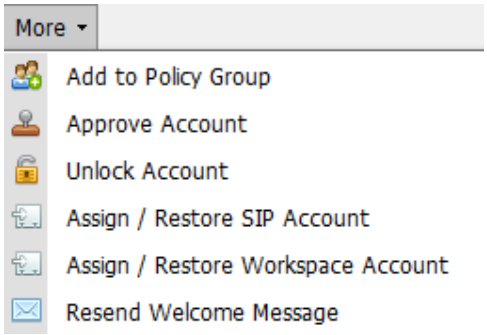


Figure 9-26 More drop-down menu

3. Place the Workspace users in a group. You may also choose to use an existing group such as **All Users**.
4. The final step is enabling Workspace in a **Group Client Policy** for the Users.
5. Select the group and click the **Modify Group** icon (pencil icon).
6. Select the **CLIENT POLICY** tab.
7. Click **Choose Settings**.
8. Select the **Workspace** settings to enable within **Client Policy** that include:
    - **Access** — Grants access to the Workspace.
    - **Upload Path** — Sets the default upload path in the Workspace.
    - **Auto Upload Media** — Enables auto upload of all media captured during a call when the call ends.
    - **Maximum Upload Bit Rate** (Kbps) — Sets the maximum bandwidth dedicated to the upload stream.
    - **Restrict Upload Folder Access to the Owner** — Only permits access to the owner's upload folder.
    - **Allow Cellular/Mobile Data Usage** — Allows cellular/mobile data usage for uploading media to the Workspace.
9. Click **OK**.
10. In the **Workspace** section set the desired Values.
    This completes the procedure.

Related information
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

9.8. Workspace Webhooks

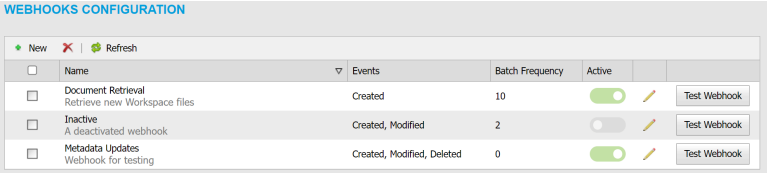


Figure 9-27 Webhooks

The On-premises Onsight Workspace and OPM solutions support a webhook notification mechanism that enables an external system to notify you when changes are made to Workspace assets. The notification is in the form of HTTP callbacks that are initiated from Onsight Workspace to your designated external service when an event occurs. Events for Workspace assets and documents are triggered when an item is created, modified, or deleted. Webhook notifications enable integrations for a variety of external platforms. For more details, please refer to the Onsight Workspace Webhooks guide.

Workspace Webhooks are created and managed by an OPM Administrator when Workspace is enabled and configured for your account.

9.8.1. Creating & Modifying a Webhook Configuration

Login to OPM as an Administrator. Click **Settings > Workspace**.

To create or modify a Webhook configuration, you will need to:

1. Access the **Webhooks CONFIGURATION** table to display a list of Webhooks.

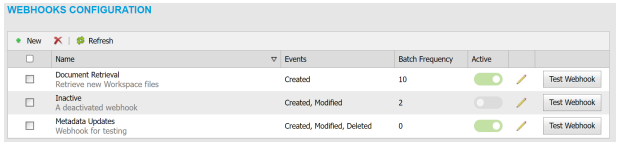


Figure 9-28 Webhooks Configuration

2. Click the **New** icon to add a webhook configuration. The New Webhook Configuration form appears.

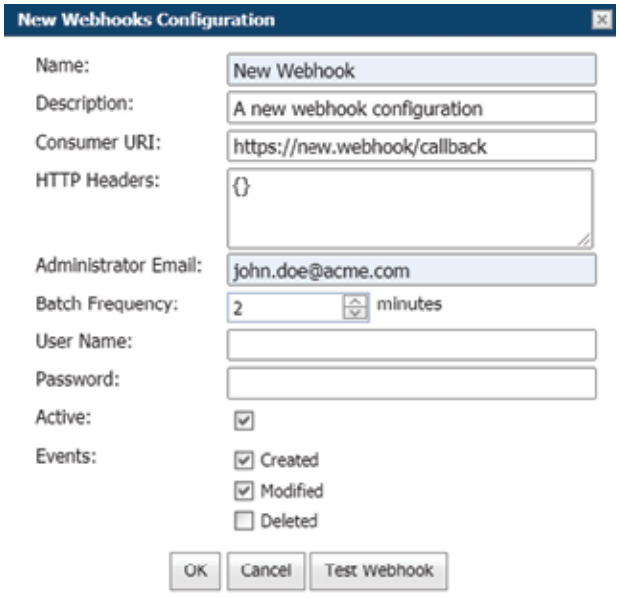


Figure 9-29 New Webhooks Configuration

3. Editable fields include:

    - **Name** (Required) — A friendly name for the webhook that is used for display purposes.
    - **Description** — An optional description for the webhook.
    - **Consumer URI** — The absolute URI for the destination service that will receive callback notifications.
    - **HTTP Headers** — Provides a list of key-value pairs for HTTP headers to be included with every notification sent to a Consumer URI.
    - **Administrator Email** — The email address for the administrator of this webhook configuration — All Status and/or delivery failure notifications will be sent to this email address.
    - **User Name/Password** — If set, the notification will use HTTP Basic authentication with these credentials.
    - **Active** — If unchecked, no notifications will be delivered for this webhook.
    - **Events** — The Types of events that will trigger webhook notifications for this configuration. You must select one event.

4. Enter all required fields and click **OK** to save the webhook configuration.

5. Click the **Edit**  icon to show the **Edit Webhook Configuration** pop-up. This is identical to the New Webhook Configuration pop-up and it enables you to make changes to an existing configuration.

6. Select one or more webhook configurations from the table and click the  **Delete** icon to permanently remove webhook(s). After deletion, no further notifications will be sent to consumer services for those configurations.

7. Click the **Test Workbook** button from within the **WEBHOOK CONFIGURATIONS** table or **New/ Edit Webhook Configuration** pop-up to test the configuration.

    - A test event notification triggers immediately and is sent to the Consumer URI from Workspace.
    - OPM will display test results including the test duration and status code returned to Workspace from your consumer service.

    This completes the procedure.

9.9. Software Updates

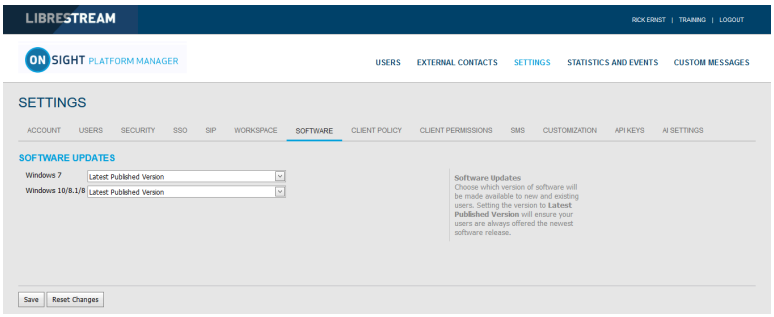


Figure 9-30 Software Page

Software distribution for Onsight Connect for Windows, the Onsight Cube, the 5000HD and the Collaboration Hub is managed by Onsight Platform Manager. Librestream provides updates as part of the Software Release process.

Related information
Software — Best Practices *(on page 116)*

9.9.1. Onsight Connect for Windows

The OPM Administrator can select which version of Onsight Connect for Windows is available for download by Onsight Connect users. You can select the **Latest Published Version** or a **Specific Version** from the drop-down list.

Depending on your selection, the Users will receive **Welcome emails** or **External Guest Invites** containing links to download the selected Versions of Onsight Connect for Windows.

Related information
Software — Best Practices *(on page 116)*

9.9.2. New Release Notifications

When the Latest Published Version is selected on the software updates page, Windows users will receive notifications at the Onsight Connect login window when a new version has been published and is available for download.

Android and iOS users will receive application updates through the App stores. Users may configure their phones to receive automatic updates from the App stores. Refer to their phone's app store instructions for automatic updates.

Related information
Software — Best Practices *(on page 116)*

9.9.3. Updates for Onsight Cube, Collaboration Hub and 5000HD

Librestream publishes the updates for the Onsight Cube and Collaboration Hub. These are available through Onsight Platform Manager as part of the regular software release process.

When a new release is available users can **Check for Updates** in order to download and install the latest software version by selecting:

- **SETTINGS > CUBE > CHECK FOR UPDATES**.
- **SETTING > COLLABORATION HUB > CHECK FOR UPDATES.**

9.9.4. On-premises Software Updates

Refer to the Onsight Platform Manager — Installation Guide for details on deploying update packages for Onsight Connect for Windows, Onsight 5000HD, and Onsight Collaboration Hub. Onsight mobile client updates are available in the App stores for on premises installations.

9.10. Client Policy & Permissions

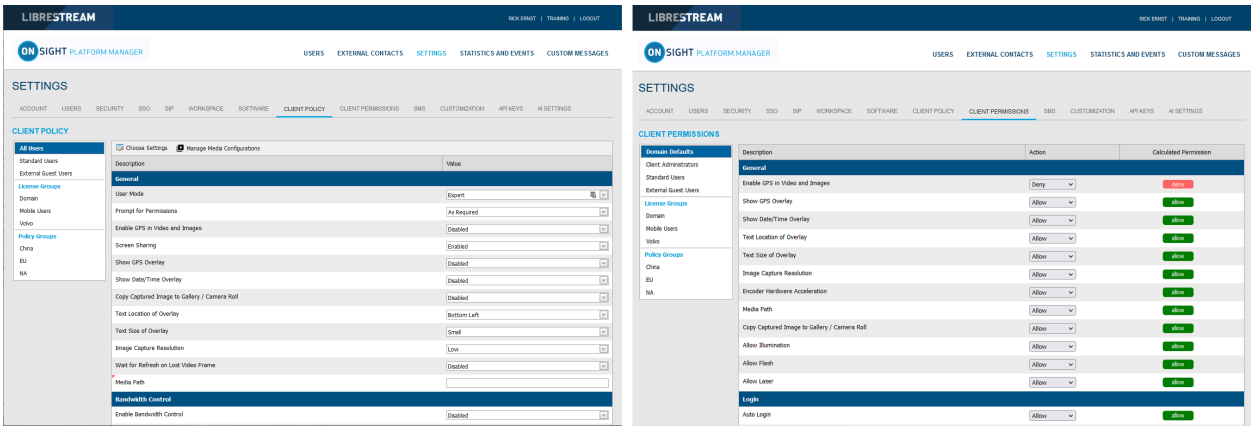


Figure 9-31 Client Policy & Client Permissions

CLIENT POLICY and **CLIENT PERMISSIONS** can be configured by clicking **SETTINGS** > **CLIENT POLICY** or **CLIENT PERMISSIONS** and are applied to the **All Users** group. The All Users group contains all users in the domain.

Client Policy allows the OPM Administrator to choose which configuration settings are applied to an Onsight endpoint based on Group membership (Group Policy) or an individually assigned User Client Policy.

Group Client Policy is applied to each member of a Group. Select the configuration for each setting based on Groups. Users can belong to multiple groups and the settings that are a higher priority take precedence.

User Client Policy is the policy associated directly with a user account. It is used to override any **Group Policy** applied based on Group Membership. If a user belongs to multiple Groups each with its own **Client Policy** applied, the user will be subject to Policy settings based on the **prioritized** setting between the Group and User Client Policy settings for that user. The default User Client Policy for a user is to **Inherit all** settings meaning **Group Policy** takes precedence. Each **Client Policy** category can be set to **Inherit**, **Override,** or **Clear**.

Edit Client Policy

To edit the **Client Policy** for a user, select the `User`, and then select the **CLIENT POLICY** tab. Set the policy for each setting under **Action**. The following options are available:

- **Inherit** — Applies the Group policy setting to the User. This is the Default for each setting when a new User is created.
- **Override** — Applies the setting that is configured on the User's Client Policy page not the Group Policy.
- **Clear** — Do not apply any policy for the settings, instead use the current value on the endpoint.

Related information

Client Policy & Priority Precedence *(on page 105)*
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

9.10.1. External Guest Users

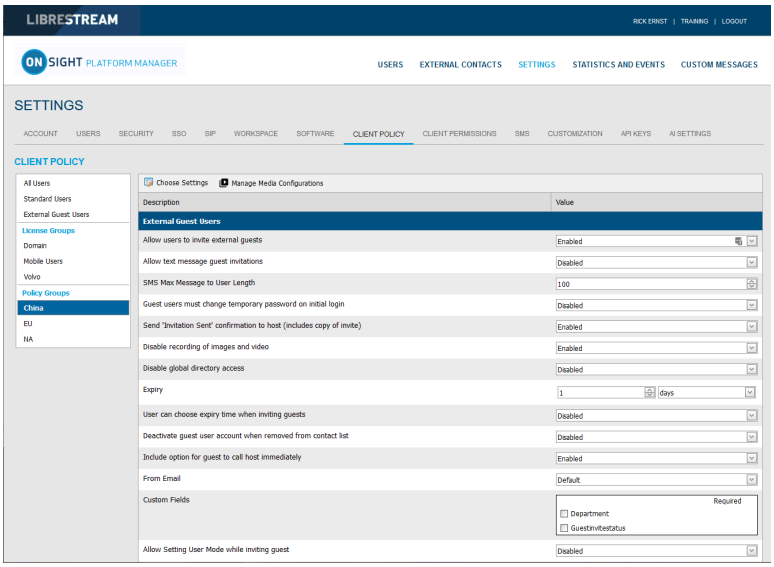


Figure 9-32 Group Client Policy

Note: Guest User behavior is now set at the group level. It is no longer a domain level configuration.

- **Allow users to invite external guest** — Allows users to invite guests. **Default**: **Enabled**.
- **Allow text message guest invitations** — Allows users to use text messages for guest invitations. **Default**: **Enabled**.
- **SMS Max Message to User Length** — Sets the number of characters allowed for the SMS message. **Default**: **100**.

  Note: SMS messages are limited to a maximum of 160 characters or less depending on the character set used. Exceeding this limit may break the links contained within the SMS message. Please respect this limit when making changes to SMS Messages. Refer to the Custom Messages Help on the CUSTOMIZATION page.

- **Password** — Controls whether External Guest users must change the temporary password on initial login. The **Default** option is **Enabled**.

  Note: You may want to disable this feature for Guest Users in order to simplify their Onsight Call experience.

- **Confirmation** — Controls whether the inviter will receive an email confirmation when the invite was sent. It will include a copy of the invite message. Colors assist with communicating the status of an invite. For example,
  - **Yellow** — The invite was sent, and the status is unknown. This typically indicates that the guest's email or SMS service provider has not acknowledged the receipt of the message.
  - **Green** — The invite was received by the guest.
  - **Red** — The invite not delivered.

  Note: Guest invite status is reported next to the guest's name in the inviter's contact list.

- **Permissions** — Set **Allow recording of images** and **video** to prevent a Guest from making Onsight recordings or capturing Onsight still images. The **Default** option is **Enabled**, i.e., External Guest Users cannot record images and video.

Tip: If desired, set **Allow global directory access** to prevent a Guest from searching the **Global Contacts Directory**. **Default**: **Disabled**, i.e., **External Guest** users can access the **Global Directory**.

Related information
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

9.10.2. External Guest Invitation Defaults

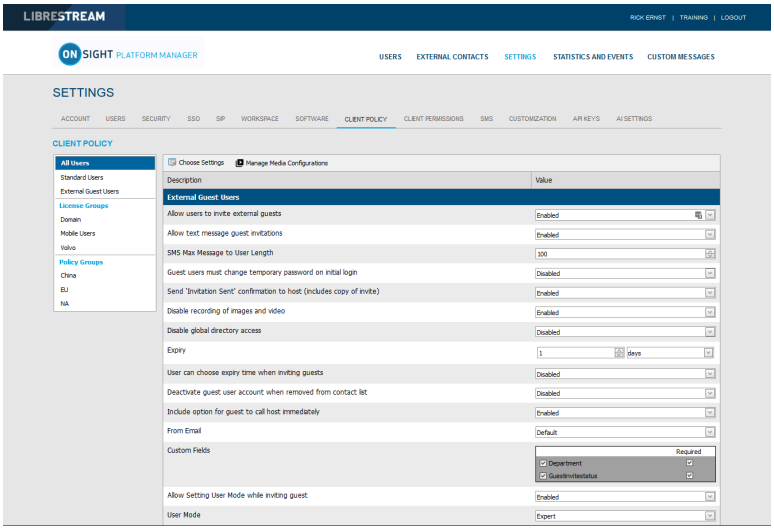


Figure 9-33 External Guest Client Policy

These settings control guest invite messages:

- **Expiry** — Sets the default expiry for the External Guest user account that is created when the guest invite is sent. **Default:** 1 day. **Minimum:** 1 day, **Maximum:** 365 days. Users can choose the expiry time when inviting guests:controls whether users can choose an expiry time other than the default. The **Default** option is **Disabled**.
- **Deactivate guest user account when removed from contact list** — Controls whether the guest user account is automatically deactivated when the inviter deletes the guest from their contact list. **Default**: **Disabled**.
- **Include option for guest to call host immediately** — Controls whether the guest user is prompted to call the inviter the first time they login. The **Default** option is **Enabled**.
- **From Email Address** — Sets the reply-to-address that is displayed in the guest invite email. You may choose the system default or to the `Inviter's email address` as the reply-to-address. The **Default** for Onsight Platform Manager is `no-reply@librestream.com`

  Note: The inviter must have an email configured for their account, if no email exists the system default will be used.

- **Custom Fields** — Set **Custom Fields** to include on the guest invite form.
- **Allow Setting User Mode while inviting guest** — Sets the guest's mode as **Expert** or **Field**.

Related information
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

9.10.3. Policy Precedence

Users who belong to multiple Groups will have configuration settings applied giving precedence to the **prioritized Client Policy** setting. For example, if Bob belongs to two groups: **Sales** and **Support**. The Sales Group has **Encryption** mode set to **Off**, but Support has **Encryption** set to **Auto**. Therefore, when Bob logs in, his configuration will be set to **Encryption** is **Auto**. In order for Bob to receive a client policy configuration set to **Encryption** is **Off**, he could either be **removed from the Support group**, or the **Encryption** setting could be set to **Override** in Bob's User **Client Policy** settings.

By default, all users in the Onsight Account Domain belong to the **All Users** group. In the example above, set the Encryption mode to **On** in the **All Users** policy. When Bob logs in, his configuration can now be set to **Encryption** is **On**, since it is a higher priority than the Encryption setting in either the **Sales** or **Support Group**. Since Bob cannot be removed from the **All Users** group, the only way to give him a lower priority Encryption setting would be to **Override** it in Bob's User **Client Policy** settings.

Related information

Client Policy & Priority Precedence *(on page 105)*
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

9.10.3.1. Setting Client Policy

Login to OPM and click **SETTINGS** from the main menu and select the **CLIENT POLICY** tab.

1. Select a `Group` within the **CLIENT POLICY** section on the left to apply a policy.

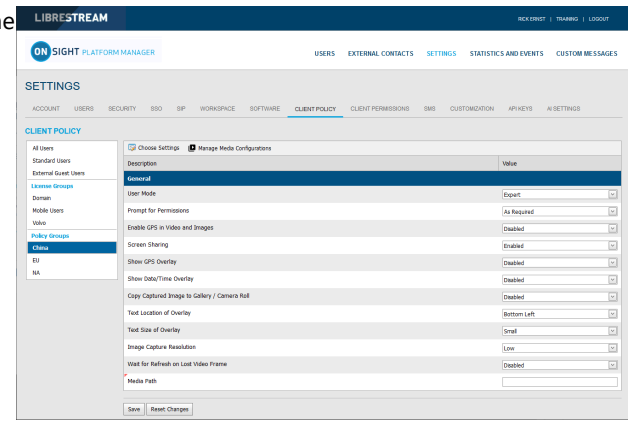


Figure 9-34 Group Client Policy

2. Click the **Choose Settings** icon. You will be presented with the **Choose Settings** window.

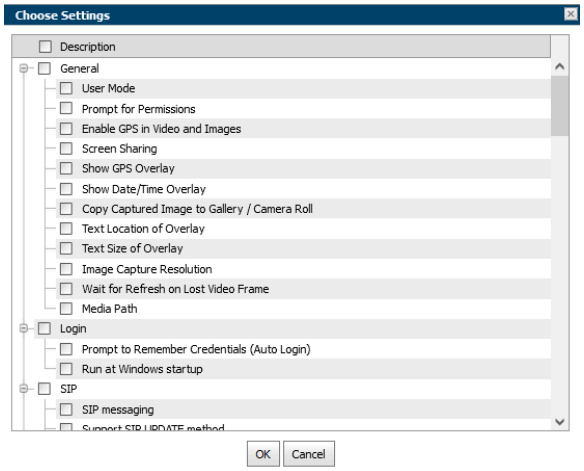


Figure 9-35 Choose Settings

3. Under each category, select each setting you would like to manage, or click the **Category Section** title to enable all. Click **OK**.
4. Click **Save**.
5. Set the appropriate value for each setting.

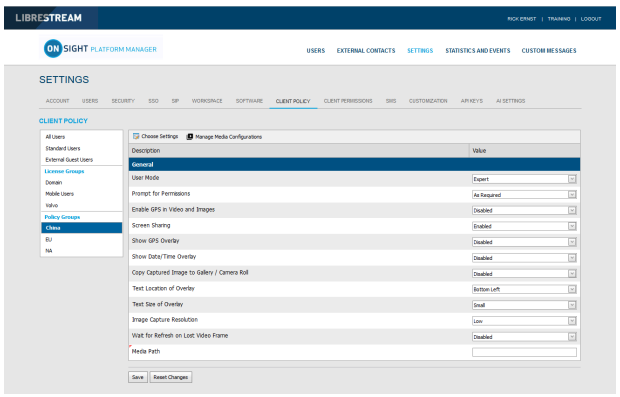


Figure 9-36 Setting Values

6. Repeat the process for each Group to which you want to apply a **Client Policy**.

Note: Client Policies can be applied to External Guest Users enabling you to manage privacy settings.

This completes the procedure.

Related information
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

9.10.3.2. Setting Client Permissions

Login to OPM and click **SETTINGS** from the main menu and select the **CLIENT PERMISSIONS** tab.

1. Select the **Group** you want to manage.

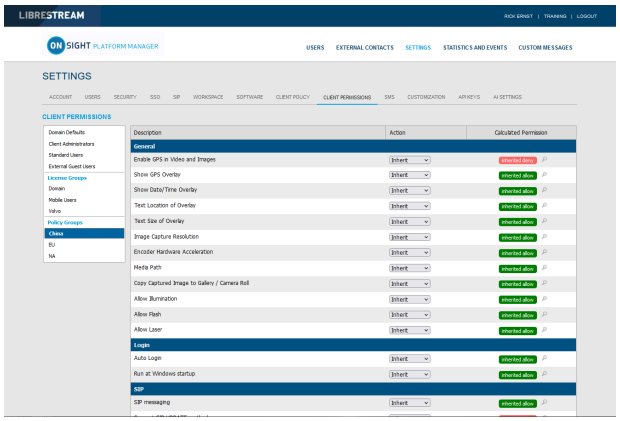


Figure 9-37 Setting Group Permissions

2. For each setting under **Description**, apply the Action you want applied for the permission.
   - **Allow** — Enables users to edit the setting.
   - **Deny** — Disables editing capability and does not allow users to edit the setting.
   - **Inherit** (Available only if the group is a child of a parent group).
3. Click **Save**.
   This completes the procedure.

Refer to the **Client Policy** and **Permissions** section for details.

Related information
Client Policy & Permissions *(on page 73)*
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

9.10.4. Group Client Policy and Permissions

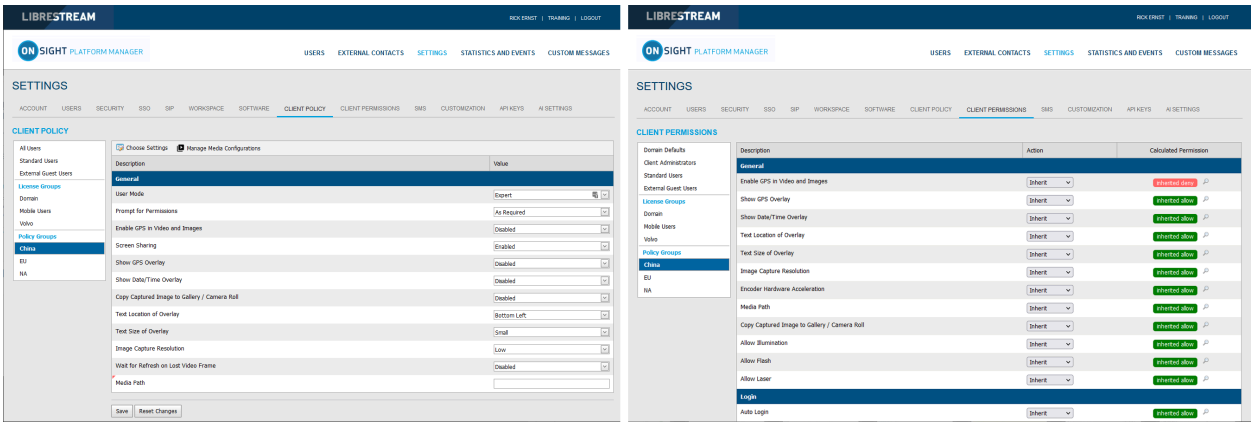


Figure 9-38 Group Client Policy & Permissions

Group Client policy is managed on the **USERS** page by editing groups. When a group client policy is created, it is 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** , **Android smartphone**, or an **Onsight Smart Camera**, their assigned **Client Policy** will be applied.

The Onsight Platform Manager Default Settings Template describes each available setting and provides best practices guidelines. It is available in the OPM section under **Manuals and Guides** on the Onsight Support website.

Group **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 for the setting. When a user is logged into Onsight Connect Software, **Allow** will let them edit the setting, **Deny** will prevent access, and **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. Refer to the [RE Insert XREF] Policy Precedence section for details.

Related information

Client Policy & Permissions *(on page 73)*
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

9.10.5. Remote Video Privacy

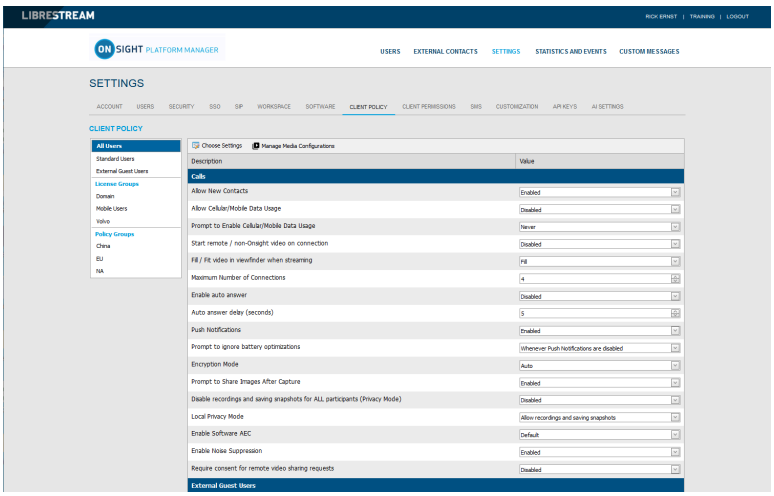


Figure 9-39 Privacy Settings

Onsight privacy settings require consent for remote video sharing requests during an Onsight call. When enabled, this gives customers greater control over video sharing, and users must provide consent before a remote participant can view video from their camera.

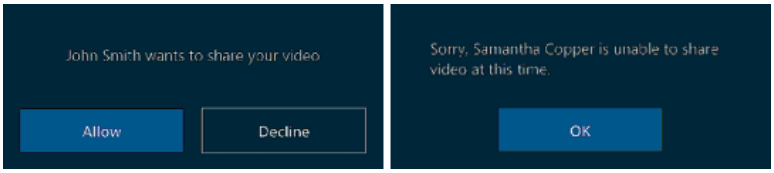


Figure 9-40 Requiring Consent

Video privacy is enhanced at sensitive locations by requiring users to provide consent before sharing video. Remote video privacy affects:

- **Client Policy > Calls** — Requires consent for remote video sharing requests. Options include:
  - **Enabled** — Forces user to grant permission to stream content from their camera.
  - **Disabled** (Default) — Automatically grants permission to stream content from their camera.
- **Client Permissions > Calls** — Requires consent for remote video sharing requests: Options include:
  - **Allow** — Grants permission for camera to be shared.
  - **Decline** (Default) — Denies camera access with the message: `"Sorry…. unable to share video at this time."`

Related information
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

9.10.6. WebEx CMR Compatibility

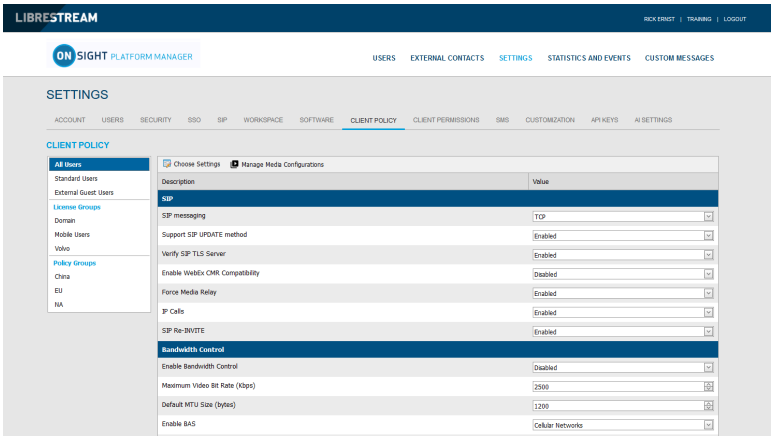


Figure 9-41 Client Policy

Access **Client Policy** and locate the **SIP** section to enable **WebEx CMR Compatibility**. **WebEx CMR Compatibility** enables Onsight Endpoints to call into WebEx Meeting rooms and act as a video/audio streaming endpoint. WebEx Meeting rooms will not accept calls from Onsight unless this feature is enabled.

Related information
Client Policy — Best Practices *(on page 117)*
Client Permissions — Best Practices *(on page 128)*

9.11. Short Message Service

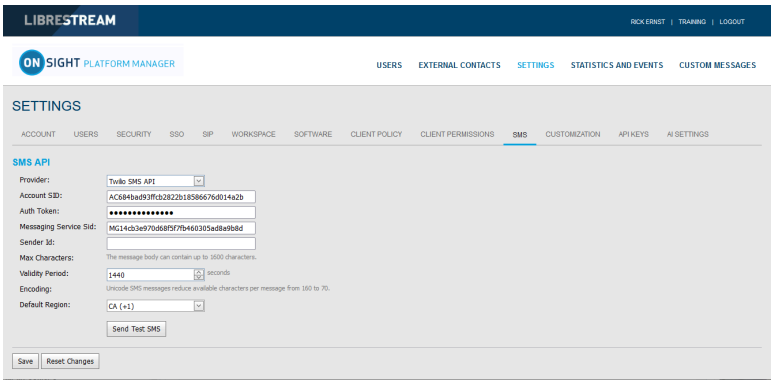


Figure 9-42 SMS Settings

Click **SETTINGS** from the main menu and click the **SMS** tab. The **SMS** page includes the **SMS API** section for configuring messaging service. This is included as part of the Enterprise and Pro platform subscriptions.

SMS enables users to send External Guest invites through the SMS Messaging Service to mobile phone clients.

Note: Librestream configures the SMS Settings page for the Customer — Changes must not be made to these settings. Please contact Librestream support for assistance if you are experiencing any issues with SMS guest invites.

Related information
CONTACT SUPPORT *(on page 103)*

9.12. Customization

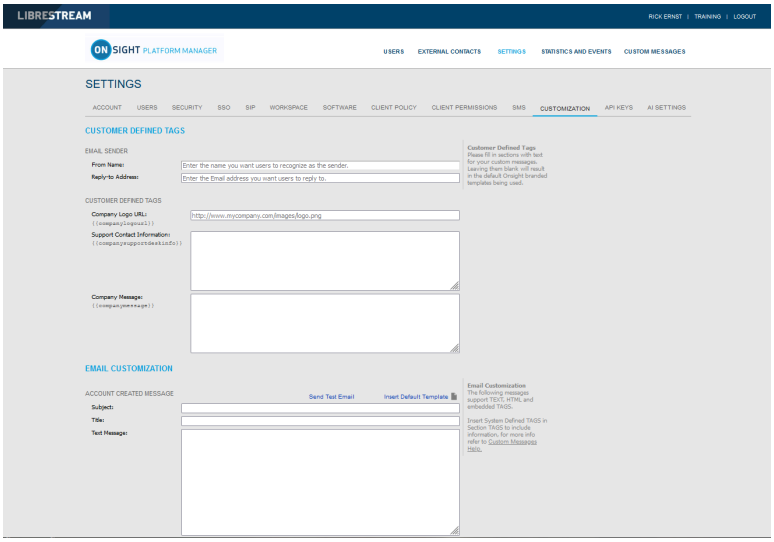


Figure 9-43 Customization

Click **SETTINGS** from the main menu and click the **CUSTOMIZATION** tab. The **CUSTOMIZATION** page includes the following sections: **CUSTOMER DEFINED TAGS**, **EMAIL CUSTOMIZATION**, and **SMS CUSTOMIZATION**.

Customization allows you to personalize email and SMS messages that Onsight Connect users receive from your company's Onsight domain.

Messages are sent out for the following events:

- **Account Created**
- **Account Deleted**
- **Account Registered**

- **External Guest Invitation**
- **External Guest Confirmation**
- **SSO Enabled Instructions**
- **Password Reset Request**
- **Password Changed Confirmation**

CUSTOMER DEFINED TAGS are used to access company and user specific information for placement in the messages. For more information, please refer to the **Custom Messages Help** on the **CUSTOMIZATION** page.

To view the default messages, click **Insert Default Template** beside the message text box. You can edit the default message template or create your own messages. Press **Save** to keep your changes.

9.13. Application Programming Interface Keys

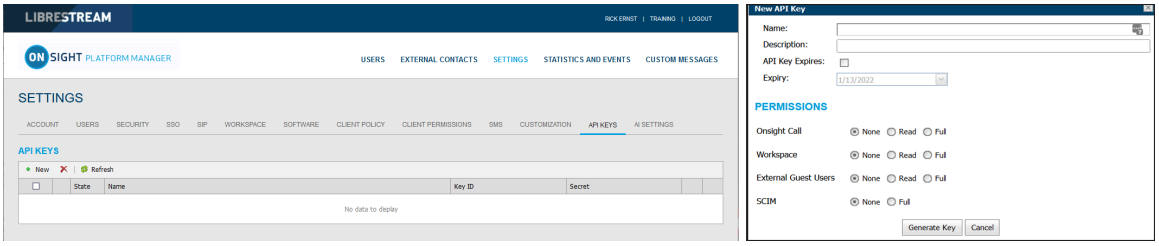


Figure 9-44 API Keys Page

Click **SETTINGS** from the main menu and click the **APIKEYS** tab. The **API KEYS** page enables you to manage access to the Onsight Call and Workspace REST APIs.

Click the  **New** icon to generate a new API authorization key. Provide the following details for each key:

1. **Name**.
2. **Description**.
3. **API Key Expires** followed by an **Expiry Date**.
4. Set the permissions for **Onsight Call**, **Workspace**, **External Guest Users** etc. as:
    - **None** — No access.
    - **Read** — Read only.
    - **Full** — Read/Write access.
5. Click **Generate Key**.

9.13.1. API Generated Key

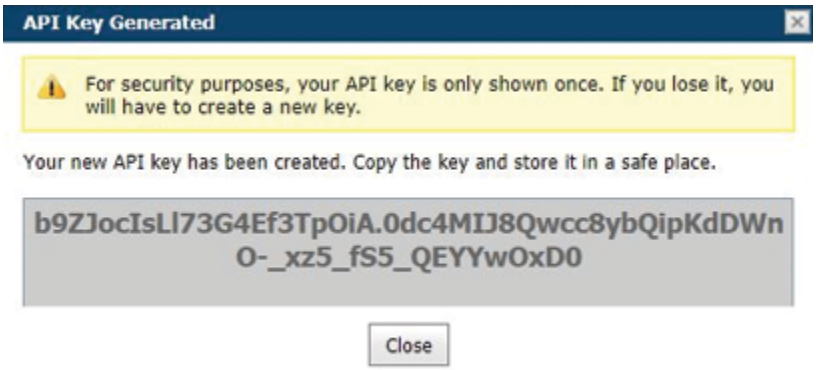


Figure 9-45 API Key Generated

Once the Key is generated the API Key Generated window will appear. It will state:

```
For security purposes, your API key is only shown once. If you lose it, you will have to create a new key.
```

When your new API key has been created, Copy the key and store it in a safe place. You will need this key to access the REST API endpoints.

After creation, the key cannot be viewed again but you may edit its associated properties such as the **Name**, **Description**, Expiry or Permissions. Click the **Edit** button to change API key properties.

You can lock the key from accessing Rest API endpoints by pressing the **Lock** button. Unlock the key to restore access to services.

Refer to the Onsight API guides for details on the REST API key usage.

9.14. Artificial Intelligence Settings

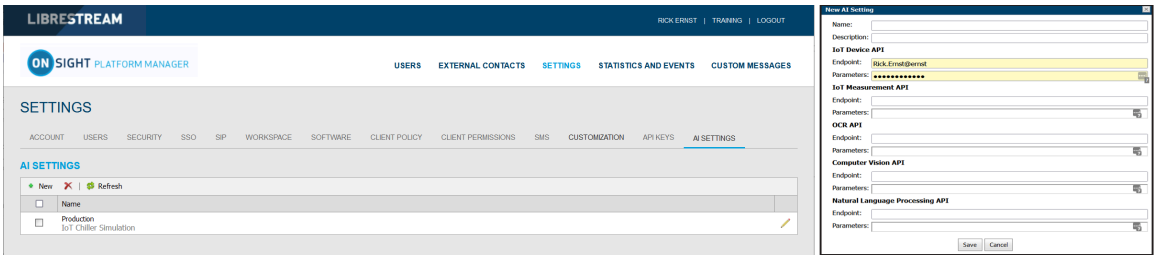


Figure 9-46 New AI Settings

Use the Artificial Intelligence (AI) Settings page to configure your Artificial Intelligence API endpoints and parameters. AI settings can be added to **Client Policy** to allow clients access to AI services including **Computer Vision** (CV), **Optical Character Recognition** (OCR), **Internet of Things** (IoT), and **Natural Language Processing** (NLP).

Press the **New** icon to create a new AI configuration. Enter the following information:

1. **Name**.
2. **Description**.
3. **IoT Device API**:
    a. **Endpoint** — Enter the URL.
    b. **Parameters** — Enter credentials.
4. **IoT Measurement API**:
    a. **Endpoint** — Enter the URL.
    b. **Parameters** — Enter credentials.
5. **OCR API**
    a. **Endpoint** — Enter the URL.
    b. **Parameters** — Enter credentials.
6. **Computer Vision API**
    a. **Endpoint** — Enter the URL.
    b. **Parameters** — Enter credentials.
7. **Natural Language Processing API**
    a. **Endpoint** — Enter the URL.
    b. **Parameters** — Enter credentials.
8. **Transcription API**
    a. **Endpoint** — Enter the URL.
    b. **Parameters** — Enter credentials.

Once the AI setting profiles are created, they are available for selection in the client policy under the **Artificial Intelligence > AI Setting Profiles** drop down list. You must add **AI settings** to the policy before they can be configured. Click **Choose Settings** on the **Client Policy** page.

A user must belong to a group that includes an **AI Setting Profile** to access AI services.

You may choose to combine or separate each AI service into a custom AI setting profile. E.g., IoT services may be configured by an AI setting profile that just describes the IoT Device API endpoint and parameters. However, only one AI setting profile may be applied to a client policy, so all AI services must be combined into a **single AI setting profile** if you want to have members of a group access more than one AI service.

10. STATISTICS AND EVENTS

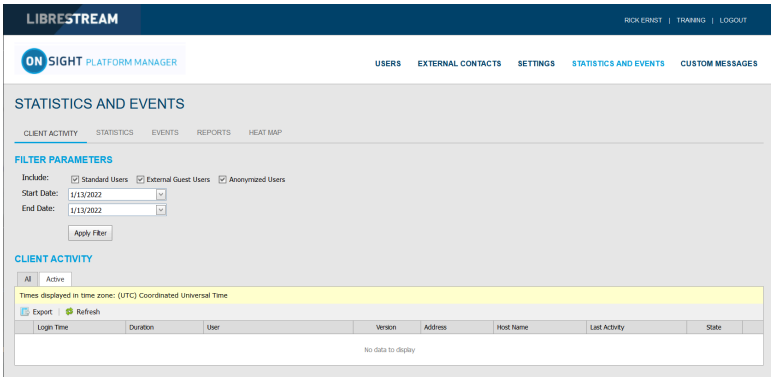


Figure 10-1 Statistics & Events

Click **STATISTICS AND EVENTS** from the main menu to configure settings that enable you to generate reports for Client Activity and Events for your organization. **STATISTICS AND EVENTS** enables you to access the following sections: **CLIENT ACTIVITY**, **STATISTICS**, **EVENTS**, **REPORTS** and **HEAT MAP**. Client Activity and Events can be viewed on the **STATISTICS AND EVENTS** page.

FILTER PARAMETERS

In general terms, modify the **FILTER PARAMETERS** using the check boxes to filter your information followed by drop-down menus to define your specific parameters and click **Apply Filter** to generate a report

10.1. Client Activity

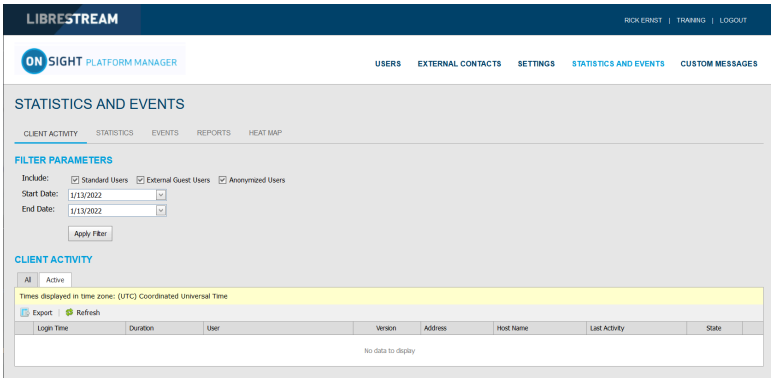


Figure 10-2 Client Activity

Click **STATISTICS AND EVENTS** from the main menu to access your **CLIENT ACTIVITY** page. The **CLIENT ACTIVITY** page contains **FILTER PARAMETERS** and a **CLIENT ACTIVITY** section.

Client Activity

The Client activity section displays all results within a table and tracks user activity for the Onsight Connect Service. The Administrator can display these results using the tabs. Select from:

- **All** — Displays all activity
- **Active** — Displays who is actively logged in.

10.1.1. Generating a Client Activity Report

Login to OPM and select **STATISTICS AND EVENTS** from the main menu, and select the **CLIENT ACTIVITY** tab.

To generate a Client Activity report, you will need to modify your **FILTER PARAMETERS**.

1. Determine which users to include by enabling one or more check boxes for:
    - **Standard Users**
    - **External Guest Users**
    - **Anonymized Users**

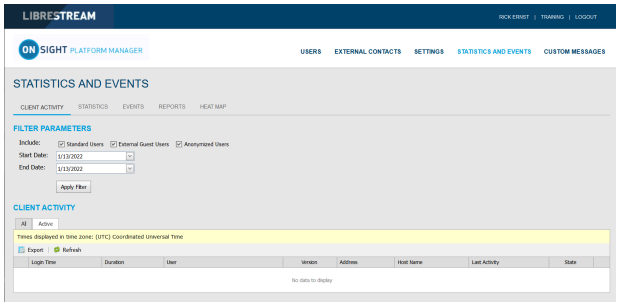


Figure 10-3 Filtering Users

2. Set your **Date** parameters. Click the drop-down menu and select a:
    a. **Start Date** using the **Calendar** pop-up menu.
    b. **End Date** using the **Calendar** pop-up menu.
3. Click **Apply Filter** to display results within the **CLIENT ACTIVITY All** tab.

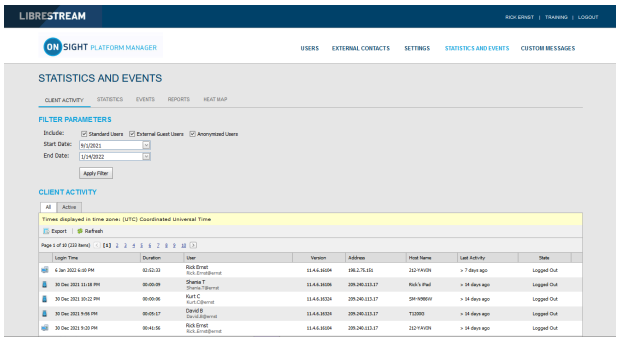


Figure 10-4 Client Activity Results

4. **CLIENT ACTIVITY** displays:
    a. **Login Time**
    b. **Duration**
    c. **User**
    d. **Version** of endpoint software
    e. **IP Address**
    f. **Host Name**
    g. **Last Activity**
    h. **State**
5. Clicking **Refresh** updates the list.
6. Clicking **Export** enables you to save a comma separated file (CSV) of the report.
   This completes the procedure.

10.2. Statistics

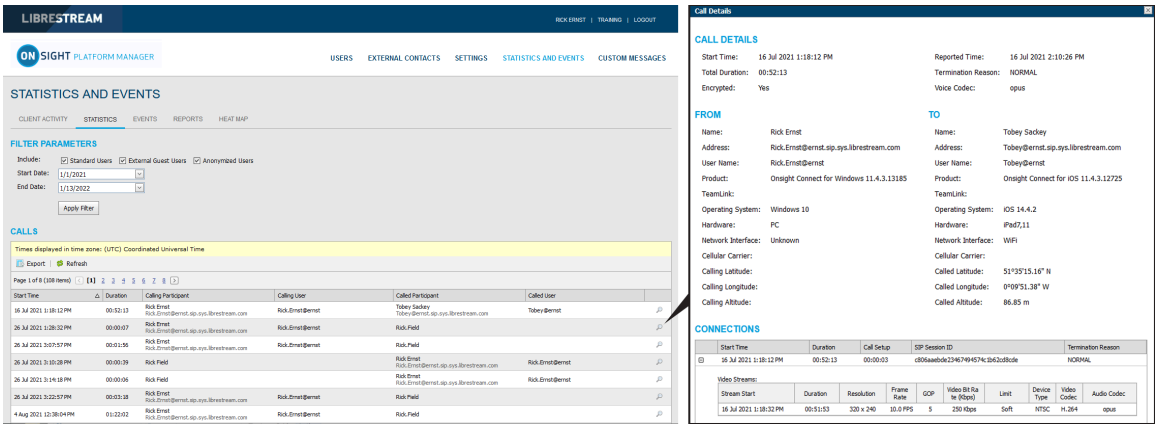


Figure 10-5 Statistics Report

Click **STATISTICS AND EVENTS** from the main menu and select the **STATISTICS** tab. The **STATISTICS** page contains **FILTER PARAMETERS** and **CALLS** section.

The **STATISTICS** page enables you to generate reports for call related statistics. Call related statistics are available for **Connect Enterprise** licensed users.

Note: Click the **Call Details** (Magnifying Glass) icon to display more information.

10.2.1. Generating a Statistics Report

Login to OPM and select **STATISTICS AND EVENTS** from the main menu, and select the **STATISTICS** tab.

To generate a Statistics report, you will need to modify your **FILTER PARAMETERS**.

1. Determine which users to include by enabling one or more check boxes for:
    - **Standard Users**
    - **External Guest Users**
    - **Anonymized Users**

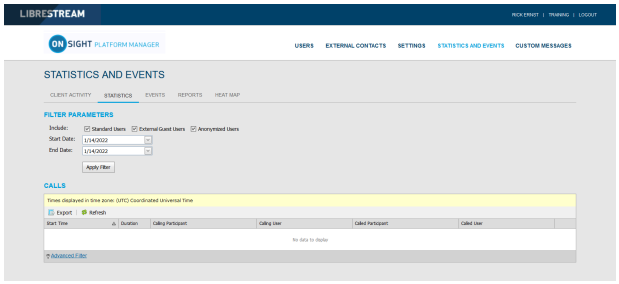


Figure 10-6 Filtering Users

2. Set your Date parameters. Click the drop-down menu and select a:
    a. **Start Date** using the Calendar pop-up menu.
    b. **End Date** using the Calendar pop-up menu.
3. Click **Apply Filter** to display results within the **CALLS** section.

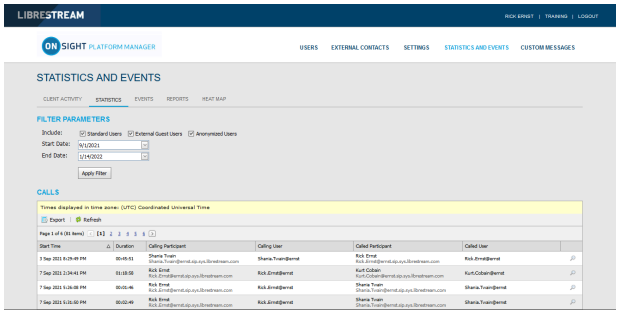


Figure 10-7 Statistic Report Results

4. **CALLS** displays the following fields:

    a. **Start Time**

    b. **Duration**

    c. **Calling Participant**

    d. **Calling User**

    e. **Called Participant**

    f. **Called User**

5. Clicking **Refresh** updates the list.

6. Clicking **Export** enables you to save a comma separated file (CSV) of the report.

Displaying Call Details

7. To view a user's details, click on the **Call Details** (Magnifying Glass) icon.

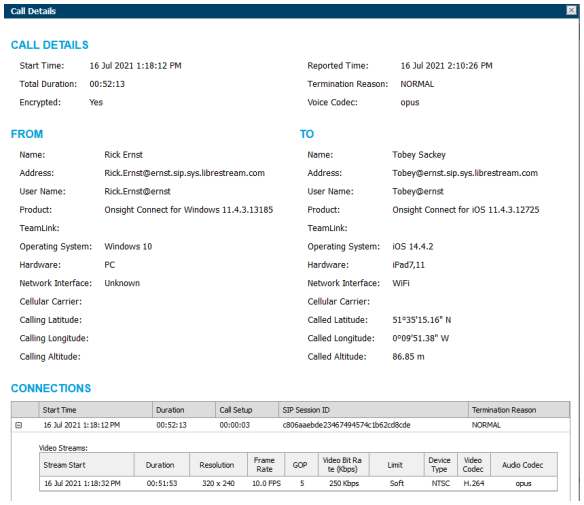


Figure 10-8 Statistic Call Details

8. The **Call Details** page displays:

    a. **CALL DETAILS**:

        i. **Start Time**

        ii. **Total Duration**

        iii. **Encrypted**

        iv. **Reported Time**

        v. **Termination Reason**

        vi. **Voice Codec**

9. **FROM**:

    a. **Name**

    b. **Address** (SIP)

    c. **User Name**

    d. **Product** (Client)

    e. **TeamLink**

f. **Operating System**

g. **Hardware**

h. **Network Interface**

i. **Cellular Carrier**

j. **Calling Latitude**

k. **Calling Longitude**

l. **Calling Altitude**

10. **TO**:

a. **Name**

b. **Address**

c. **User Name**

d. **Product** (Client)

e. **TeamLink**

f. **Operating System**

g. **Hardware**

h. **Network Interface**

i. **Cellular Carrier**

j. **Called Latitude**

k. **Called Longitude**

l. **Called Altitude**

11. **CONNECTIONS**:

a. **Start Time**

i. **Duration**

ii. **Call Setup**

iii. **SIP Session ID**

iv. **Termination Reason**

b. **Stream Start**

c. **Duration**

d. **Resolution**

e. **Frame**

f. **Group of Pictures (GOP)**

g. **Video Bit Rate**

h. **Limit**

i. **Device Type**

j. **Video Codec**

k. **Audio Codec**

12. Exit the page when done viewing.
    This completes the procedure.

10.3. Events

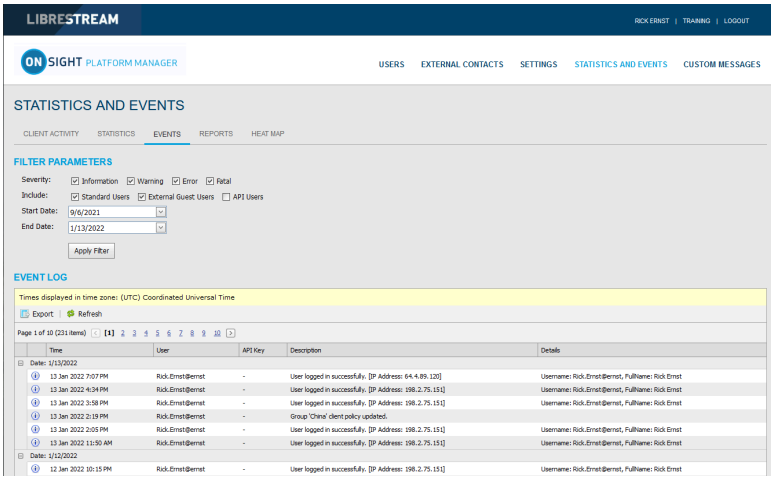


Figure 10-9 Events

Click **STATISTICS AND EVENTS** from the main menu and select the **EVENTS** tab. This page contains **FILTER PARAMETERS** and an **EVENT LOG** section.

The **EVENTS** page tracks administrator and user activity on OPM as well as Server based event messages. Set the **FILETER PARAMETERS** and click **Apply Filter** to display results within the **EVENT LOG** section.

10.3.1. Generating an Events Report

Login to OPM and select **STATISTICS AND EVENTS** from the main menu, and select the **EVENTS** tab.

To generate an **Events** report, you will need to modify your **FILTER PARAMETERS**.

1. Define **Severity** options by enabling check boxes for:
    - **Information**
    - **Warning**
    - **Error**
    - **Fatal**

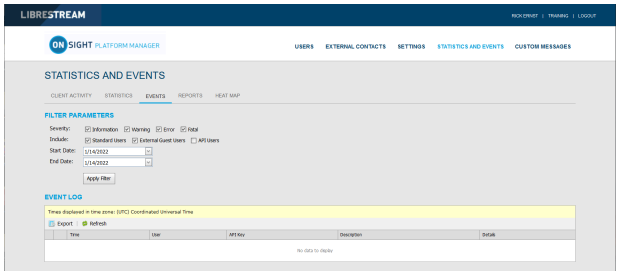


Figure 10-10 Filtering by Severity and Users

2. Determine which users to include by enabling one or more check boxes for:
    - **Standard Users**
    - **External Guest Users**
    - **API Users**
3. Set your **Date** parameters. Click the drop-down menu and select a:

a. **Start Date** using the Calendar pop-up menu.

b. **End Date** using the Calendar pop-up menu.

4. Click **Apply Filter** to display results within the **EVENT LOG** section.

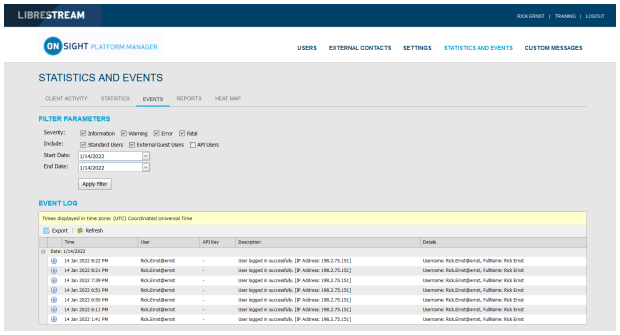


Figure 10-11 Statistics Report Results

5. The Event Log displays:

   a. **Time**

   b. **User**

   c. **API Key**

   d. **Description**

   e. **Details**

6. Clicking **Refresh** updates the list.

7. Clicking **Export** enables you to save a Comma Separated Value (CSV) file of the report.
   This completes the procedure.

10.4. Reports

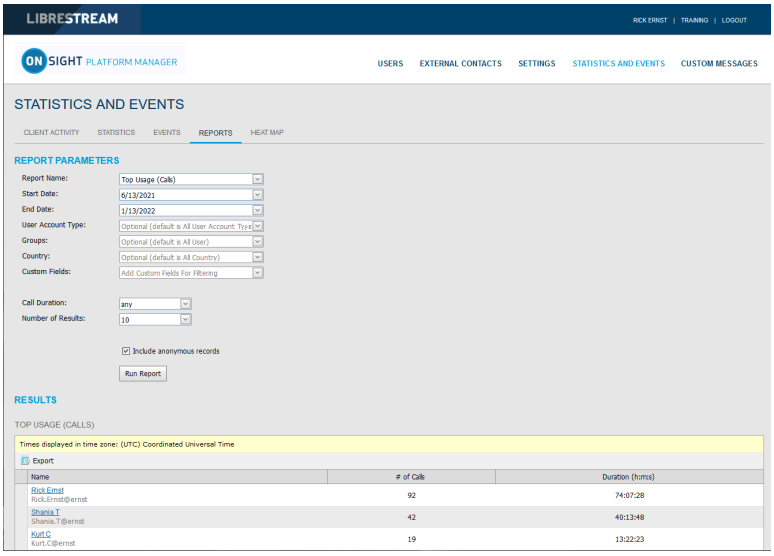


Figure 10-12 Reports

Click **STATISTICS AND EVENTS** from the main menu and select the **REPORTS** tab. The **REPORTS** page contains **FILTER PARAMETERS** section. When a report is generated, the **RESULTS** section appears with the report data.

Reports enable you to generate usage statistics, including who logged in to the software, how many calls a person placed and received, and the total and average duration of calls to help determine how well the technology is being adopted. Some of the benefits of regular Top and Least Usage review include:

- Identification of top users as potential leaders.
- Identification of candidates for mentorship/coaching.
- Underscoring management's support and interest in the new technology.

License and Overall Usage Summary reports list the # of licenses used or # of calls made during a period.

Note: If Data Anonymization is enabled for your domain, then any data that exceeds the Data Retention Period (DRP) is anonymized. Anonymized call records can be:

- Used to provide historical trends.
- Included in the counts for Call reports.
- Attributed to the user's groups, country, custom fields and other filters.
- Included in an exported CSV file.
- Visible in the Client Activity table.
- Filtered using Custom Fields.

Note: Call History is stored locally on clients and is not anonymized. It can be removed when the app is uninstalled. Previously deleted users data can be anonymized upon request.

10.4.1. Generating a Report

Login to OPM and select **STATISTICS AND EVENTS** from the main menu and select the **REPORTS** tab.

To generate a report, you will need to modify your **FILTER PARAMETERS**.

1. Select the name of the report to run within the **Report Name** drop-down menu.

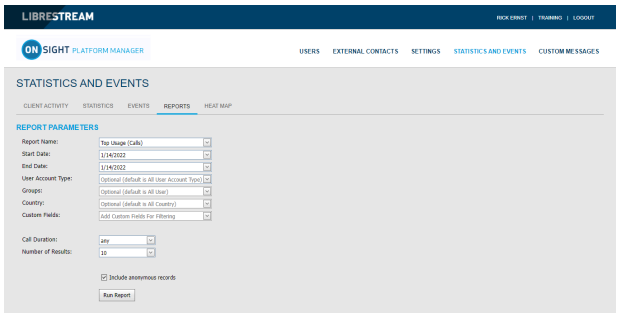


Figure 10-13 Report Parameters

2. Select from:
    a. **Top Usage** (Calls)
    b. **Least Usage** (Calls)
    c. **Top Usage** (Logins)
    d. **Least Usage** (Logins)
    e. **Top Usage** (Bandwidth)
    f. **Least Usage** (Bandwidth)
    g. **License Usage Summary** — Provides a list of the # of licenses used during the period.

h. **Guest Invite Summary** — Provides a list of the # of guest invites sent for the period including sender, guest, invite status, etc.

i. **Overall Usage Summary** — Provides a list of the # of calls and the total duration for the period.

3. Define the **Start Date** and **End Date** for the report by clicking the drop-down menus to access a **Calendar** pop-up.
4. Define the user type from the **User Account Type** drop-down menu. Select from:
   - **Standard Users**
   - **External Guest Users**
   - **All Users**
5. (Optional) Click to enable check boxes for the **Groups** to include in the report. The default is **All Users**).
6. (Optional) Click to enable check boxes for the **Country** to filter on. The default is **All Countries**.
7. (Optional) Select **Custom Fields** for filtering (optional — default includes all custom fields).
8. Set **Call Duration** using the drop-down menu. Select from:
   a. **any**
   b. **greater or equal**
   c. **less or equal**
   d. **between**
9. Set the **Number of Results** using the drop-down menu to include in the report. Select from **10**, **25, 50 100** etc.
10. Enable the check box option to **Include anonymous records**, as necessary.
11. (Optional) Click **Run Report** to display results.

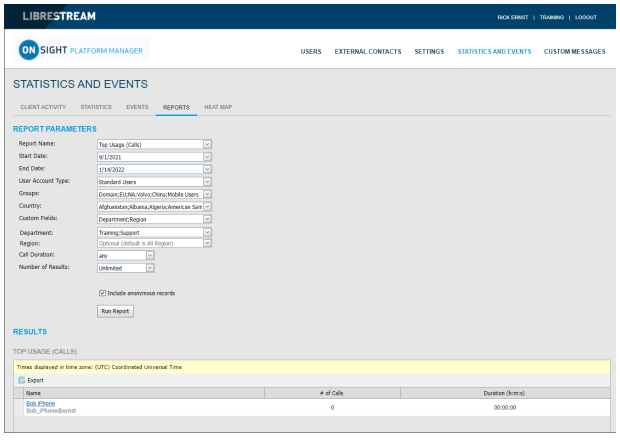


Figure 10-14 Report Results

12. (Optional) Click **Export** to save, download and view the results as a Comma Separated Value (CSV) file.
This completes the procedure.

10.5. Heat Maps

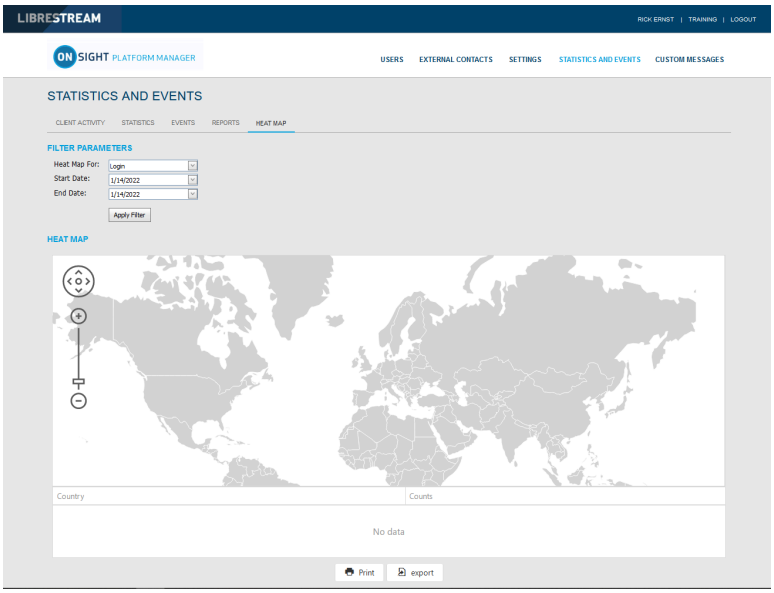


Figure 10-15 Heat Map Page

Click **STATISTICS AND EVENTS** from the main menu to access **HEAT MAP** page. The **HEAT MAP** page contains a **FILTER PARAMETERS** and a **HEAT MAP** section.

Heat Maps present Calls or Logins quantities that are filtered by IP address location and quantity. Calls can be filtered to display the **Caller**, **Callee**, or **Both** on the map.

Note: The Heat Map represents a count of client connections based on apparent IP address. Some variation could occur due to routing to cell towers or firewall entry to public Internet.

10.5.1. Generating a Heat Map Report

Login to OPM and select **STATISTICS AND EVENTS** from the main menu, and select the **HEAT MAP** tab.

To generate a Heat Map report, you will need to modify your **FILTER PARAMETERS**.

1. Use the **Heat Map For** drop-down menu to choose the information source to generate the report from. Select from:
    - **Call**
    - **Login**

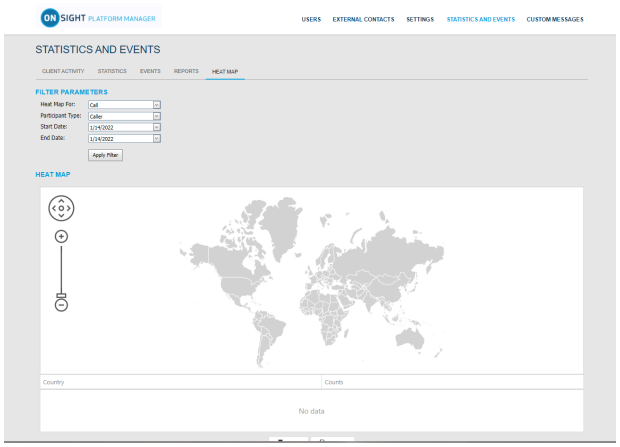


Figure 10-16 Heat Map Filter Parameters

2. **Call** Option Only — Enables you to also select the **Participant Type** as:
    - **Caller**
    - **Callee**
    - **Both**
3. Define the **Start Date** and **End Date** of the report by clicking the drop-down menus to access a calendar pop-up.
4. Click **Apply Filter** to run the report. The Heat Map will be displayed indicating the location and quantity of calls/ logins.

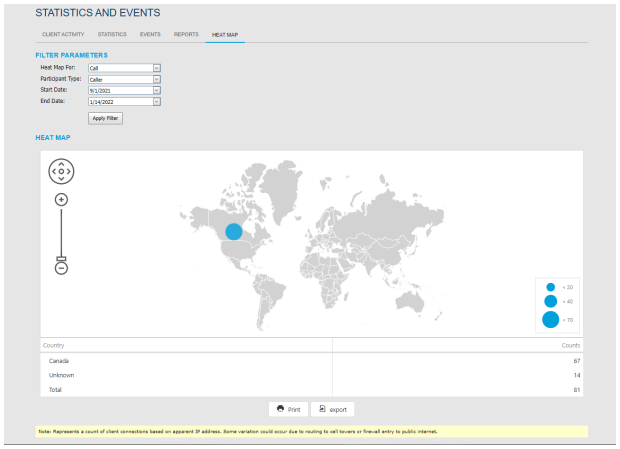


Figure 10-17 Heat Map Report Results

5. (Optional) Click **Print** to print a PDF copy of the map.
6. (Optional) Click **Export** to save, download and view the results as a Comma Separated Value (CSV) file.
This completes the procedure.

11. LANGUAGE SUPPORT

Onsight Connect supports the following languages for **Windows**, **Smartphones**, and **Tablets**:

- Chinese (Simplified)
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Portugal and Brazil)
- Russian
- Spanish
- Swedish

OPM will display the pages requested by Onsight Connect based on the client system's language. No configuration is required or your Onsight domain.

The Onsight Platform Manager is currently available in English only, but it displays localized pages to the client's browser for the following:

1. **Invite Guest**
    - **Onsight Connect for Windows** download
    - **Register for an Account**
    - **Forgot Password**
    - **Reset Password**
    - **SSO** login
2. **Emails originating from OPM** are localized and include:
    - Account registered (HTML, text)
    - Guest user confirmation (text)
    - Guest user invitation (HTML, text, SMS)
    - Password reset request (text, SMS)
    - User password changed (text, SMS)

12. CUSTOM MESSAGES

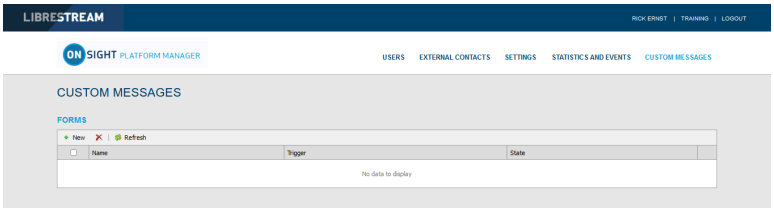


Figure 12-1 Custom Messages

Custom Messages can be displayed within the Onsight Connect application at login or before starting a recording. **Custom Messages** must be acknowledged by a user before login completes or a recording is started. If the message is not accepted by the user then the action will not be allowed. The Users must press **OK** to continue or the user will be returned to the login window and the recording will not start.

Tip: Typically, custom messages are used to display the terms of use for using the Onsight Connect within your company.

12.1. Creating a Custom Message (Form)

Login to OPM and click the **CUSTOM MESSAGES** from the main menu to manage custom messages forms.

1. Press the **New** icon to create a new custom message.

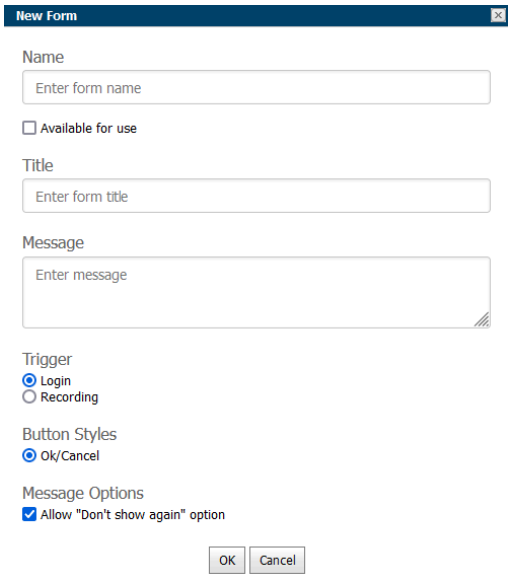


Figure 12-2 New Form

2. Enter the following parameters:

    a. **Name** — This field is only visible within OPM.

    b. Enable the **Available for Use** check box if you want the form available for use in **Client Policy**.

    c. **Title** — This field is displayed in the app.

    d. **Message** — This is the message the users will see. There is a 500-character limit.

    e. **Trigger** — Select the event that will trigger the display of the message, **Login** or **Recordings**.

    f. **Button Styles** — Select the style of response buttons you to display. **OK**/**Cancel** is currently the only option.

g. **Message Options** — Set whether you want the user to be able to select the **Don't show again** option. If you want a user to be prompted each time they login or make a recording, then disable this option.

h. Click **OK** to save your custom message. Click **Cancel** if you don't want to save your changes.

This completes the procedure.

12.2. Custom Messages & Client Policy

Custom Messages must be added to a **Client Policy** in order to be displayed within Onsight Connect. You can display one or more custom messages within the application i.e., both **Login** and **Recording** messages can be used in the same client policy.

12.2.1. Modifying Client Policy to Support Custom Messages

Login to OPM.

1. Click **USERS** from the main menu and select a group.
2. Press the **New Group** icon.
3. Select the **CLIENT POLICY** tab.
4. Select **Choose Settings**.
   a. Select **Login** if you want to display a Login message.
   b. Select **Recording** if you want to display a Recording message.
5. Click **OK** to return to the **Client Policy** section.
6. Scroll down the page to the **Custom Messages** section.
   a. Select the **Login** message you want to display.
   b. Select the **Recording** message you want to display.

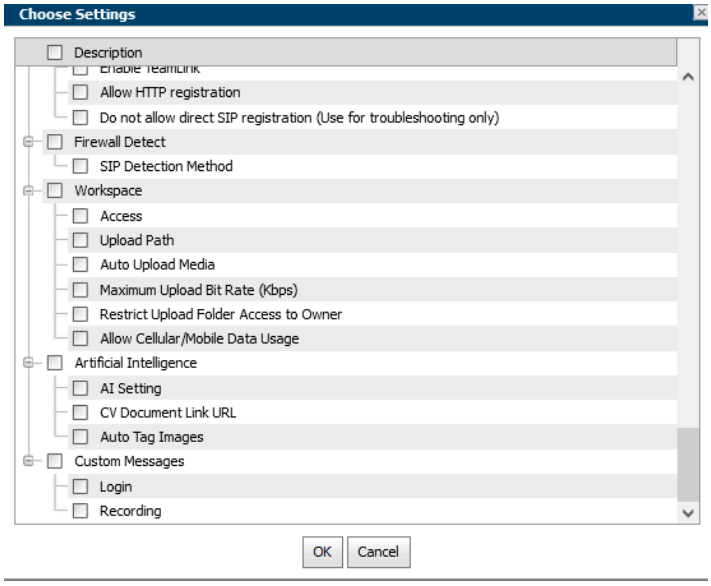


Figure 12-3 Choose Settings

7. Press **Save** to keep your changes.
   This completes the procedure.

13. 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/

14. CONTACT SUPPORT

Figure 14-1 Contact Support QR Code

For Support inquiries:

- **Email**: mailto:support@librestream.com
- **Web**: https://librestream.com/contact-us-support/
- **Phone**: 1.800.849.5507 or +1.204.487.0612

APPENDICES

Client Policy & Priority Precedence

Client Policy Item	Priority (High to low)
General	
User Mode	1. **Field** 2. **Expert**
Prompt for Permissions	1. **On Login** 2. **As Required**
Enable GPS Location in Video and Images	1. **FALSE** 2. **TRUE**
Show GPS Overlay	1. **FALSE** 2. **TRUE**
Show Date/Time Overlay	1. **FALSE** 2. **TRUE**
Copy Captured Image to Gallery / Camera Roll	1. **FALSE** 2. **TRUE**
Text Location of Overlay	1. **Bottom Left** 2. **Bottom Right** 3. **Top Left** 4. **Top Right**
Text Size of Overlay	1. **Large** 2. **Medium** 3. **Small**

Client Policy Item	Priority (High to low)
Image Capture Resolution	1. **Max** 2. **High** 3. **Medium** 4. **Low**
Media Path	**Undefined** — This setting accepts the value for the last group in list.
Login	
Prompt to Remember Credentials (Auto Login)	1. **Disabled** 2. **Enabled**
Run at Windows startup	1. **FALSE** 2. **TRUE**
SIP	
SIP messaging	1. **UDP** 2. **TCP**
Support SIP UPDATE method	1. **FALSE** 2. **TRUE**
Verify SIP TLS Server	1. **TRUE** 2. **FALSE**
Enable WebEx CMR Compatibility	1. **TRUE** 2. **FALSE**
Force Media Relay	1. **FALSE** 2. **TRUE**
Media Configurations	
Custom Media Configurations	**Combined list from all groups**
Bandwidth Control	
Enable Bandwidth Control	1. **TRUE** 2. **FALSE**

Client Policy Item	Priority (High to low)
Maximum Video Bit Rate (Kbps)	1. **Lower Value** 2. **Higher Value**
Enable BAS	1. **On** 2. **Cellular Networks** 3. **Off**
Media Configuration on Connection	**Undefined** — This setting accepts the value for the last group in list.
Pause Video While Transferring Image	1. **FALSE** 2. **TRUE**
Preferred Voice Codec	1. **Low Bandwidth (GSM)** 2. **Default (G.711)**
Preferred Subject Audio Codec	1. **Disabled** 2. **Low Bandwidth (GSM)** 3. **Default (G.711)**
Audio Efficiency	1. **Lower bandwidth** 2. **Mid** 3. Lower latency
Calls	
Allow Cellular / Mobile Data Usage	1. **FALSE** 2. **TRUE**
Prompt to Enable Cellular / Mobile Data Usage	1. **On Every Login** 2. **On First Login** 3. **Never**
Start remote / non-Onsight video on connection	1. **FALSE** 2. **TRUE**

Client Policy Item	Priority (High to low)
Fill / Fit video in viewfinder when streaming	1. **Fill** 2. **Fit** 3. **Actual Size**
Maximum Number of Connections	1. **Lower Value** 2. **Higher Value**
Enable auto answer	1. **FALSE** 2. **TRUE**
Auto answer delay (seconds)	1. **Lower Value** 2. **Higher Value**
Push Notifications	1. **TRUE** 2. **FALSE**
Prompt to ignore battery optimizations	1. **Only when user disables Push Notifications** 2. **Whenever Push Notifications are disabled**
Encryption Mode	1. **On** 2. **Auto** 3. **Off**
Prompt to Share Images After Capture	1. **FALSE** 2. **TRUE**
Disable recordings and saving snapshots for ALL participants (Privacy Mode)	1. **TRUE** 2. **FALSE**
Local Privacy Mode	1. **Disable recordings and saving snapshots** 2. Disable recordings 3. Disable saving snapshots 4. **Allow recordings and saving snapshots**

Client Policy Item	Priority (High to low)
Networking	
Diffserv DSCP (Voice)	1. **Voice** 2. **Audio / Video / Guaranteed** 3. **Controlled Load** 4. **Best Effort**
Diffserv DSCP (Video)	1. **Voice** 2. **Audio / Video / Guaranteed** 3. **Controlled Load** 4. **Best Effort**
Diffserv DSCP (Subject Audio)	1. **Voice** 2. **Audio / Video / Guaranteed** 3. **Controlled Load** 4. **Best Effort**
Diffserv DSCP (Data Stream)	1. **Voice Audio** 2. **Video** 3. **Gauranteed Controlled Load Best Effort**
TeamLink	
Enable TeamLink	1. **TRUE** 2. **FALSE**
Allow HTTP registration	1. **TRUE** 2. **FALSE**
Do not allow direct SIP registration (User for troubleshooting only)	1. **TRUE** 2. **FALSE**
Firewall Detect	
SIP Detection Method	1. **SIP Server — Full** 2. **SIP Server — Basic** 3. **TeamLink**
Workspace	

Client Policy Item	Priority (High to low)
Access	1. **TRUE** 2. **FALSE**
Upload Path	**Undefined** — This setting accepts the value for the last group in list.
Auto Upload Media	1. **TRUE** 2. **FALSE**
Maximum Upload Bit Rate (Kbps)	1. **Lower Value** 2. **Higher Value**
Restrict Upload Folder Access to Owner	1. **TRUE** 2. **FALSE**
Allow Cellular / Mobile Data Usage	1. **TRUE** 2. **FALSE**

Client Policy Item	Priority (High to low)
Custom Messages	
Login	**Undefined** — This setting accepts the value for the last group in list.
Recording	**Undefined** — This setting accepts the value for the last group in list.

Related information

Client Policy & Permissions *(on page 73)*
Policy Precedence *(on page 75)*

Best Practices

15.2.1. Account — Best Practices

Table 15-1 Account — Best Practices

Settings		Description	Best Practices/Tips
ACCOUNT INFORMATION			
Company Name:		Enter a company name	
Customer Domain:		Enter the company domain	
Account Owner:			
Customer Created:		Date and time customer created	
Customer Expires:		Date account usage will expire	
Super Administrator Access:		Ability to remove account access from Librestream Internal Operations. **Note:** Enable access when Librestream Support needs to review your OPM settings	
ACTIVATION — Displayed for On Premises installations only.			
Status:		States the current license status.	
Type:		States the type of installation.	
Expires:		Displays the license expiry date.	
LICENSES		The active Licenses in the domain.	
LICENSES > Onsight Users			
Connect Enterprise		# of domain user licenses	
Workspace Enterprise		# of Workspace user licenses	
Workspace Contributor		# of Workspace Contributor user licenses	
User Expiry		Support for user account expiry dates.	
External Guest Users		Enables External Guest Users	
Advanced External Guest Expiry			
License Group		Allows groups to be assigned license pools, each group manages their own pool of licenses.	
LICENSES > Client Functionality			
User Mode (Expert/Field)		Allows Expert and Field modes for users.	

Table 15-1 Account — Best Practices (continued)

Settings		Description	Best Practices/Tips
Team Link		When Enabled, Onsight Platform Manager will determine whether the Firewall allows direct SIP registration or whether it must use HTTPS to proxy SIP messages via the TeamLink Servers.	
Multiparty Calling		Allows Windows PC Conference Hosting.	
Bandwidth Control		Allows Bandwidth Control for Client Policy.	
Content Privacy		Allows privacy control over recordings and images.	
Onsight 5000HD Updates		Allows 5000HD software updates.	
Onsight Collaboration Hub Updates		Allows Onsight Collaboration Hub software updates.	
Cube Updates		Allows Onsight Cube software updates.	
LICENSES > Hosted Features			
Call Statistics		Enables Call Statistic data collection.	
Advanced Reporting		Enables Advanced Reporting of Call Stats.	
Customization		Enables message customization.	
SMS		Enables SMS external guest invitations.	
Client Permissions		Enables Client Permission control.	
Custom Media Configurations		Enables Custom Media Configuration for Client Policy.	
SSO		Enables SSO support.	
Custom Email (SMTP)		Enables emails to be sent from the customers mail server.	
Custom Messages		Enables custom messages to be used.	
LICENSES > Common Actions			
Change Account Owner		Enables you to assign an Account Owner from a list of current users.	
Disable Super Admin Access		This disables Librestream's ability to access the domain for support purposes. Access may be granted by your OPM Admin if necessary.	

Related information

Account *(on page 48)*

15.2.2. Users — Best Practices

Table 15-2 Users — Best Practices

USER ACCOUNTS	Value	Default	Description	Best Practices/Tips
Default Time Zone:	(UTC) Coordinated Time		Set the default Time Zone for your Region.	If operating across multiple regions set the time zone where the Administrator resides.
Default Language:	Chinese, English, German, Italian, Japanese, Korean, Portuguese, Portuguese (Brazil), Russian, Spanish, and Swedish	English		
EXTERNAL GUEST USERS				
External Guest Settings moved to Client Policy	Moved to Client Policy [LINK]			
GLOBAL DIRECTORY				
Global Directory Availability	☑ **External Contacts are public by default** (External Contacts that do not belong to any Contact lists will be available to everyone in the Global Directory)	default enabled	When checked all contacts that are not in a defined list will be visible in the Global directory, if not checked only contacts that belong in a contact list will be visible in the global directory.	This allows you to have contacts that are not visible to everyone but can be manually added to users contact lists by the administrator. Leave this unchecked if you want contacts not on a list not to show up in the Global directory.
CUSTOM FIELDS		Optional		Custom fields are included in an exported user report.
Custom Field Name		Department, Region	Enter a name	You can create custom fields that can be used as report filters.
Custom Field Value		Null	Enter a value or list of values	Create a value or list of values that can be used in reporting.

Related information

Users *(on page 53)*

15.2.3. Security — Best Practices

Table 15-3 Security — Best Practices

Settings	Value	Description	Best Practices/Tips
		PASSWORD POLICY	
Minimum Length:	8	Set the minimum length of allowed passwords.	Follow your enterprise's security policy.
Minimum Capital Letters:	1	Set the minimum number of Capital Letters required.	
Minimum Non-Alpha Characters:	1	Set the minimum number of Non-Alpha characters required.	
		PASSWORD EXPIRATION	
Password Expiration:	☐ **Enable password expiration**	default disabled	Follow your enterprise's security policy.
Password Expires:	60 days		
Warn Users Before Expiration:	3 days		
		LOGIN POLICY	
Maximum Bad Login Attempts:	3	default 3	Follow your enterprise's security policy.
Account Lockout Duration:	5 minutes	default 5 mins	
SELF REGISTRATION	default disabled	Self Registration settings apply to accounts created using the Self Registration Page and accounts provisioned automatically through Single Sign On	
Enable Self Registration	default enabled ☑ **Enable self registration page**	Enable the Self Registration page	Self Registration can make preparation for training sessions and deployment easier, having a list of all the users in advance is not necessary. You would typically just email the self-registration instructions.
URL:	https://onsight.librestream.com/OamDevl/AccountServices/Register.aspx?id=librestream.com	id=domain, identifies the Customer domain to which the user is self-registering. In the example provided the domain = librestream.com	Distribute the URL to associates who will need to register for an Onsight Account.
Key:	xxxxxxxxxxxxxxxxxxxx: default disabled	When populated with a value, the user must enter this key to self register for an Onsight account.	Set a key to ensure users are authorized to request an account. Use Generate Random Key to enter a value.
Licenses:	☐ default disabled	If Self Registration is enabled you can specify the license type	

Table 15-3 Security — Best Practices (continued)

Settings	Value	Description	Best Practices/Tips
Account Activation Method:	default enabled ☑ **Administrator must approve accounts registered using the Self Registration key**	When enabled all account requests must be approved by an Administrator before they are assigned.	It's recommended to enable this option, however, if a significant number of users are self-registering and you don't want to approve each account request, leave it unchecked. It is recommended that you use the **Self Registration Key** and set the **Allowed Email domains** as an added precaution.
Notification:	default enabled ☑ **Notify Administrators by email when an account is registered**	OPM Admins will receive emails whenever a user registers.	
Email	default enabled ☑ **Require Email Address for Self Registered Accounts**	Email addresses are required for User Notifications.	**Require Email Addresses**... should be enabled so that User Notifications are received. It is mandatory if you want the **Forgot Password** feature available for all users. Typically, the only time you would not require passwords for users accounts is when your Security Policy does not allow email addresses to be stored offsite.
Allowed Email Domains:	company.com	The list of allowed email domains from which a user can register.	Set this to your company's domain and any other third Party partner's domain to restrict access.

Related information
Security *(on page 55)*

15.2.4. Software — Best Practices

Table 15-4 Software — Best Practices

SOFTWARE UPDATES	Default	Description	Best Practices/Tips
Onsight Connect for Windows	**Latest Published Version**	Set the version of software you would like Windows PC users and External Guest Users to install.	You may choose 'Latest...' or a specific version. The standard install will be applied if users do not have admins rights.
Onsight 5000HD	**Latest Published Version**	Set the version of software you would like Onsight 5000HD devices to install.	

Related information
Software Updates *(on page 72)*

15.2.5. Client Policy — Best Practices

Table 15-5 Client Policy — Best Practices

Settings	Value	Description	Best Practices/Tips
General			
User Mode	**Expert**	Sets the mode the user operates in when logged in on an Onsight device.	Most users will be Expert. You may consider using Field mode for External Guests or Field Service personnel.
Prompt for Permissions	As Required*	Smartphone users must grant permissions to access resources such as data usage and images.	
Allow GPS in Video and Images	☐ Disabled*	GPS meta data will be embedded in recordings and images	
Screen Sharing	☑ Enabled*	Enables Screen Sharing between participants.	
Show GPS Overlay	☐ Disabled*		
Show Date/Time Overlay	☐ Disabled*		
Copy Captured Image to Gallery/Camera Roll	☐ Disabled*	If enabled, copies of photos/videos will be placed in the Gallery/Camera Roll	
Text Location of Overlay	Bottom Left*		
Text Size of Overlay	Small*		
Image Capture Resolution	Low*	Sets the maximum image resolution at which images will be captured locally. This setting will also determine the Highest Resolution image that can be shared in a call for Onsight Images. Gallery/Camera Roll images will be shared at the native resolution at which they were captured. Resolutions are defined based on image height in pixels: low (768), med (1080), high (1440) and max (depends on the max resolution of the device's camera).	When an image is shared during a call it will be shared initially using the default low resolution of 1024x768. If the image was captured at a higher resolution locally, the higher resolution image is made available during an Image sharing session by allowing a user to request the Higher Res image by pressing the High-res button in the Viewfinder. **Note:** Gallery/Camera Roll Images are shared at their native resolution when the High-res button is pushed.

* All default values are marked with an asterisk.

Table 15-5 Client Policy — Best Practices (continued)

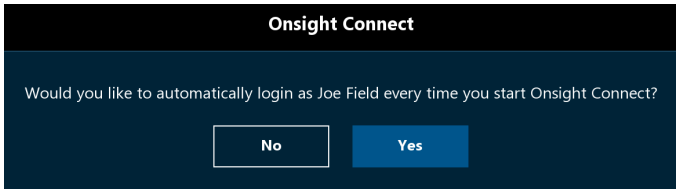
Settings	Value	Description	Best Practices/Tips
Copy captured images to Gallery/ Camera Roll	off*	Copies all captured images to the User's Gallery/Camera Roll	
Wait for Refresh on Lost Video Frame	☐ Disabled*	When enabled, this setting enhances the video quality by including adjustments to Maximum Transmission Unit (MTU) that optimizes the delivery of media packets in challenging environments. This capability enables you to display the last best picture until full frame video packets are received.	This capability is ideal in situations where picture quality is more important than motion. **Note:** This setting requires that Onsight Connect Users download and install the latest Onsight Connect software and that they enable the Wait for refresh on packet loss setting. Within Onsight Connect, click SETTINGS > CALLS > Video and enable the Wait for refresh on packet loss option.
Media Path	{ApplicationData}	Sets the default path for Onsight Media storage on the user's Windows PC.	The Media Path storage must be fast enough to accept real time file write speeds in order to keep up with saving video streams as recordings. The inability to keep up with the write speed will cause frames to be dropped in the recording and could cause file corruption. Network delays may impact recording quality.
Login			
Prompt to Remember Credentials (Auto Login)	☐ Disabled*	When enabled, **Prompt to Remember Credentials (Auto Login)** allows all users to enter their login credentials for auto login when the app launches. The prompt message below will show up when the user attempts to login for the first time.	Not recommended for users who share devices.
			
Run at Windows startup	☐ Disabled*		

Table 15-5 Client Policy — Best Practices (continued)

Settings	Value	Description	Best Practices/Tips
SIP			
SIP messaging	TCP*	The default transport for the SIP protocol.	
Support SIP UPDATE method	☑ Enabled*	A SIP compatibility feature used by some SIP Servers to update session parameters.	
Verify SIP TLS Server	☑ Enabled*	Determines whether SIP Servers must have their Certificates verified as authentic before allowing calls. This means the endpoint must have the Public certificate of the signing Certificate Authority (CA) which issued the SIP Server certificate.	Enabling may block some calls if the third Party SIP server is using self-signed certificates. The self-signing public certificate of the CA must be installed for the verification to be successful and of course you must trust the self-signing CA.
Enable WebEx CMR Compatibility	☐ Disabled*	Required for compatibility with WebEx CMR.	When placing the Onsight Call to the CMR, it will appear as if a 'double call' is happening but the call will connect successfully. The double call is when the initial call is answered but disconnects immediately, Onsight will immediately call back to connect to WebEx with the supported call parameters.
Force Media Relay	☑ Enabled*	Forces all media through the Media Servers opposed to allowing peer to peer media routing when clients are on the same subnet.	This is enabled by default to prevent media traffic being blocked by networks that do not allow peer to peer network traffic. You can disable it if you are confident peer to peer traffic is allowed, if your clients are behind using 'Guest Networks' at third party locations, they may have their calls blocked if peer to peer is not allowed.
Media Configurations			
Custom Media Configurations	Manage Media Configurations	Create Custom Media Configurations and select them to distribute through Client Policy.	Custom Media configurations can be defined based on location or situation. For example, you know a group of Field Service workers always encounter poor cellular network conditions at a certain location. Define a Media configuration specific to that location and assign that configuration to the Field Service Group Client Policy.
Bandwidth Control			
Bandwidth Control	☐ Disabled*	When enabled it allows the Administrator to set the Maximum allowed Video bit rate for Media configurations on an endpoint.	

Table 15-5 Client Policy — Best Practices (continued)

Settings	Value	Description	Best Practices/Tips
Maximum Video Bit Rate (Kbps)	2500*	Sets the Maximum allowed Video Bit Rate. (8 — 6000)	
Default MTU Size (bytes)	1200	By default, the Maximum Transmission Unit (MTU) is defined as 1200 bytes. Customers can adjust these settings in challenging environments to improve video quality.	
Bandwidth Adaptive Streaming (BAS)	Cellular Networks*	Enables BAS (Bandwidth Adaptive Streaming) for Smartphone users. BAS will dynamically drop frames to maintain a connection over low bandwidth networks giving preference to Audio packets.	BAS is recommended to ensure call connectivity in unreliable networks such as Cellular networks. Audio is given priority in a call to maintain communication during an Onsight call. Users may adjust the media configuration to lower resolutions and share high resolution still images under low bandwidth conditions.
Media configuration on connection	Null	Set the default Media configuration used when connecting calls.	This should be set to a lower bandwidth media configuration since calls can be happening over unknown network conditions. Higher resolution/bandwidth Media configurations can be selected during the call. Users typically would run a Bandwidth test to determine the maximum Bandwidth available during the call.
Pause Video While Transferring Image	☑ Enabled*	This setting pauses video while an image transfer is occurring. The endpoint that is the active video source will dictate whether the video is paused based on this setting.	
Preferred Voice Codec	Default*	Determines the Audio bandwdith used for Voice audio in a call.	The Opus Audio Codec will use 24Kbps as the target bit rate when set to default, it will use 10 Kbps when set to 'Low bit rate'. This does not include the packet overhead associated with audio packets.
Preferred Subject Audio Codec	Default*	Determines the Audio bandwidth for Video-associated Audio also known as Subject Audio. Most users will not require Subject Audio to be enabled.	The Opus Audio Codec will use 24Kbps as the target bit rate when set to default, it will use 10 Kbps when set to 'Low bit rate'. This does not include the packet overhead associated with audio packets. Subject Audio should be used when Audio isolation is required as part of troubleshooting. E.g., Engine noise. Typically, an external microphone is used with either an Onsight Collaboration Hub or with the 5000HD multi-port adapter.

Table 15-5 Client Policy — Best Practices (continued)

Settings	Value	Description	Best Practices/Tips
Audio Efficiency	Lower Latency*	Used to determine how Voice Audio packets are delivered in a call. Lower Latency will send Audio packets as they are generated. Lower Bandwidth will group Audio packets to reduce the associated network overhead of sending packets individually.	For High Bandwidth Networks: >1Mbps choose LOWER LATENCY For Medium Bandwidth Networks: 500Kbps — 1Mbps choose MID LATENCY/BANDWIDTH For Low Bandwidth Networks: <500Kbps choose LOWER BANDWIDTH For Satellite Networks: <500Kbps with high latency choose HIGHER LATENCY
Calls			
Allow New Contacts	☑ Enabled*	Disabled by default, this setting allows customers to add contacts outside of their organization using a SIP address. When enabled, users can only access their organization's Global directory and the Plus sign is missing from the Contacts window.	Use the default setting unless the customer has privacy concerns and wants this capability enabled to restrict calls only to their Global directory and group members.
Allow Cellular/Mobile Data Usage	☐ Disabled*	Required for Smartphone users without Wi-Fi access.	Cellular Data users must have this enabled. E.g., Field Service users who do not have access to 802.11 wireless networks.
Prompt to Enable Cellular/Mobile Data Usage	Never*	Sets when you prompt the user for permission to use Cellular Data.	
Start remote / non-Onsight video on connection	☐ Disabled*	When calling non-onsight endpoints the video stream will start automatically.	This prevents confusion when calling third party video conference or meeting rooms. Users sometimes forget to start the video stream.
Fill / Fit video in viewfinder when streaming	Fill*	Fill — Fills the display horizontally. Top and bottom may be trimmed to fit. Fit — Fills the screen vertically. A black border may appear on the sides of the Viewer. Actual Size: displays video in its native resolution. Video may appear with a black border all around it.	
Maximum Number of Connections	4	Windows PC can act as a conference host and add multiple participants to a call. The PC hardware and network bandwidth available to the Windows PC can affect call quality.	
Auto Answer	☐ Disabled*	Enables the ability to auto answer an incoming call.	Useful for unattended endpoints such as Onsight Rugged Smart Cameras.
Auto answer delay (seconds)	5	Sets the delay before an incoming call is auto answered.	

Table 15-5 Client Policy — Best Practices (continued)

Settings	Value	Description	Best Practices/Tips
Push Notifications	☑ Enabled*	Determines whether Android clients use Push Notifications when the application is in the background or not running. iOS devices always use Push Notifications as per Apple policy.	Enabling Push Notifications allows Onsight Connect to be battery optimized by an Android device, if Push Notifications are disable, Onsight Connect must be ignored by battery optimization so that it can access the network while a device is in Standby or Doze mode.
Prompt to Ignore Battery Optimizations	**Whenever Push Notifications are disabled***	There are two options: Whenever Push Notifications are disabled. Only when user disables Push Notifications.	Ignoring Battery Optimizations allows an app to access the network when the device is in Standby or Doze mode. For Android devices: When a user disables Push Notifications this will trigger a pop-up, requesting the user to enable Ignore Battery Optimizations. This will take them to the external Android Battery Optimization settings where they must select Onsight to remove it from the list of battery optimized apps on the device. **Note:** If a user chooses not to enable Ignore Battery Optimizations, they will not receive notifications when the device is in Doze mode. And they will not be prompted to enable Ignore Battery Optimizations again unless they re-enable then re-disable Push Notifications.
Encryption Mode	Auto*	The default should be Auto, this ensures that all Onsight connections will have encryption enabled during the call. Auto also gives the flexibility of calling Video conference systems that do not have encryption set.	If calling systems that do not have encryption set is not desired, set Encryption to On. Any endpoints that do not support encryption would not be accepted as a valid connection.
Prompt to Share Images After Capture	☑ Enabled*	The user will be prompted to share after an image capture.	Enable for novice users and guests.
Allow recording video/audio and saving images for ALL participants (Privacy Mode)	☑ Enabled*	Disables recordings and snapshots for all participants in a call.	May be used for External Guests or specific Groups based on privacy requirements.
Local Privacy Mode	Allow recordings and saving snapshots*	Allows flexibility in what media can be stored by users.	May be used for External Guests or specific Groups based on privacy requirements.

Table 15-5 Client Policy — Best Practices (continued)

Settings	Value	Description	Best Practices/Tips
Software Acoustic Echo Cancellation (AEC)	Default	Default On or Off	TBD
Software Acoustic Echo (AEC)	TBD	Default On or Off	TBD
Noise Suppression	☑ Enabled	Default On or Off	
Save Call Transcript	☐ Disabled*	Default Enabled	Enables all calls to be transcribed in the (Default) language.
Allow Meeting Scheduling	☐ Disabled*	Default On or Off	Enable this option to allow the user to send Outlook meeting invitations for Onsight calls.
Allow Guests for Meetings	☐ Disabled*	Default On or Off	Enable this option to allow the user to forward a meeting invite to support guests.
Require consent for remote video sharing requests	☐ Disabled*	The default is disabled. When enabled, consent must be granted before starting a video stream with a participant.	May be used for External Guests or specific Groups based on privacy requirements. This setting gives customers greater control over video sharing during an Onsight call. Video privacy is enhanced at sensitive locations by requiring users to provide consent before sharing video.
External Guest Users			
Allow users to invite external guests	☑ default enabled	Enables users to send guest invites	
Allow text message guest invitations	☐ default enabled	Enables users to send guest invites by text.	
SMS Max Message to User Length	100	Maximum character length	
Guest users must change temporary password on initial login	☐ default disabled		
Send 'Invitation Sent' confirmation to host (includes copy of invite)	☑ default enabled	Enables you to view a copy of the invitation	
Allow recording of images and video	☑ default enabled		
Allow global directory access	☑ default disabled	Not enabled for guest users	
Expiry	1	Day	
User can choose expiry time when inviting guests	☐ default disabled		

Table 15-5 Client Policy — Best Practices (continued)

Settings	Value	Description	Best Practices/Tips
Deactivate guest user account when removed from contact list	☐ default disabled	When enabled, and an inviter deletes a guest contact from the contact list and then selects Deactivate this user's guest account; If data anonymization is enabled, the guest user's personal data will be anonymized.	Enabling this setting will make licenses available once the guest account is no longer needed.
Include option for guest to call host immediately	☑ default enabled	When enabled, this setting enables the guest to call the inviter at their earliest convenience. It also provides for a link to Join Call on the form. When disabled, the Join call option is replaced with Login to Onsight Connect.	Leave this setting as enabled to make it easier for the guest to join the call.
From Email	Default	This determines whether the guest invite comes from the system email or the personal email of the inviter.	Setting this to the Inviter's Email Address can help identify emails as coming from a trusted source.
Custom Fields	Required	When set to required, the inviter must fill-out the custom fields when sending guest invites.	Leave this setting as required to provide more information when generating reports.
Allow Setting User Mode while inviting guest	☐ Disabled	When disabled, the user is unable to specify a User Mode when inviting a guest. When Enabled, the user is able to specify Expert (Experienced user) or Field Mode (User with limited experience).	Enable this setting when you want your users to have more flexibility in terms of assigning user modes to guests.
User Mode	**Expert**	Set the default user mode for guest invites.	Set the default user mode to best fit your use case.
Networking			
Diffserv DSCP (Voice)	Best Effort*	Best Effort: 0, Controlled Load: 24, Audio/ Video/Guaranteed: 40, Voice: 56	
Diffserv DSCP (Video)	Best Effort*		
Diffserv DSCP (Subject Audio)	Best Effort*		
Diffserv DSCP (Data Stream)	Best Effort*		
TeamLink			
Enable TeamLink	☑ Enabled*	When Enabled TeamLink will determine whether the Firewall allows direct SIP registration or whether it must use HTTPS to proxy SIP messages via the TeamLink Servers.	

Table 15-5 Client Policy — Best Practices (continued)

Settings	Value	Description	Best Practices/Tips
Allow HTTP registration	☐ Disabled*	Used for troubleshooting.	HTTPS is used by default and is the preferred transport for TeamLink, HTTP is only used if HTTPS is not available.
Do not allow direct SIP registration (Use for troubleshooting only)	☐ Disabled*	When Enabled, TeamLink will proxy all traffic over HTTPS.	This is only recommended for troubleshooting. Forcing TeamLink may cause it's use when not necessary.
Firewall Detect			
SIP Detection Method	SIP Server - Full*	Used to determine which servers are targeted by TeamLink for the Firewall Detect test. The Firewall detect test will determine the best method to use to get through the Firewall.	This setting should not be changed unless you have consulted with Librestream Support.
Workspace			
Access	☑ Enabled*	Authorizes access to Onsight Workspace for the members of the group.	Only enable Onsight Workspace when users need to upload, view, and edit files when using Onsight Connect.
Upload Path	~/onsight	Sets the top-level directory structure in the Workspace. All uploaded files will be placed under the upload path in a Call folder.	All members of the group will have their call folders placed under the Upload path. Use a different upload path for different groups.
Auto Upload Media	☐ Disabled*	When enabled any files captured during an onsight call will be automatically uploaded to the Workspace once the call has ended.	Users will not have control over which files get uploaded.
Maximum Upload Bit Rate (Kbps)	0*	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.	**Note:** The upload bitrate will be subject to any network limitations on bandwidth.

Table 15-5 Client Policy — Best Practices (continued)

Settings	Value	Description	Best Practices/Tips
Restrict Upload Folder Access to Owner	☐ Disabled*	By default, all Workspace users can view all folders. When enabled, users can only access the upload folders they own. Folder permissions in Workspace will need to be manually edited to reverse this setting.	File and Folder permissions can be edited by an Administrator by logging in to Onsight Workspace. Be cautious when enabling this setting, undoing the permissions to allow sharing can be tedious for multiple directories. **Note:** That even if all users have full access to all Workspace folders the original files are always protected from editing. Edits can only be performed on versioned copies of the original files.
Allow cellular/mobile data usage	☐ Disabled*	When enabled files will be uploaded using the cellular/mobile data if a wireless connection is not available. When disabled files will not be uploaded until a wireless network connection is available.	Priority will be given to uploading files over a wireless network. Cellular/Mobile data will only be used in the absence of a wireless network.
Display Transcription Summary	Disabled	When enabled, a transcription summary is visible within Onsight Workspace providing all required licenses and AI settings are correct.	Enabled.
Display Transcription Sentiment	Disabled	When enabled, sentiment analysis will display at the line level and for the complete transcript within Onsight Workspace providing all required licenses and AI settings are correct.	Enabled.
Artificial Intelligence			
AI Setting	None	Sets the default AI profile.	**Note:** Only one AI setting profile may be applied to a client policy. We recommend that you combine all AI settings within a single profile.

Table 15-5 Client Policy — Best Practices (continued)

Settings	Value	Description	Best Practices/Tips
CV Document Link URL	None	Sets the Computer Vision Document Link URL	Enter the URL within the **CV Document Link URL** field. This will enable you to manage all of your document links from one location. **Note:** Custom (Document) Links will not work if **Local Privacy Mode** is enabled for your domain, group or user account.
CV Document Link URL for OCR, barcodes, and QR codes	None	Sets the Computer Vision Document Link URL for barcodes.	Enter the URL within the **CV Document Link URL for OCR, barcodes, and QR codes** field. This will enable you to manage all of your document links for OCR, barcodes and QR codes from one location. **Tip:** You can use the {(Regex)} tag to simply the recognition of codes that begin with a series of characters. For example, use *"JF"* as an indication that the code is a Vehicle Identification Number (VIN).
Auto Tag Images	☐ Disabled*		
Transcription Language		Sets the default language for Transcriptions.	
Custom Messages			
Login		Sets the login custom message when a user logs in.	TBD
Recording		Sets a recording custom message that appears to all participants when a call starts recording.	TBD

15.2.6. Client Permissions — Best Practices

Table 15-6 Client Permissions — Best Practices

Settings	Action					Best Practices/Tips
	Domain Defaults	Client Administrators	Standard Users	External Guest Users	Domain License Group	
General						
Enable GPS in Video and Images	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Do not use Inherit as the Action for the External Guest Users group without considering the access the Guest will have to the configuration setting. For example, if you have set Local Privacy mode to Disable recordings and saving snapshots for the External Guest Users group, but have granted permissions to edit the setting, then you have effectively allowed the guest user to have access to saving recordings and snapshots, if they edit the setting locally on the endpoint.
Show GPS Overlay	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Show Date/Time Overlay	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Text Location of Overlay	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Text Size of Overlay	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Image Capture Resolution	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Enables the user to define the image capture resolution.
Encoder Hardware Acceleration	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Applies to Windows PC's only.
Media Path	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Copy Captured Image to Gallery / Camera Roll	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Allow Illumination	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Applies to any client that supports illumination.
Allow Flash	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Applies to any client that supports Flash.
Allow Laser	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Applies to Cube only.
Login						
Auto Login	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Not recommended for users who share a device.
Run at Windows startup	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
SIP						
SIP messaging	Allow*	Allow*	Inherit*	Inherit*	Inherit*	

* All default values are marked with an asterisk.

Table 15-6 Client Permissions — Best Practices (continued)

Settings	Action					Best Practices/Tips
	Domain Defaults	Client Administrators	Standard Users	External Guest Users	Domain License Group	
Support SIP UPDATE method	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
Verify SIP TLS Server	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
Enable WebEx CMR Compatibility	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
Force Media Relay	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
IP Calls	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Media Configurations						
Low Profile	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Medium Profile	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
High Profile	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
HD (720p) Profile	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Full HD (1080p) Profile	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Custom Profiles	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Bandwidth Control						
Enable Bandwidth Control	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Maximum Video Bit Rate	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Enable BAS	Allow*	Allow*	Inherit*	Inherit*	Inherit*	You may want to give users the ability to edit BAS, as it may not be required on uncongested cellular networks. BAS may restrict frame rate unnecessarily if the network experiences a temporary drop in Bandwidth.
Media MTU	Deny*	Allow*	Inherit*	Inherit*	Inherit*	An average user should never need to adjust MTU. IT personnel may find this useful when troubleshooting network issues.
Media configuration on connection	Allow*	Allow*	Inherit*	Inherit*	Inherit*	This should be set to a lower bandwidth media configuration since calls can be happening over unknown network conditions. Higher resolution/bandwidth Media configurations can be selected during the call. Users typically would run a Bandwidth test to determine the maximum Bandwidth available during the call.
Pause Video while transferring image	Allow*	Allow*	Inherit*	Inherit*	Inherit*	On poor networks streaming video while transferring an image may affect call quality, you may want to allow users to be able to set 'Pause video while transferring'.

Table 15-6 Client Permissions — Best Practices (continued)

Settings	Action					Best Practices/Tips
	Domain Defaults	Client Administrators	Standard Users	External Guest Users	Domain License Group	
Preferred Voice Codec	Allow*	Allow*	Inherit*	Inherit*	Inherit*	G.7.11 can be used when network bandwidth is good (>300Kbps), GSM should be used in low bandwidth conditions. In poor network conditions it may be an advantage to switch to the lower Bandwidth codec (GSM). However, it is best practice to control Audio codecs through Client Policy.
Preferred Subject Audio Codec	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Subject Audio should be used when Audio isolation is required as part of troubleshooting. E.g., Engine noise. Typically, an external microphone is used with either an Onsight Collaboration Hub or with the 5000HD multi-port adapter. If a user needs Subject Audio occasionally this should be set to 'Allow'.
Audio Efficiency	Allow*	Allow*	Inherit*	Inherit*	Inherit*	This setting may be useful for users who are streaming over BGAN satellite. However, BGAN users should have Audio Efficiency set to 'Lower Bandwidth' through Client Policy.
Calls						
Allow Cellular/Mobile Data Usage	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Start remote / non-Onsight video on connection	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Maximum Number of Connections	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
Enable auto answer	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Required for compatibility with some third Party video conference systems.
Auto answer delay (seconds)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Push Notifications	Allow*	Allow*	Inherit*	Inherit*	Inherit*	For Android clients only.
Encryption Mode	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Prompt to Share Images After Capture	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Disable recordings and saving snapshots for all participants	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Local Privacy Mode	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
Require consent for remote video sharing requests	Deny*	Allow*	Inherit*	Inherit*	Inherit*	

Table 15-6 Client Permissions — Best Practices (continued)

Settings	Action					Best Practices/Tips
	Domain Defaults	Client Administrators	Standard Users	External Guest Users	Domain License Group	
Networking						
Diffserv DSCP (QoS)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
TeamLink						
Enable/Disable TeamLink	Allow	Allow	Inherit*	Inherit*	Inherit* *	
Change TeamLink Settings	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
Firewall Detect						
SIP Detection Method	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Workspace						
Maximum Upload Bit Rate (Kbps)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Allowing users to edit the upload bit rate may be useful for large file uploads.
Allow cellular/mobile data usage	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Allowing users to edit the cellular/mobile data usage may impact data plans.
Software Updates						
Install Software Updates	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Allows users to install Software updates from OPM (PC, Cube, 5000HD, Hub).
Update Server	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Allows a user to enter a SW update URL on a local network that points to an Onsight Update package.
Check for updates automatically	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Allows automatic SW update alerts when the user logs in to a client.

Related information

Client Policy & Permissions *(on page 73)*

Index

E

F

T

U