



Onsight Platform Manager Admin Guide

Copyright

Onsight Platform Manager Guide

Doc #: 400199-24 Rev: I

September 2022 (v11.4.13)

Information in this document is subject to change without notice. Reproduction in any manner whatsoever without the written permission of Librestream is strictly forbidden.

Copyright Notice:

Copyright 2004-2022 Librestream Technologies Incorporated. All Rights Reserved.

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

Copyright.....	ii
1. OVERVIEW.....	7
1.1. Onsight Augmented Reality Platform Architecture.....	7
2. NETWORK REQUIREMENTS.....	9
2.1. Firewall Configuration.....	9
2.2. On Premises.....	9
2.3. Login to OPM for the First-time.....	9
3. DASHBOARD.....	11
4. ADMINISTRATOR'S SETTINGS.....	13
4.1. Changing The Administrator's Password	13
4.2. Changing The Administrator's Personal Contacts.....	14
4.3. Adding Administrators To OPM.....	16
5. USER LICENSES.....	19
5.1. License Options.....	19
5.2. Capture Mode.....	20
6. MANAGE USERS & GROUPS.....	21
6.1. Domain License and Policy Management.....	21
6.2. License Group Management.....	21
6.3. License/Policy Groups & User Management.....	22
6.4. Adding a Group.....	23
7. USERS AND GROUPS.....	25
7.1. Create New User.....	25
7.1.1. Creating a New User.....	25
7.2. Welcome Email.....	27
7.2.1. On-Premises Welcome Email.....	27
7.2.2. On-premises-URL Formats.....	28
7.3. User Email Requirement.....	29
7.4. User Account Types and Permissions.....	30
7.5. Promoting Users and Assigning a Group Administrator.....	31
7.6. Edit Groups.....	33
7.6.1. Adding/Removing Group Members.....	33
7.6.2. Assigning Group Administrators.....	34
7.6.3. Edit Client Policy and Permissions.....	35
7.6.4. Global Directory.....	36
7.7. Import/Export Users.....	38
7.7.1. Creating a Users Import Template.....	38
7.7.2. Importing Users.....	39
7.8. Export Users.....	41
7.9. Self-Register Users.....	42
8. EXTERNAL CONTACTS.....	43
8.1. Manually Adding an External Contact to the Global Directory.....	43
8.2. Importing An External Contacts List.....	44
8.3. Adding an External Contacts List.....	45
8.4. Adding/Removing External Contacts from Lists.....	46

9. SETTINGS.....	49
9.1. Authentication Time-out.....	49
9.2. Account.....	50
9.2.1. Super Administrator Access.....	50
9.2.2. Change Account Owner.....	51
9.2.3. Licenses.....	51
9.2.4. Data Anonymization.....	54
9.2.5. Scheduled Anonymization.....	54
9.3. Users.....	55
9.3.1. User Accounts.....	55
9.3.2. External Guest Users.....	56
9.3.3. Global Directory.....	56
9.3.4. Custom Fields.....	57
9.4. Security.....	57
9.4.1. Password Policy.....	58
9.4.2. Password Expiration.....	59
9.4.3. Login Policy.....	59
9.4.4. Self Registration.....	59
9.5. Single Sign On.....	60
9.5.1. Single Sign ON.....	60
9.5.2. Security Assertion Markup Language Configuration.....	61
9.5.3. User Identity Federation.....	62
9.5.4. SSO Self Registration.....	65
9.5.5. User Provisioning Links.....	66
9.5.6. Notify Existing Users.....	67
9.5.7. On-premises — SSO Certificate Setup.....	68
9.6. Session Initiation Protocol	68
9.6.1. SIP Settings.....	68
9.6.2. SIP Account.....	69
9.7. Onsite Workspace.....	71
9.7.1. Enabling Workspace Access for Users.....	71
9.8. Workspace Webhooks.....	73
9.8.1. Creating & Modifying a Webhook Configuration.....	73
9.9. Software Updates.....	74
9.9.1. Onsite Connect for Windows.....	75
9.9.2. New Release Notifications.....	75
9.9.3. Updates for Onsite Cube, Collaboration Hub and 5000HD.....	75
9.9.4. On-premises Software Updates.....	75
9.10. Client Policy & Permissions.....	75
9.10.1. External Guest Users.....	76
9.10.2. External Guest Invitation Defaults.....	77
9.10.3. Policy Precedence.....	78
9.10.4. Group Client Policy and Permissions.....	80
9.10.5. Remote Video Privacy.....	81
9.10.6. WebEx CMR Compatibility.....	82
9.11. Short Message Service.....	82
9.12. Customization.....	83

9.13. Application Programming Interface Keys.....	83
9.13.1. API Generated Key.....	84
9.14. Artificial Intelligence Settings.....	84
10. STATISTICS AND EVENTS.....	87
10.1. Client Activity.....	87
10.1.1. Generating a Client Activity Report.....	87
10.2. Statistics.....	89
10.2.1. Generating a Statistics Report.....	89
10.3. Events.....	92
10.3.1. Generating an Events Report.....	92
10.4. Reports.....	94
10.4.1. Generating a Report.....	94
10.5. Heat Maps.....	96
10.5.1. Generating a Heat Map Report.....	96
11. LANGUAGE SUPPORT.....	99
12. CUSTOM MESSAGES.....	101
12.1. Creating a Custom Message (Form).....	101
12.2. Custom Messages & Client Policy.....	102
12.2.1. Modifying Client Policy to Support Custom Messages.....	102
13. END USER LICENSE AGREEMENT.....	103
14. CONTACT SUPPORT.....	105
APPENDICES.....	107
Client Policy & Priority Precedence.....	107
Best Practices.....	112
15.2.1. Account — Best Practices.....	112
15.2.2. Users — Best Practices.....	114
15.2.3. Security — Best Practices.....	115
15.2.4. Software — Best Practices.....	116
15.2.5. Client Policy — Best Practices.....	117
15.2.6. Client Permissions — Best Practices.....	127
Index.....	a

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

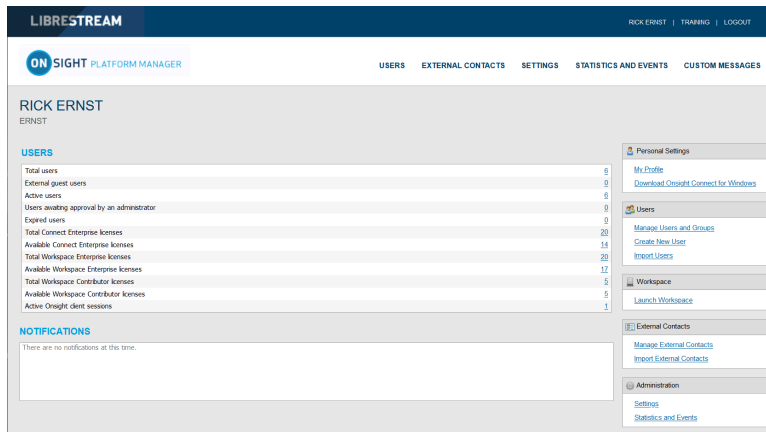


Figure 3-1 Dashboard

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

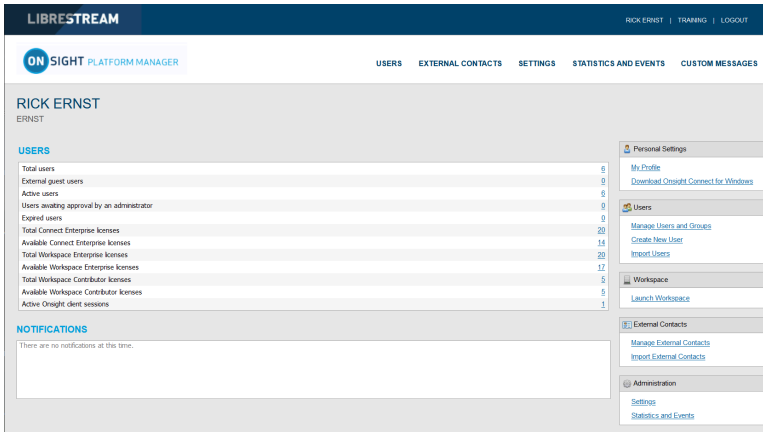



Figure 4-1 Dashboard

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.

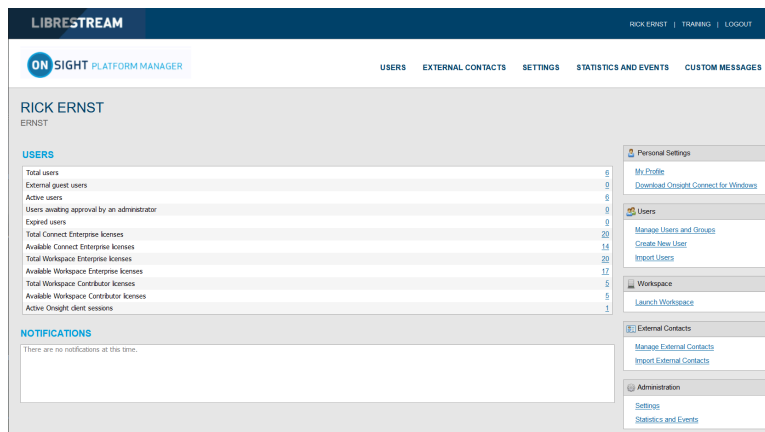


Figure 4-2 Dashboard

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

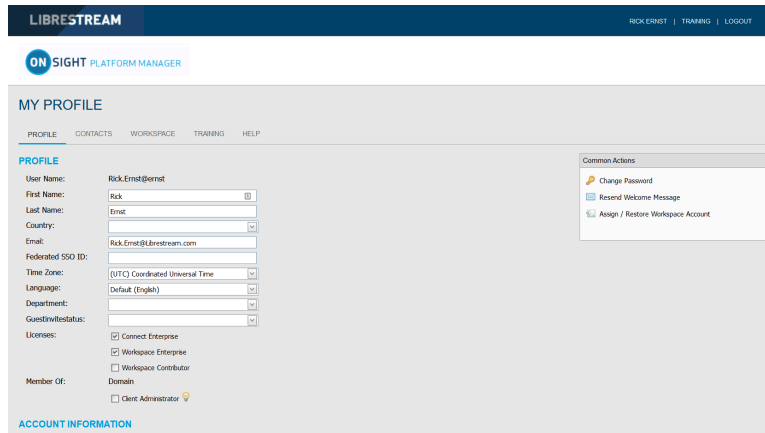



Figure 4-3 My Profile

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

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

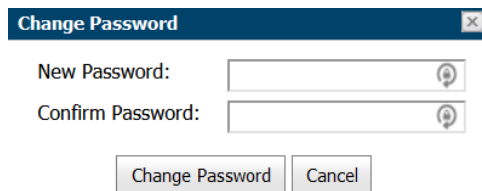


Figure 4-4 Change Password

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**.

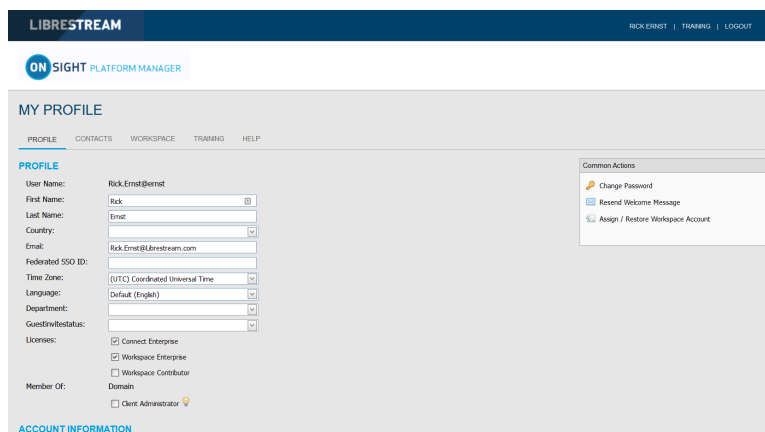


Figure 4-5 My Profile

2. Select the **CONTACTS** tab.

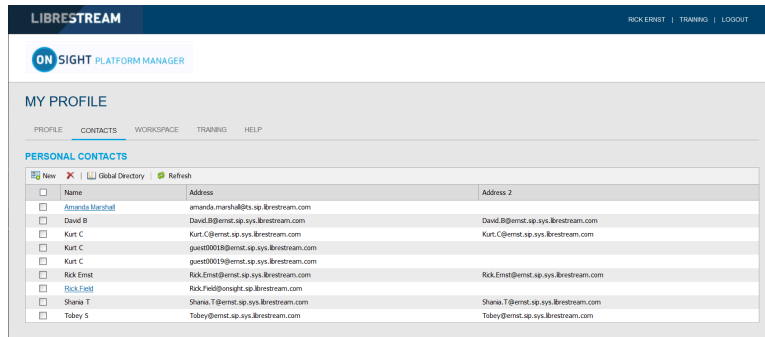



Figure 4-6 My Contacts

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

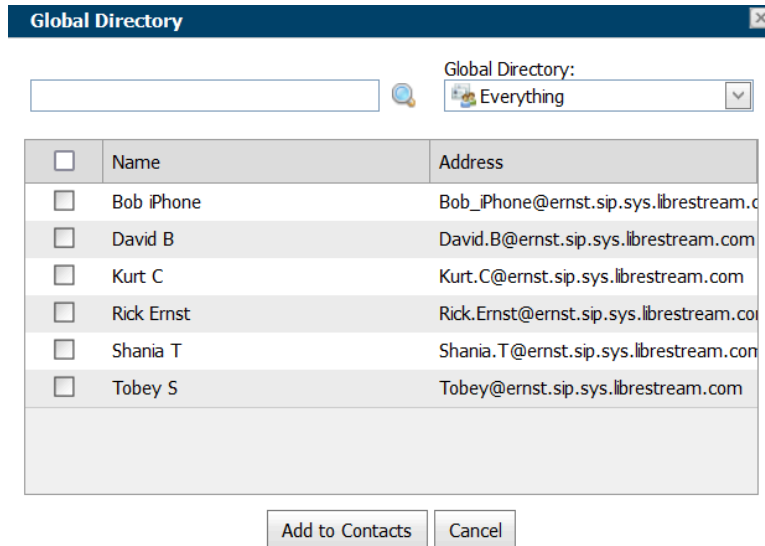




Figure 4-7 Global Directory

- Enter a name to search and press the  **Search** icon to see a list of all users.
- Enable the check box next to the person's name and click **Add to Contacts**.
- To manually create a contact, click the  **New Contact** icon. This is only necessary if you need to add a third-party contact.

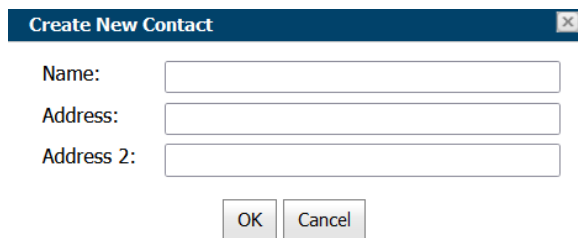


Figure 4-8 Create New Contact

- 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**.

- 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.

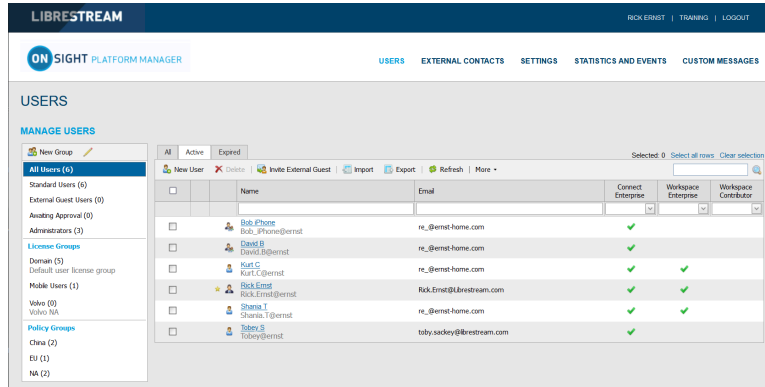


Figure 4-9 USERS

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

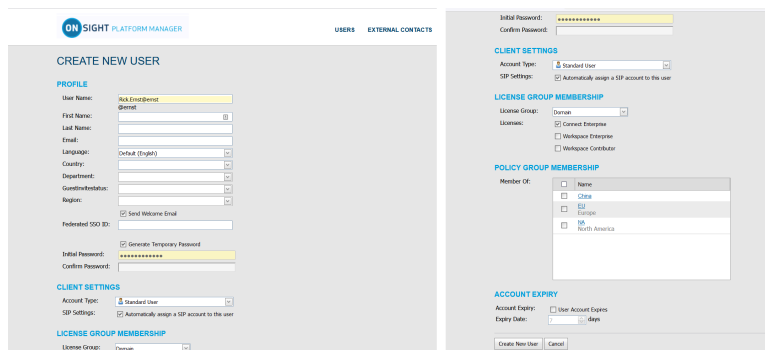


Figure 4-10 Create New User

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

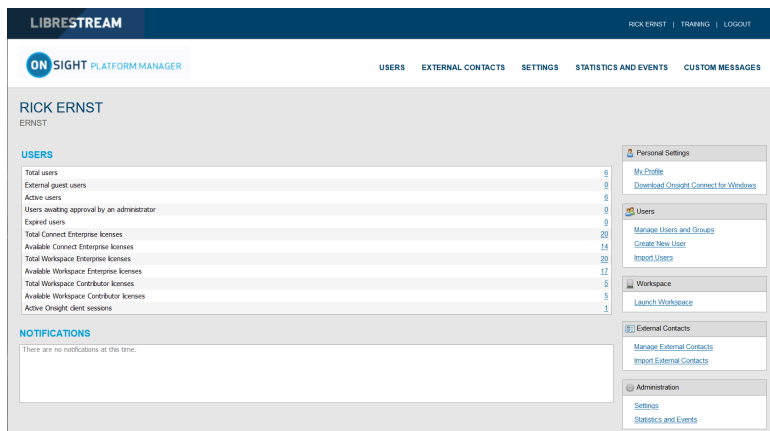



Figure 5-1 Dashboard

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

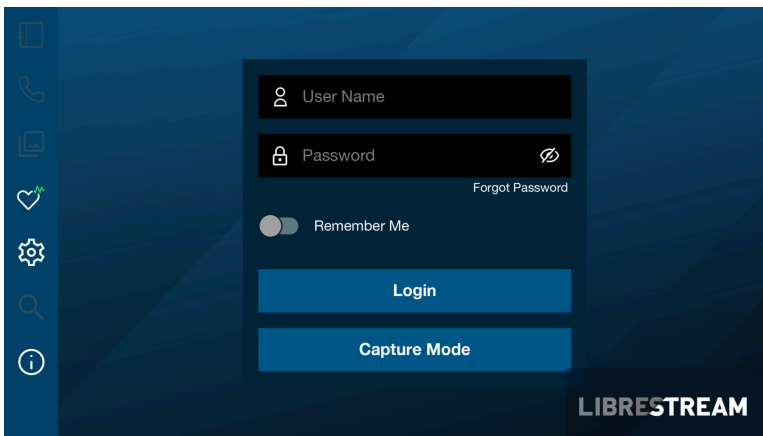


Figure 5-2 Capture Mode

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

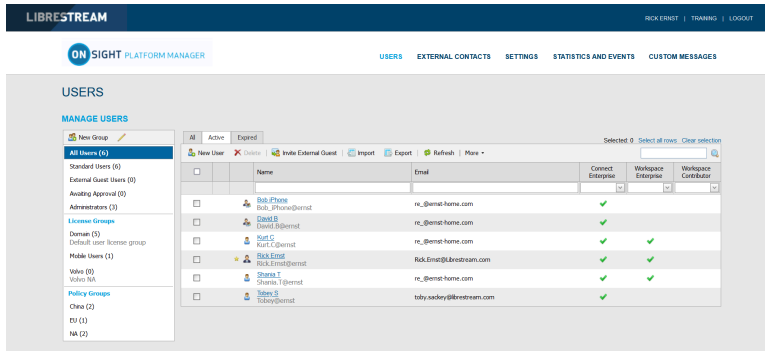


Figure 6-1 Manage User & Groups

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

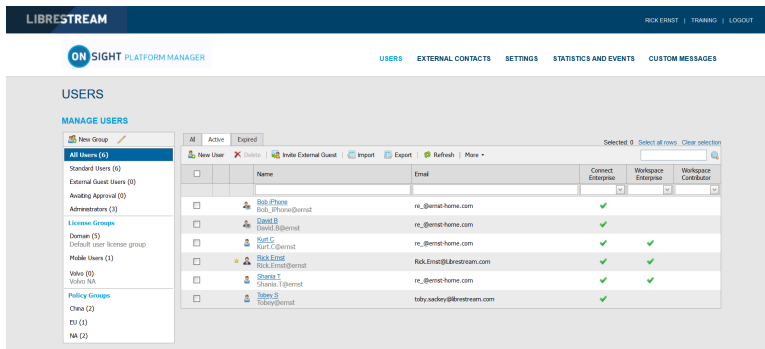


Figure 6-2 All Users/Domain License Group

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 reference

[Client Policy — Best Practices \(on page 117\)](#)

6.2. License Group Management

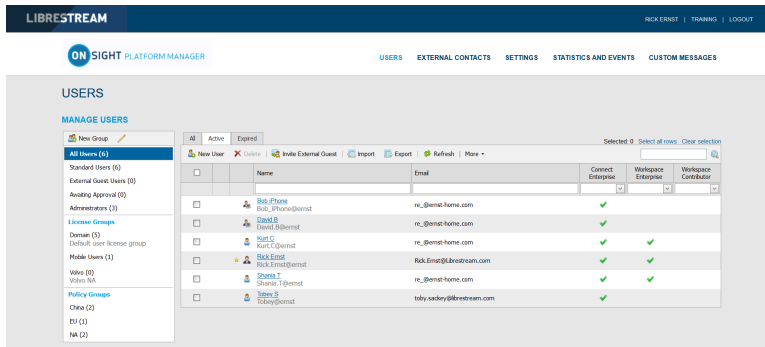


Figure 6-3 License Groups

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 reference

[Client Policy — Best Practices \(on page 117\)](#)

6.3. License/Policy Groups & User Management

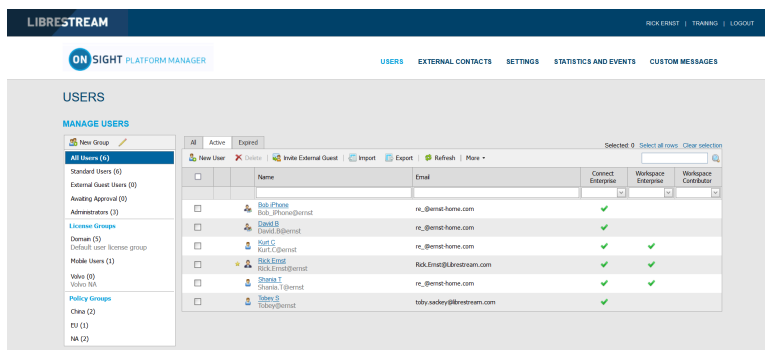


Figure 6-4 Policy and License Groups

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 there 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 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 reference

[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.

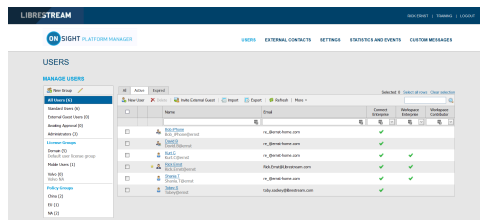


Figure 6-5 USERS

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 \(on page 75\)](#) section.

Related reference

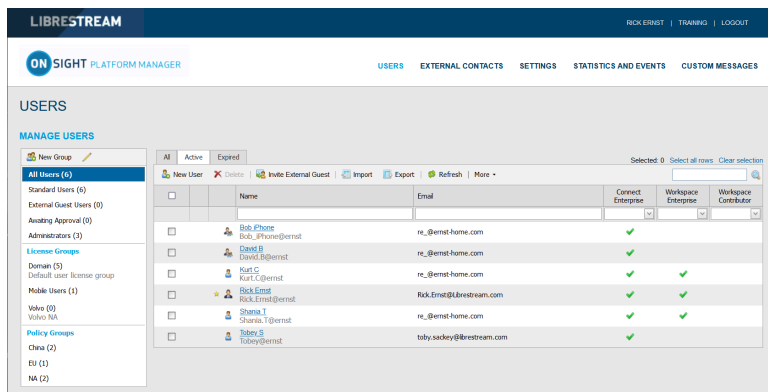
[Client Policy — Best Practices \(on page 117\)](#)

[Client Permissions — Best Practices \(on page 127\)](#)

Related information

[Client Policy & Permissions \(on page 75\)](#)

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

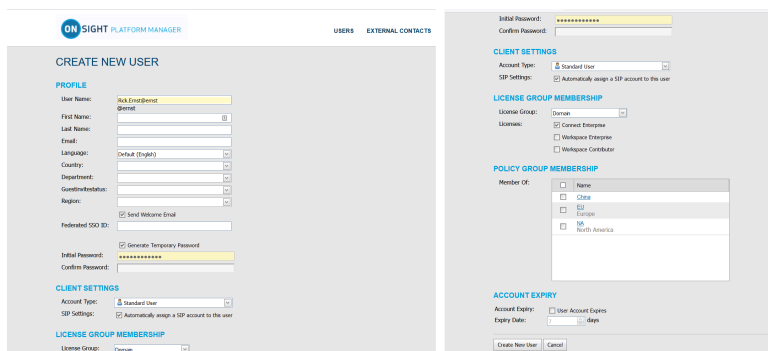



Figure 7-2 Create a New User

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.

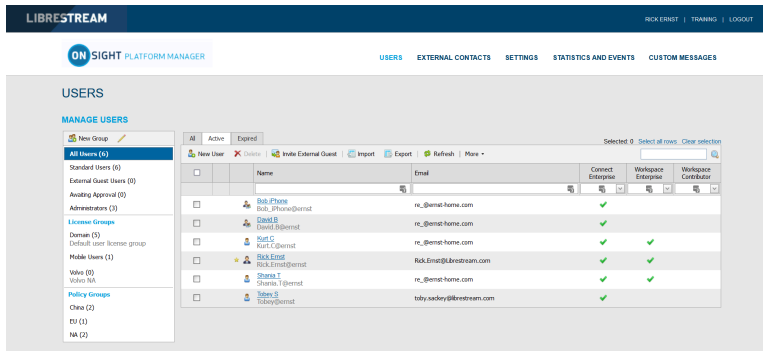


Figure 7-3 Users Page

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

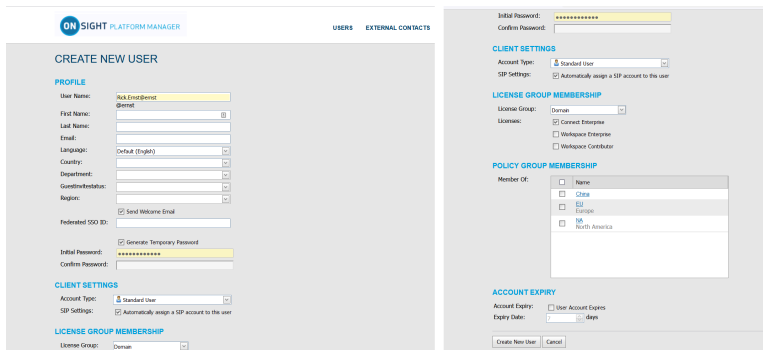





Figure 7-4 Creating a New User

 **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 license 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

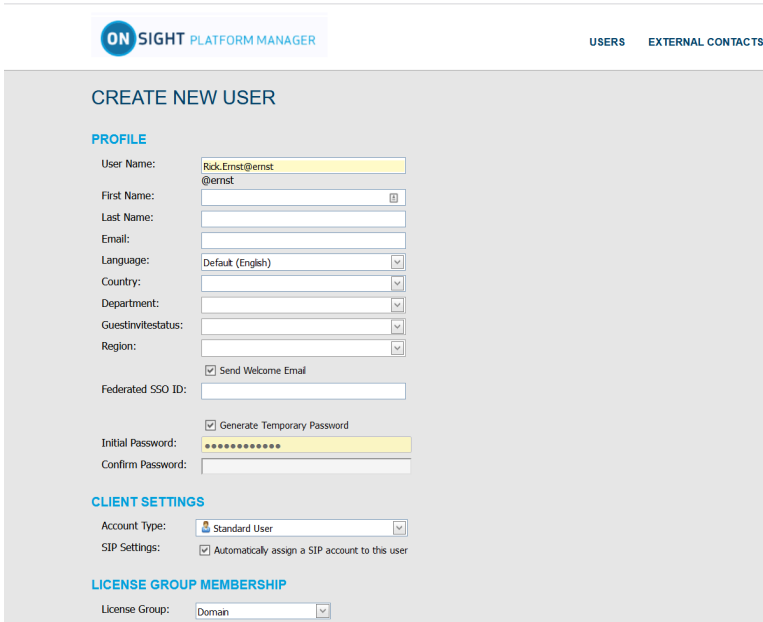


Figure 7-5 Welcome Email Option

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

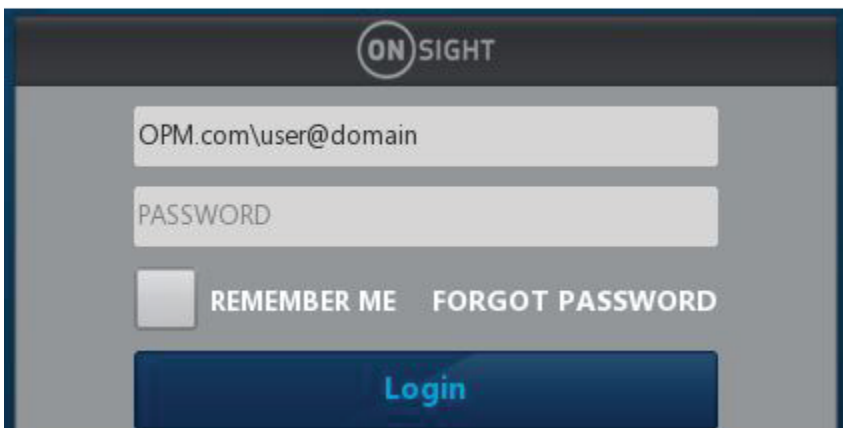


Figure 7-6 On-premises URL

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 Onsite 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

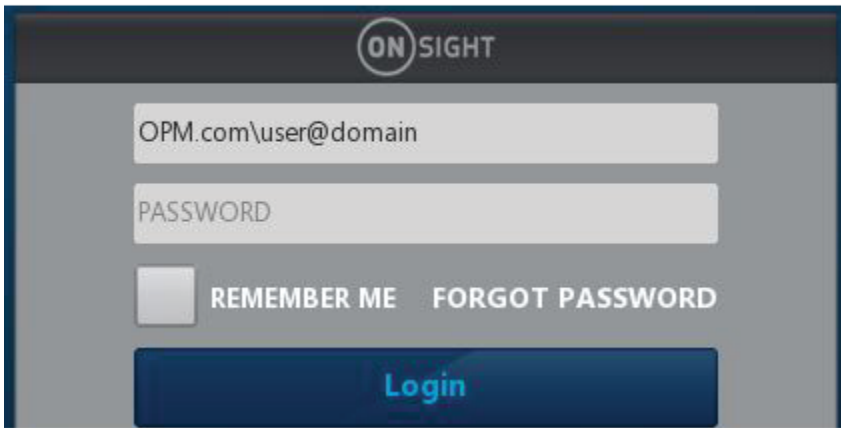


Figure 7-7 On-premises URL

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 Onsite Connect from your Onsite 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 Onsite Connect, they **MUST** click the **Login to Onsite Connect** button to correctly configure the software to log in to your OPM installation.

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

7.3. User Email Requirement

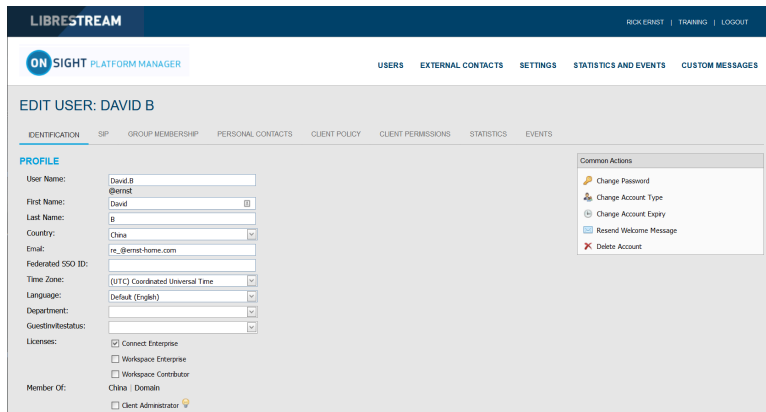


Figure 7-8 User Email Requirement

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

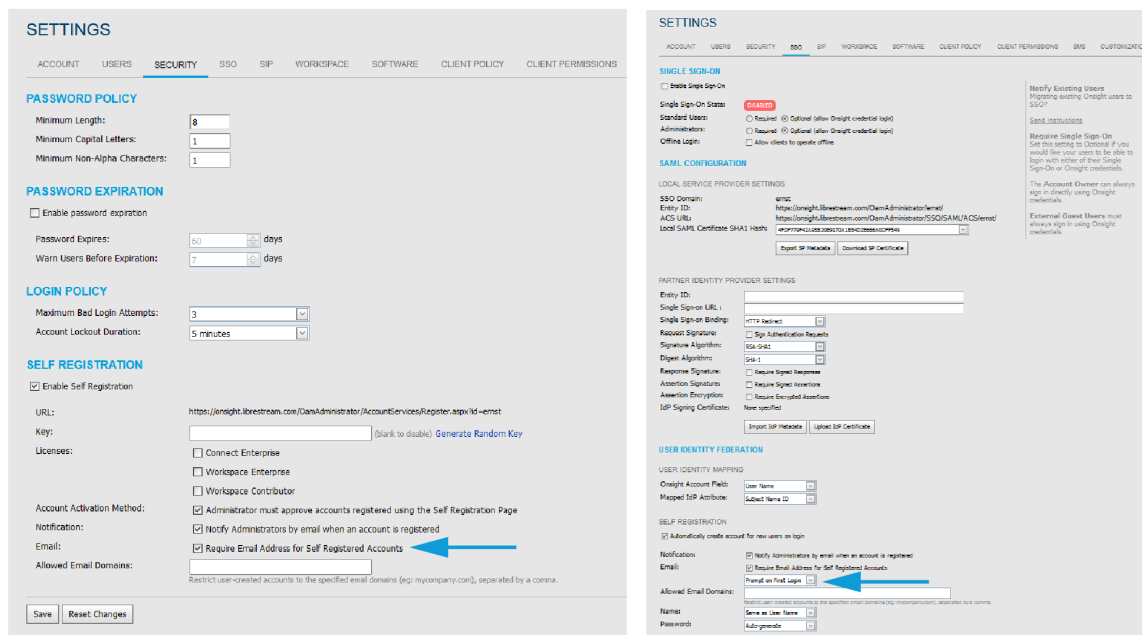


Figure 7-9 Security & SSO Settings

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

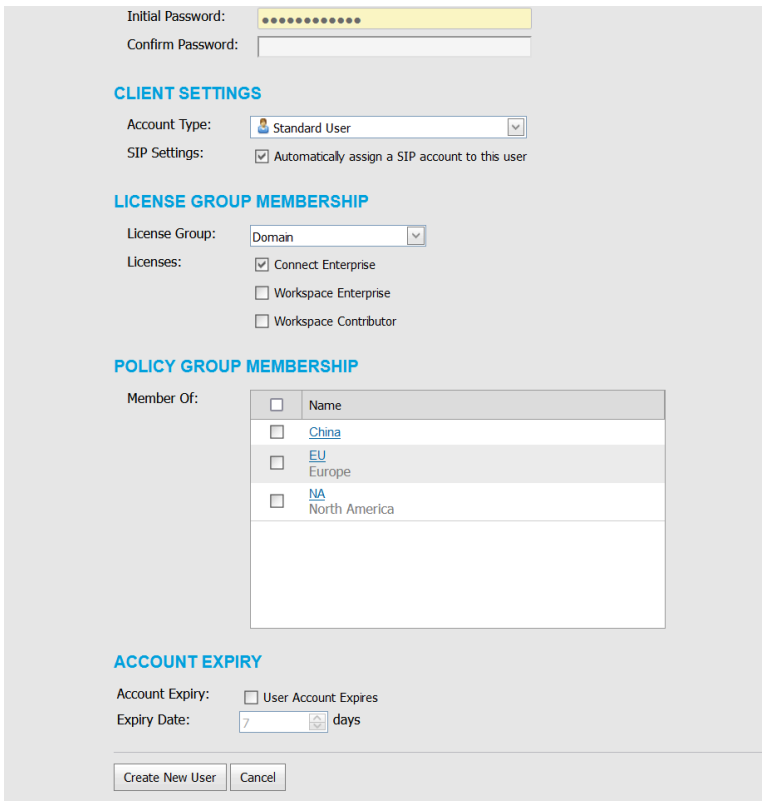



Figure 7-10 User Account Type

Within **CLIENT SETTINGS**, the **Account Type** drop-down menu indicates the level of access the User has to Onsite Platform Manager. The licenses assigned to the user determines the features the user has access to in Onsite 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.

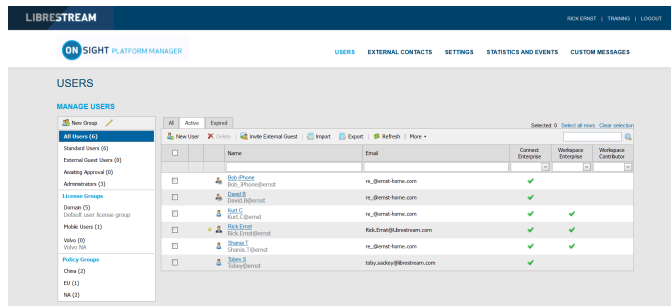


Figure 7-11 Users Page

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

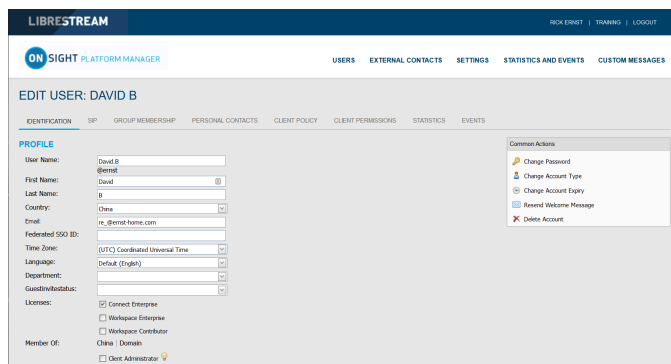


Figure 7-12 Edit User Page

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

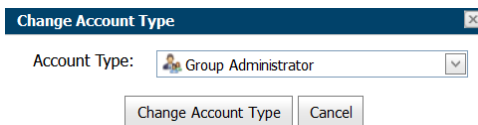


Figure 7-13 Change Account Type

- c. Click **OK**.

Assigning an Administrator to a Group

3. To assign a group administrator to a Group, you will need to:
 - a. Select **Users** from the main menu and select the group to assign a group administrator.

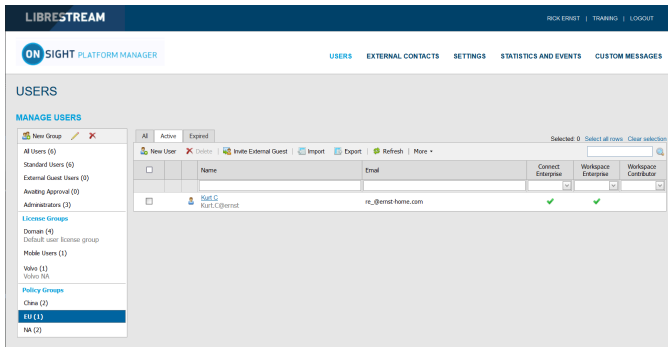


Figure 7-14 Selecting a Group

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

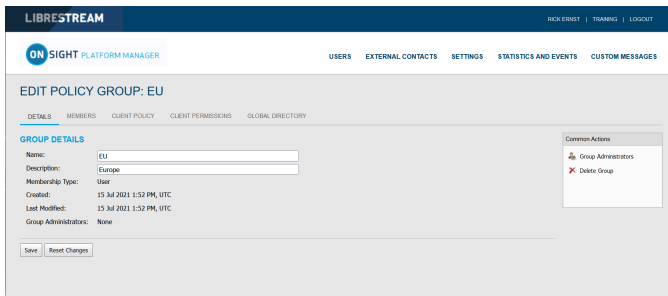


Figure 7-15 Edit Policy Group

- c. In the **Common Actions** section, click  **New Group**.

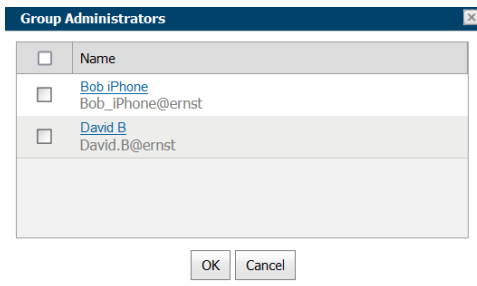


Figure 7-16 Group Administrators

- d. Enable the check box next to one or more **Group Administrator(s)** from the list; and click **OK**. The **Group Administrators** section updates accordingly.
 - e. Click **Save**.

7.6. Edit Groups

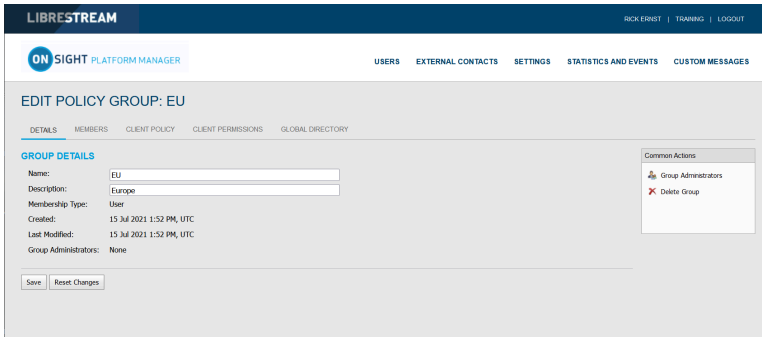


Figure 7-17 Edit a Group

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 reference

[Client Policy — Best Practices \(on page 117\)](#)

[Client Permissions — Best Practices \(on page 127\)](#)

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.

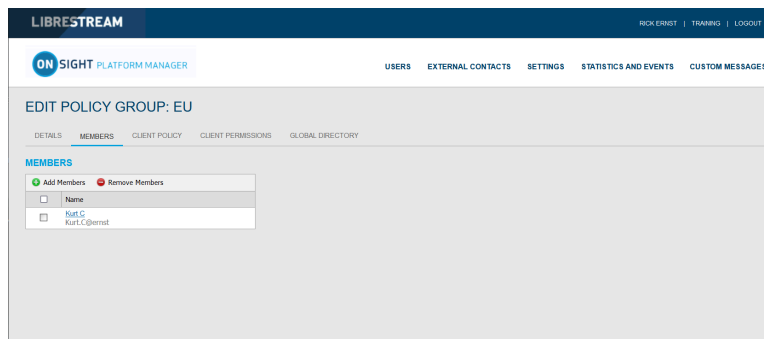


Figure 7-18 Edit Policy Group

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

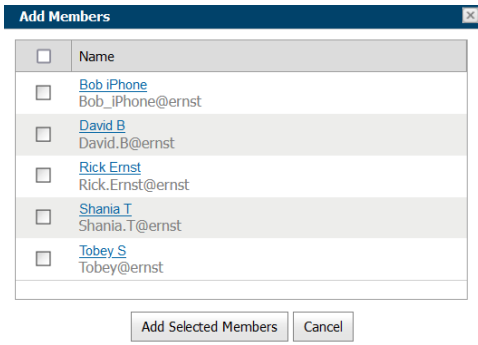




Figure 7-19 Add members

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 .

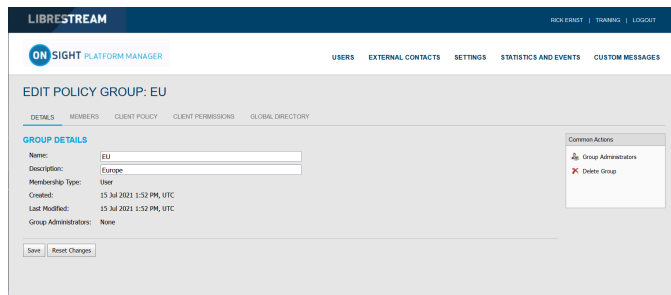


Figure 7-20 Group Details

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

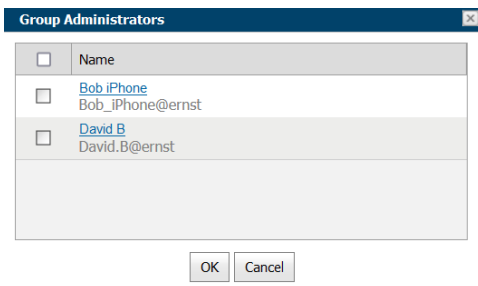



Figure 7-21 Group Administrators

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.

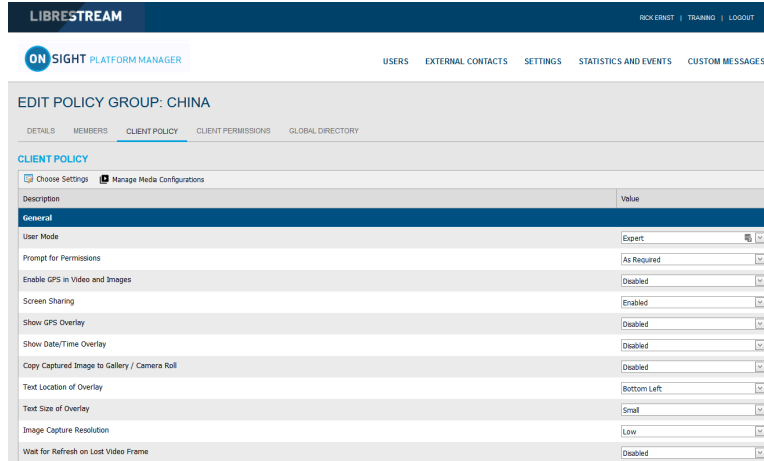



Figure 7-22 Edit Policy Group

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

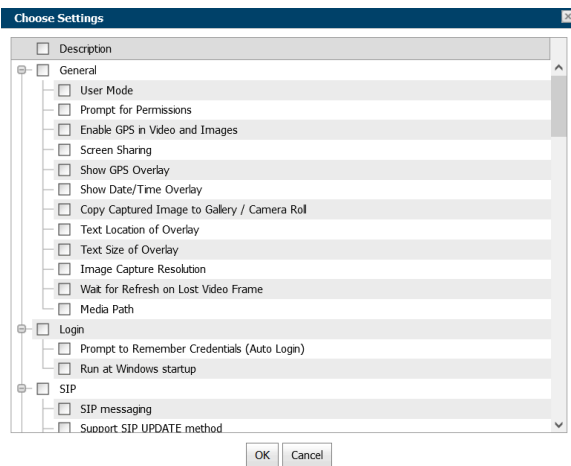


Figure 7-23 Choose Settings

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

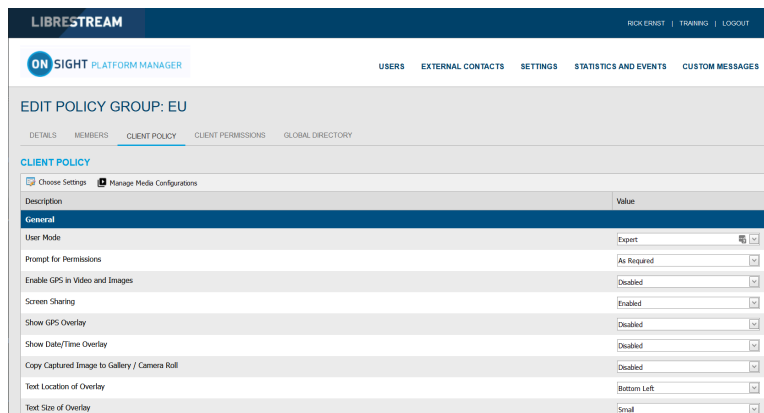
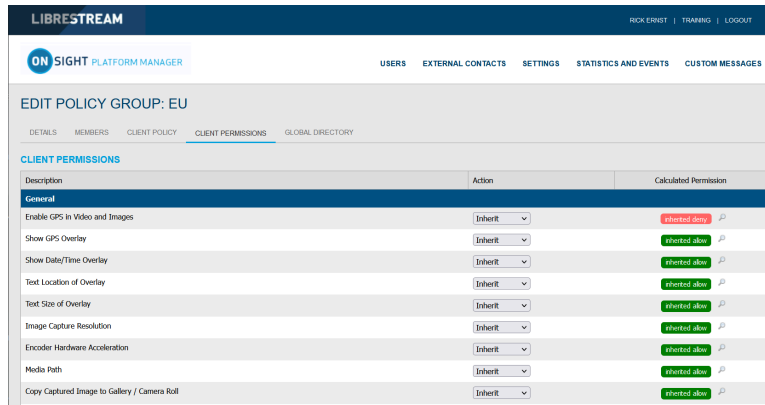


Figure 7-24 Client Policy

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



Description	Action	Calculated Permission
General		
Enable GPS in Video and Images	Inherit	inherited deny
Show GPS Overlay	Inherit	inherited allow
Show Date/Time Overlay	Inherit	inherited allow
Text Location of Overlay	Inherit	inherited allow
Text Size of Overlay	Inherit	inherited allow
Image Capture Resolution	Inherit	inherited allow
Encoder Hardware Acceleration	Inherit	inherited allow
Media Path	Inherit	inherited allow
Copy Captured Image to Gallery / Camera Roll	Inherit	inherited allow

Figure 7-25 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 \(on page 75\)](#) 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 reference

[Client Policy — Best Practices \(on page 117\)](#)

[Client Permissions — Best Practices \(on page 127\)](#)

Related information

[Client Policy & Permissions \(on page 75\)](#)

7.6.4. Global Directory

7.6.4.1. Global Directory Availability

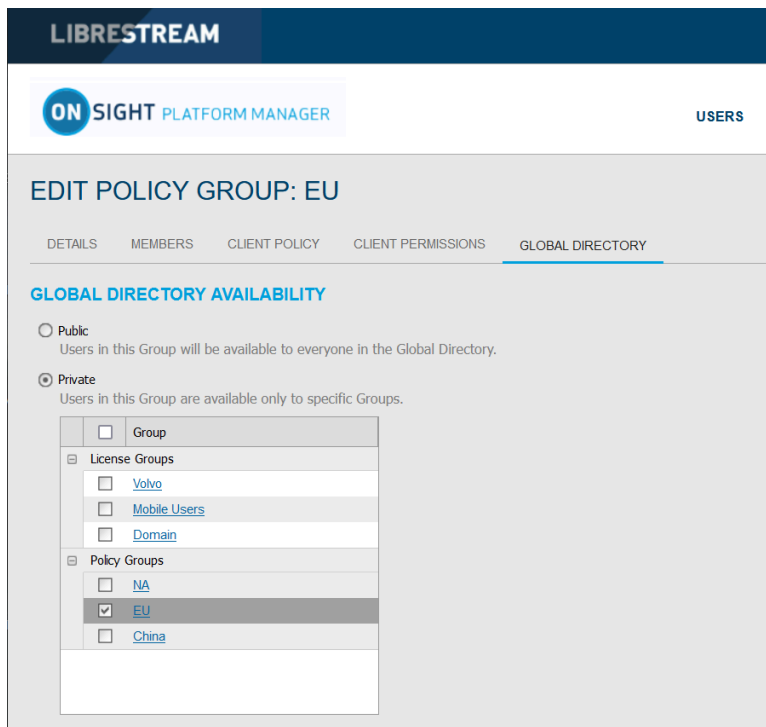




Figure 7-26 Edit Policy Group

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

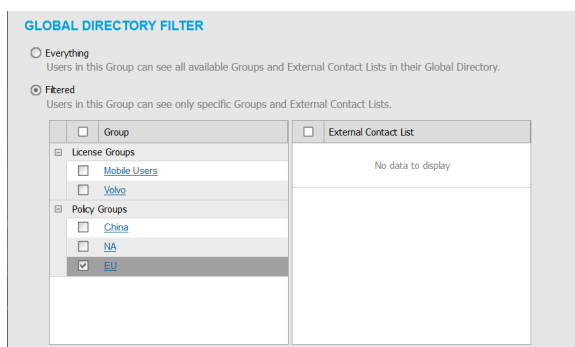


Figure 7-27 GLOBAL DIRECTORY FILTER

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

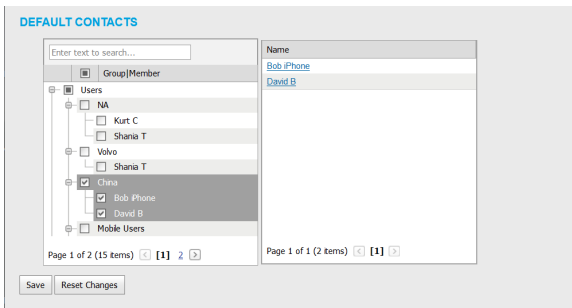


Figure 7-28 Default Contacts

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.

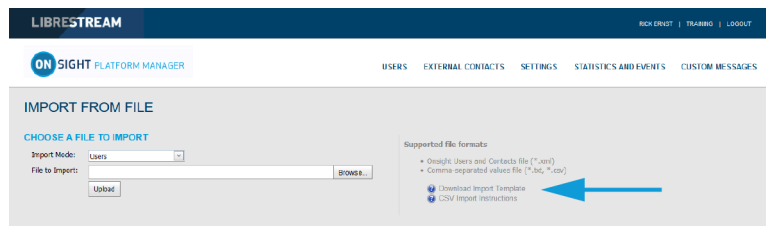


Figure 7-29 Import from File

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.

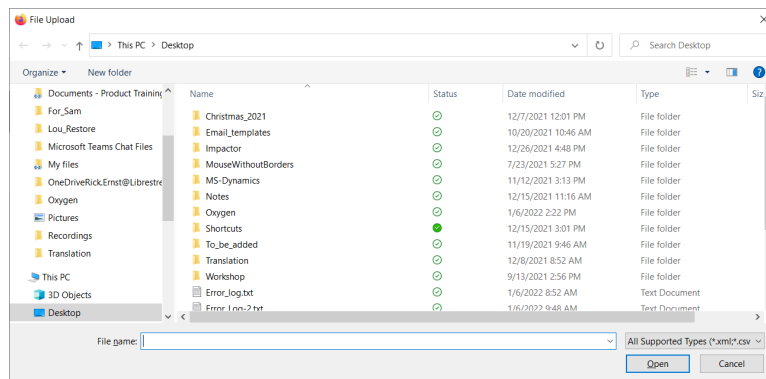



Figure 7-30 File Upload


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.

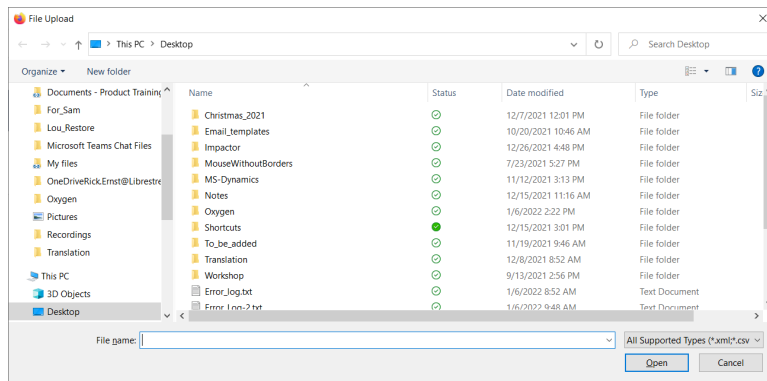


Figure 7-31 File Upload

4. Navigate to and select your `Users Import` template and click **Open**.
5. Click **Upload**. The Import Users window appears.

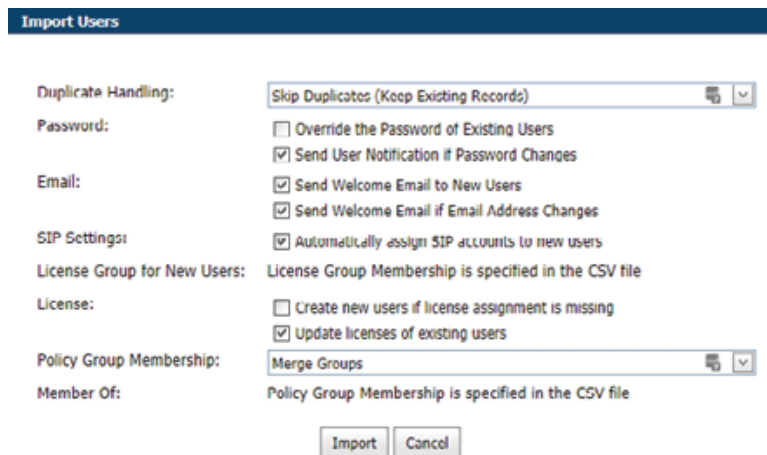



Figure 7-32 Import Users

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 Onsite 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.

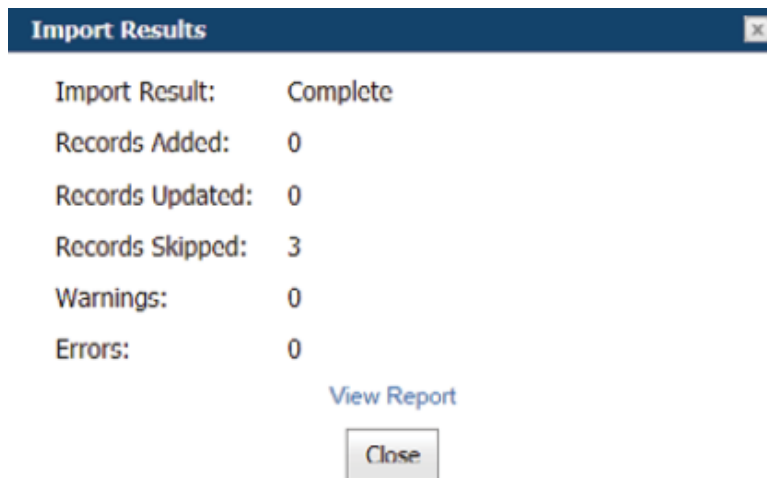



Figure 7-33 Import Results

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

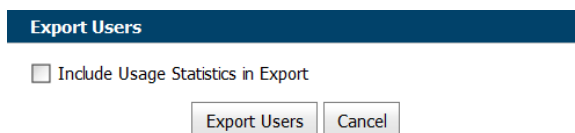


Figure 7-34 Export Users

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 Onsite Administrator can enable self-registration for Onsite accounts. The administrator distributes the link to the self-registration page with instructions to the Onsite 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 Onsite Connect.

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

Related reference

[Security — Best Practices \(on page 115\)](#)

8. EXTERNAL CONTACTS

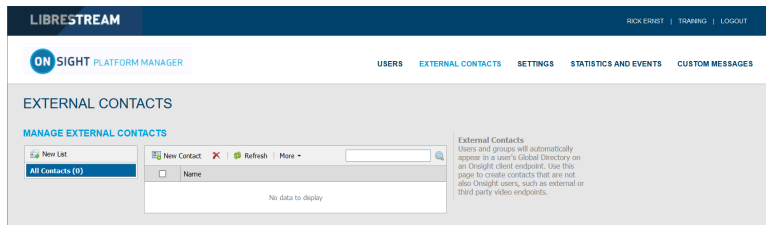



Figure 8-1 External Contacts

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.

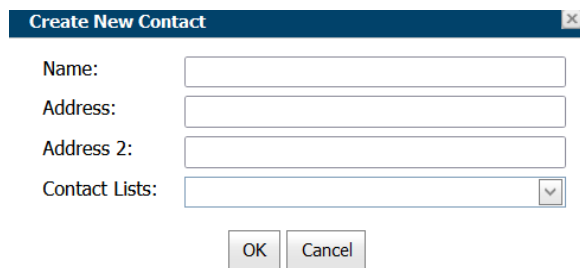
 **Tip:** Click **More > Import** to access the **CSV Import instructions** link within the **Supported file formats** section, as necessary.

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 Contact** icon.



The dialog box titled "Create New Contact" has a close button (X) in the top right corner. It contains four input fields: "Name:", "Address:", "Address 2:", and "Contact Lists:". The "Contact Lists:" field is a dropdown menu. Below the input fields are two buttons: "OK" and "Cancel".

Figure 8-3 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.

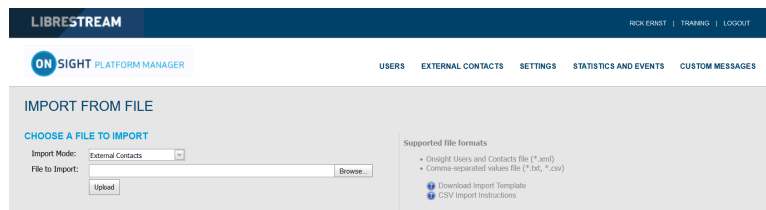
3. Select the **Contacts Lists** drop-down menu to add the external contact to.
4. Click **OK**. You will now be able to see the External Contact when searching the Global Directory from an Onsight endpoint. This completes the procedure.

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.



The "IMPORT FROM FILE" window is part of the OnSight Platform Manager interface. It has a header with "LIBRESTREAM" and "ON SIGHT PLATFORM MANAGER". Below the header are navigation tabs: "USERS", "EXTERNAL CONTACTS", "SETTINGS", "STATISTICS AND EVENTS", and "CUSTOM MESSAGES". The main content area is titled "IMPORT FROM FILE" and "CHOOSE A FILE TO IMPORT". It features a dropdown menu for "Import Mode" set to "External Contacts" and a "File to Import:" field with a "Browse..." button. Below the field is an "Upload" button. To the right, under "Supported file formats", there are three bullet points: "Onsight Users and Contacts file (*.xml)", "Comma-separated values file (*.csv, *.tsv)", and "CSV Import Instructions" with a link icon.

Figure 8-4 Import from File

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

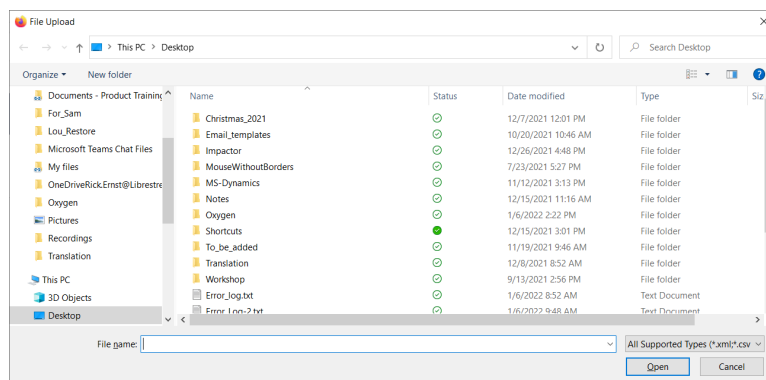


Figure 8-5 File Upload

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


Figure 8-6 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.

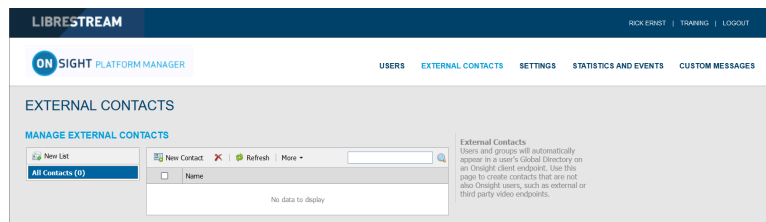


Figure 8-7 Manage External Contacts

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

Figure 8-8 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**.

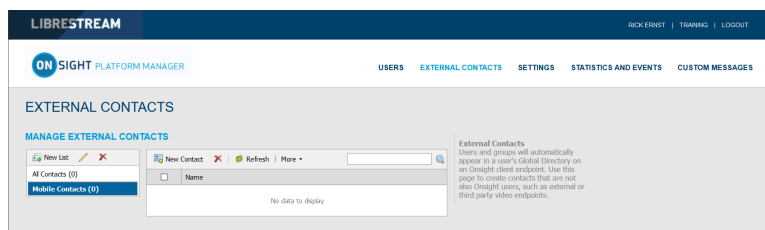


Figure 8-9 New List Appears

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.

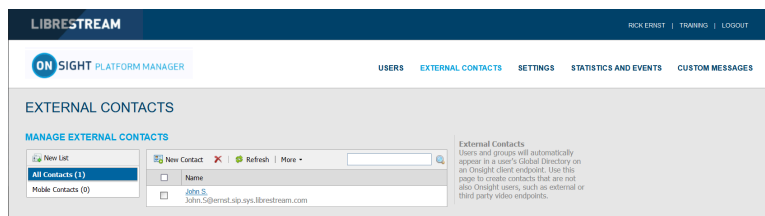


Figure 8-10 Manage External Contacts

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.

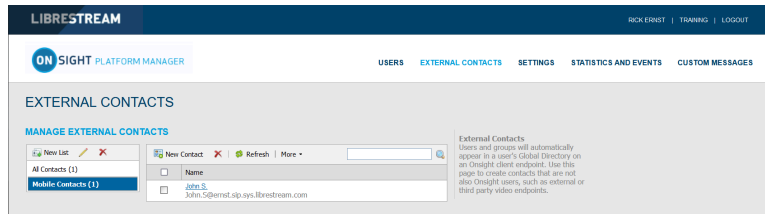


Figure 8-11 Contact Name Appears within the List

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

i **Tip:** You can remove a contact's 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

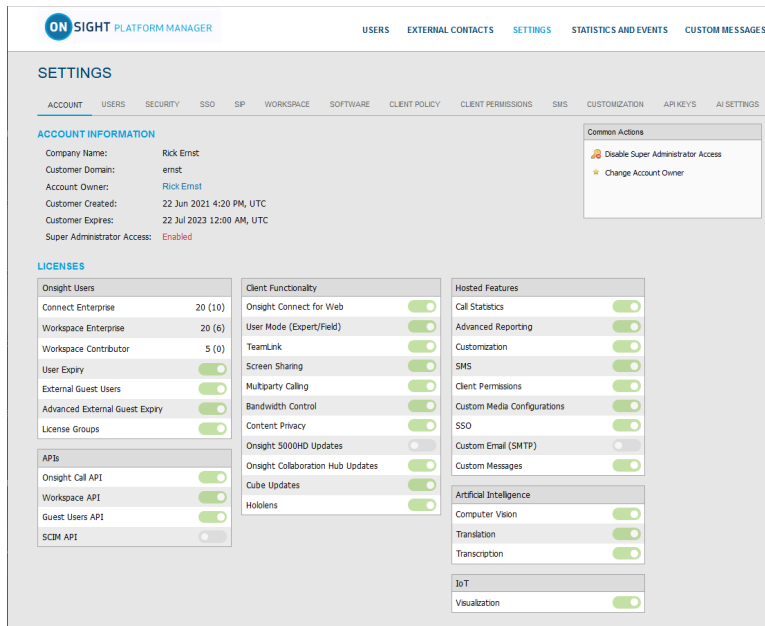


Figure 9-1 Settings

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

The screenshot displays the 'ON SIGHT PLATFORM MANAGER' interface. At the top, there are navigation tabs: 'USERS', 'EXTERNAL CONTACTS', 'SETTINGS', 'STATISTICS AND EVENTS', and 'CUSTOM MESSAGES'. The 'SETTINGS' tab is active, and within it, the 'ACCOUNT' sub-tab is selected. The 'ACCOUNT INFORMATION' section shows details for 'Rick Ernst', including the customer domain 'ernst', creation and expiry dates, and 'Super Administrator Access' status (Enabled). To the right, the 'Common Actions' panel contains two buttons: 'Disable Super Administrator Access' and 'Change Account Owner'. The 'LICENSES' section is divided into three columns: 'Onsight Users' (listing Connect Enterprise, Workspace Enterprise, Workspace Contributor, User Expiry, External Guest Users, Advanced External Guest Expiry, License Groups, and APIs), 'Client Functionality' (listing various features like Onsign Connect for Web, User Mode, TeamLink, etc.), and 'Hosted Features' (listing Call Statistics, Advanced Reporting, Customization, etc.).



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 reference

[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 \(on page 105\)](#) if assistance is required.

Related reference


[Account — Best Practices \(on page 112\)](#)

Related information

[CONTACT SUPPORT \(on page 105\)](#)

9.2.2. Change Account Owner

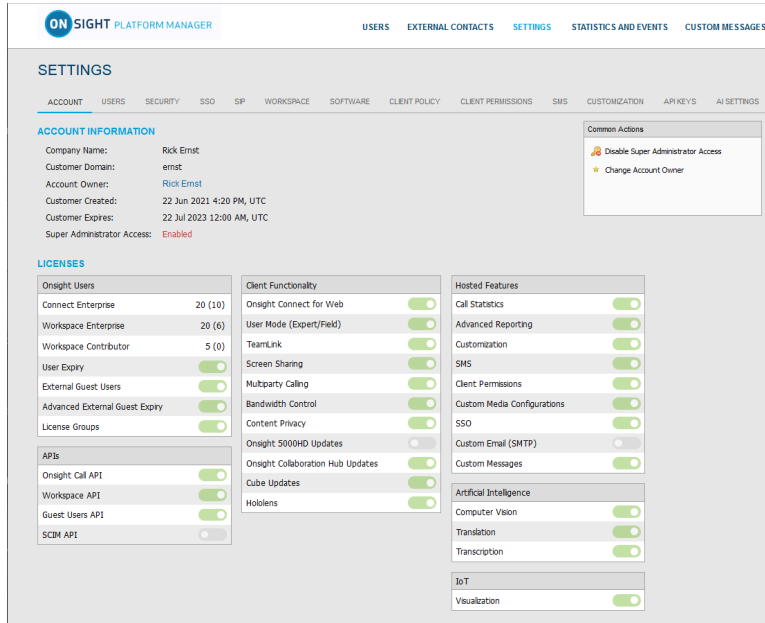
Within the **Common Actions** section, you can use **Change Account Owner** to specify the primary **OPM Administrator** for your Onsight Account Domain. **Change Account Owner** enables an Onsight Platform Manager Administrator to assign another user as the **Account Owner**.

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

Related reference

[Account — Best Practices \(on page 112\)](#)

9.2.3. Licenses



The screenshot shows the Onsight Platform Manager interface. The top navigation bar includes 'USERS', 'EXTERNAL CONTACTS', 'SETTINGS', 'STATISTICS AND EVENTS', and 'CUSTOM MESSAGES'. The 'SETTINGS' page has a sub-navigation bar with 'ACCOUNT INFORMATION', 'SECURITY', 'SSO', 'SP', 'WORKSPACE', 'SOFTWARE', 'CLIENT POLICY', 'CLIENT PERMISSIONS', 'SMS', 'CUSTOMIZATION', 'API KEYS', and 'AI SETTINGS'. The 'ACCOUNT INFORMATION' section displays details for Rick Ernst, including company name, domain, creation and expiration dates, and super administrator access status. The 'LICENSES' section is divided into four categories: 'Onsight Users' (Connect Enterprise: 20 (10), Workspace Enterprise: 20 (6), Workspace Contributor: 5 (0), User Expiry, External Guest Users, Advanced External Guest Expiry, License Groups), 'APIs' (Onsight Call API, Workspace API, Guest Users API, SCIM API), 'Client Functionality' (Onsight Connect for Web, User Mode (Expert/Field), TeamLink, Screen Sharing, Multiparty Calling, Bandwidth Control, Content Privacy, Onsight 5000HD Updates, Onsight Collaboration Hub Updates, Cube Updates, HoloLens), and 'Hosted Features' (Call Statistics, Advanced Reporting, Customization, SMS, Client Permissions, Custom Media Configurations, SSO, Custom Email (SMTP), Custom Messages, Artificial Intelligence (Computer Vision, Translation, Transcription), and IoT (Visualization)).

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 reference

[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

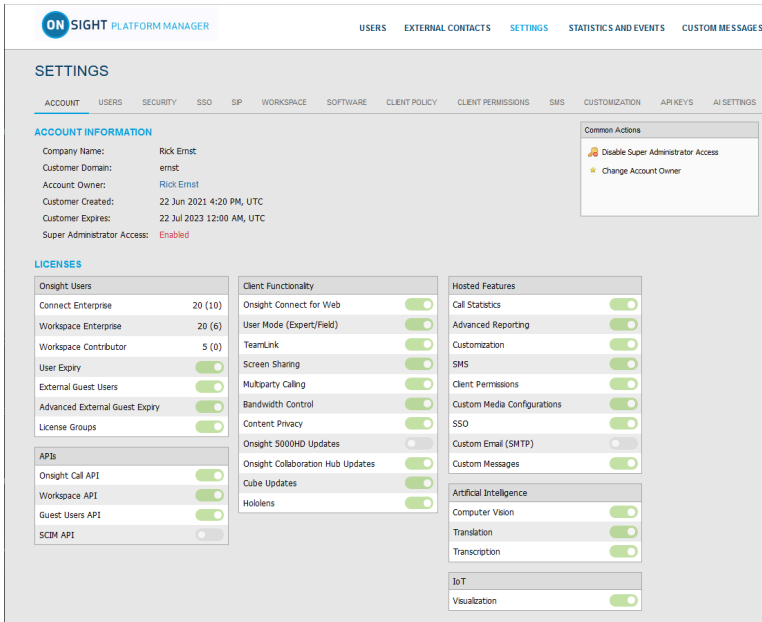


Figure 9-4 Settings

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 can be enabled or disabled for:

- **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**
- **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)
- **Custom Messages**

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, 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 Onsite 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: Onsite Workspace content is the property and responsibility of the customer. When an Onsite 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

The screenshot shows the 'LIBRESTREAM' interface with the 'ON SIGHT PLATFORM MANAGER' logo. The top navigation bar includes 'USERS', 'EXTERNAL CONTACTS', 'SETTINGS', 'STATISTICS AND EVENTS', and 'CUSTOM MESSAGES'. The 'SETTINGS' page is active, with sub-tabs for 'ACCOUNT', 'USERS', 'SECURITY', 'SSO', 'SIP', 'WORKSPACE', 'SOFTWARE', 'CLIENT POLICY', 'CLIENT PERMISSIONS', 'SMS', 'CUSTOMIZATION', 'API KEYS', and 'AI SETTINGS'. The 'USERS' sub-tab is selected. The page is divided into four sections: 'USER ACCOUNTS' with 'Default Time Zone' and 'Default Language' dropdowns; 'EXTERNAL GUEST USERS' with a note 'External Guest Settings moved to Client Policy'; 'GLOBAL DIRECTORY' with a checked checkbox 'External Contacts are public by default' and a sub-note; and 'CUSTOM FIELDS' with two columns: 'Custom Field Name' (listing Department, GuestInvtStatus, Region) and 'Custom Field Values' (listing Support, Training). Each column has 'Add', 'Modify', and 'Remove' buttons. A 'Save' and 'Reset Changes' button is at the bottom.

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 reference

[Users — Best Practices \(on page 114\)](#)


9.3.1. User Accounts

This screenshot is identical to Figure 9-5, showing the 'LIBRESTREAM' interface with the 'ON SIGHT PLATFORM MANAGER' logo. The top navigation bar includes 'USERS', 'EXTERNAL CONTACTS', 'SETTINGS', 'STATISTICS AND EVENTS', and 'CUSTOM MESSAGES'. The 'SETTINGS' page is active, with sub-tabs for 'ACCOUNT', 'USERS', 'SECURITY', 'SSO', 'SIP', 'WORKSPACE', 'SOFTWARE', 'CLIENT POLICY', 'CLIENT PERMISSIONS', 'SMS', 'CUSTOMIZATION', 'API KEYS', and 'AI SETTINGS'. The 'USERS' sub-tab is selected. The page is divided into four sections: 'USER ACCOUNTS' with 'Default Time Zone' and 'Default Language' dropdowns; 'EXTERNAL GUEST USERS' with a note 'External Guest Settings moved to Client Policy'; 'GLOBAL DIRECTORY' with a checked checkbox 'External Contacts are public by default' and a sub-note; and 'CUSTOM FIELDS' with two columns: 'Custom Field Name' (listing Department, GuestInvtStatus, Region) and 'Custom Field Values' (listing Support, Training). Each column has 'Add', 'Modify', and 'Remove' buttons. A 'Save' and 'Reset Changes' button is at the bottom.

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 reference

[Users — Best Practices \(on page 114\)](#)

9.3.2. External Guest Users

The screenshot shows the OnSight Platform Manager interface. At the top, there's a navigation bar with 'LIBRESTREAM' on the left and 'RICK ERNST | TRAINING | LOGOUT' on the right. Below that, a secondary navigation bar includes 'ON SIGHT PLATFORM MANAGER' and several menu items: 'USERS', 'EXTERNAL CONTACTS', 'SETTINGS', 'STATISTICS AND EVENTS', and 'CUSTOM MESSAGES'. The main content area is titled 'SETTINGS' and has a sub-menu with 'ACCOUNT', 'USERS', 'SECURITY', 'SSO', 'SIP', 'WORKSPACE', 'SOFTWARE', 'CLIENT POLICY', 'CLIENT PERMISSIONS', 'SMS', 'CUSTOMIZATION', 'API KEYS', and 'AI SETTINGS'. The 'USERS' sub-menu is active. Under 'USERS', there are sections for 'USER ACCOUNTS' (with dropdowns for 'Default Time Zone' and 'Default Language'), 'EXTERNAL GUEST USERS' (with a note 'External Guest Settings moved to Client Policy'), 'GLOBAL DIRECTORY' (with a checked checkbox 'External Contacts are public by default' and a note), and 'CUSTOM FIELDS' (with two columns: 'Custom Field Name' containing 'Department', 'GuestInvitedStatus', and 'Region', and 'Custom Field Values' containing 'Support' and 'Training'). At the bottom, there are 'Save' and 'Reset Changes' buttons.

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 reference

[Users — Best Practices \(on page 114\)](#)

[Client Policy — Best Practices \(on page 117\)](#)

[Client Permissions — Best Practices \(on page 127\)](#)

9.3.3. Global Directory

This screenshot is identical to Figure 9-7, showing the OnSight Platform Manager Settings page. The 'EXTERNAL GUEST USERS' section is expanded, showing the 'GLOBAL DIRECTORY' section. It features a checked checkbox labeled 'External Contacts are public by default' and a note below it: 'External Contacts that do not belong to any Contact List will be available to everyone in the Global Directory.' The 'CUSTOM FIELDS' section remains the same, with 'Department', 'GuestInvitedStatus', and 'Region' listed under 'Custom Field Name' and 'Support' and 'Training' under 'Custom Field Values'. 'Save' and 'Reset Changes' buttons are at the bottom.

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 reference

[Users — Best Practices \(on page 114\)](#)

9.3.4. Custom Fields

The screenshot shows the Librestream Settings page with the 'USERS' tab selected. Under the 'CUSTOM FIELDS' section, there are two columns: 'Custom Field Name' and 'Custom Field Values'. The 'Custom Field Name' column contains a list with 'Department', 'GuestInvtStatus', and 'Region'. The 'Custom Field Values' column contains a list with 'Support' and 'Training'. Below each list are 'Add', 'Modify', and 'Remove' buttons. At the bottom of the section are 'Save' and 'Reset Changes' buttons.

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 reference

[Users — Best Practices \(on page 114\)](#)

9.4. Security

The screenshot shows the Librestream Settings page with the 'SECURITY' tab selected. It contains several sections: 'PASSWORD POLICY' with fields for Minimum Length (8), Minimum Capital Letters (1), and Minimum Non-Alpha Characters (1); 'PASSWORD EXPIRATION' with checkboxes for 'Enable password expiration', 'Password Expires' (30 days), and 'Warn Users Before Expiration' (7 days); 'LOGIN POLICY' with fields for 'Maximum Bad Login Attempts' (3) and 'Account Lockout Duration' (5 minutes); and 'SELF REGISTRATION' with a checkbox for 'Enable Self Registration', a URL field, a 'Key' field, and checkboxes for 'Connect Enterprise', 'Workspace Enterprise', and 'Workspace Contributor'. There are also checkboxes for 'Account Activation Method', 'Notification', and 'Require Email Address for Self Registered Accounts', and a text field for 'Allowed Email Domains'. At the bottom are 'Save' and 'Reset Changes' buttons.

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 reference

[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 reference

[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 reference

[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 reference

[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 reference

[Security — Best Practices \(on page 115\)](#)

9.5. Single Sign On


The screenshot shows the 'LIBRESTREAM ON SIGHT PLATFORM MANAGER' interface. The 'SETTINGS' menu is active, and the 'SSO' tab is selected. The 'SINGLE SIGN-ON' section has 'Enable Single Sign-On' checked and 'Single Sign-On State' set to 'DISABLED'. Under 'Standard Users', 'Required' is selected. Under 'Administrators', 'Optional (allow OnSight credential login)' is selected. 'Offline Login' is set to 'Allow clients to operate offline'. A blue arrow points to the 'Send Instructions' link. The 'SAML CONFIGURATION' section shows 'SSO Domain' as 'ernst', 'Entry ID' as 'https://onsight.librestream.com/OamAdministrator/ernst/', and 'ACS URL' as 'https://onsight.librestream.com/OamAdministrator/SSO/SAML/ACS/ernst/'. The 'PARTNER IDENTITY PROVIDER SETTINGS' section includes fields for 'Entry ID', 'Single Sign-on URL', and 'Single Sign-on Binding' set to 'HTTP Redirect'. The 'USER IDENTITY FEDERATION' section has 'Require Signed Assertions' and 'Require Encrypted Assertions' unchecked, and 'IDP Signing Certificate' set to 'None specified'.

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 Onsign 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 Onsign. This value is equal to the Onsign 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

The screenshot shows the Onsign Platform Manager interface. The top navigation bar includes 'LIBRESTREAM', 'ON SIGHT PLATFORM MANAGER', and 'SETTINGS'. The main content area is titled 'SETTINGS' and has a sub-tab 'SSO'. Under 'SINGLE SIGN-ON', there is a 'Send Instructions' link highlighted by a blue arrow. The 'SAML CONFIGURATION' section is expanded to show 'LOCAL SERVICE PROVIDER SETTINGS' and 'PARTNER IDENTITY PROVIDER SETTINGS'. The 'PARTNER IDENTITY PROVIDER SETTINGS' section includes fields for 'Entity ID', 'Single Sign-on URL', and various SAML configuration options. The 'USER IDENTITY FEDERATION' section includes options for 'User Identity Mapping', 'Self Registration', 'Notification', 'Allowed Email Domains', and 'User Provisioning Links'.

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 IDENTITY FEDERATION** within the **SAML CONFIGURATION** section.

User Identity Federation settings define how SSO enterprise users map to Onsite 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 Onsite Account Fields.

The mapping tells OPM which Onsite 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 Onsite User's **Username** if these two attributes are mapped. The attribute name and values are case sensitive.

Choose one of the following mapping methods:

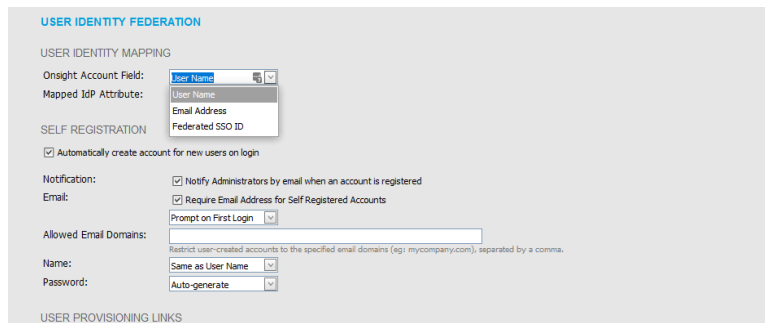
- **Username Mapping**
- **Email Mapping**
- **Federated SSO ID mapping**

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 **Onsite Account Field** drop-down menu to compare its values to the **Mapped IdP Attribute**:
 - **User Name** — Onsite Account User name
 - **Email Address** — Onsite Account Email Address
 - **Federated SSO Id** — Onsite user's associated Federated SSO Id. This is defined by the Onsite 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.



USER IDENTITY FEDERATION

USER IDENTITY MAPPING

Onsite Account Field: **User Name**

Mapped IdP Attribute: **User Name**

SELF REGISTRATION

Automatically create account for new users on login

Notification:

Notify Administrators by email when an account is registered

Email:

Require Email Address for Self Registered Accounts

Prompt on First Login

Allowed Email Domains:

Restrict user-created accounts to the specified email domains (e.g. mycompany.com), separated by a comma.

Name: **Same as User Name**

Password: **Auto-generate**

USER PROVISIONING LINKS

Figure 9-13 Onsite Account Field

2. Select the **Mapped IdP Attribute** drop-down menu to compare its values with the **Onsite Account Field**:
 - **Subject Name ID**
 - **Attribute** — Set the Attribute Name of the Attribute to be compared to the Onsite 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 Onsignt username.
 - **Attribute Name** — Sets the attribute name that will be used as the Onsignt username.
- **Auto-generate** — Creates the Onsignt username.
 - **Prefix** — Sets the prefix for auto-generated Onsignt usernames.
- **Prompt on First Login** — Prompts the user to enter an Onsignt 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 Onsignt 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 Onsignt 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 Onsignt credential login) has been selected. Users will be able to log in to Onsignt Connect directly without using their SSO credentials.

9.5.5. User Provisioning Links

USER IDENTITY FEDERATION

USER IDENTITY MAPPING

Onsignt Account Field: Federated SSO ID
 Mapped IDP Attribute: Attribute Attribute Name:

SELF REGISTRATION

Automatically create account for new users on login

Notification: Notify Administrators by email when an account is registered

User Name: Auto-generate Prefix: user_
 Email: Require Email Address for Self Registered Accounts
 Prompt on First Login

Allowed Email Domains:
Restrict user-created accounts to the specified email domains (eg. mycompany.com), separated by a comma.

Name: Same as User Name
 Password: Auto-generate

USER PROVISIONING LINKS

SSO Client Login: User Provisioning Links
The provided links can be included in an email message to your enterprise users to get them started with using Onsignt.

Windows Client Download:

Mobile Client Download:

Save Reset Changes

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 Onsignt 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

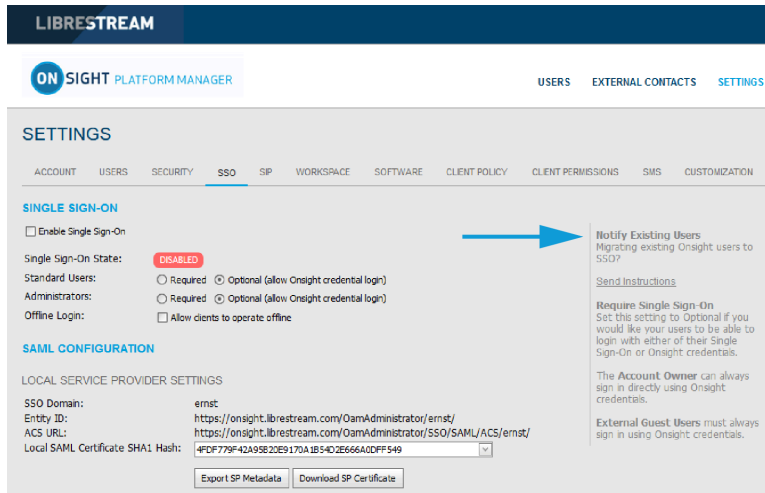


Figure 9-19 Notify Existing Users

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.

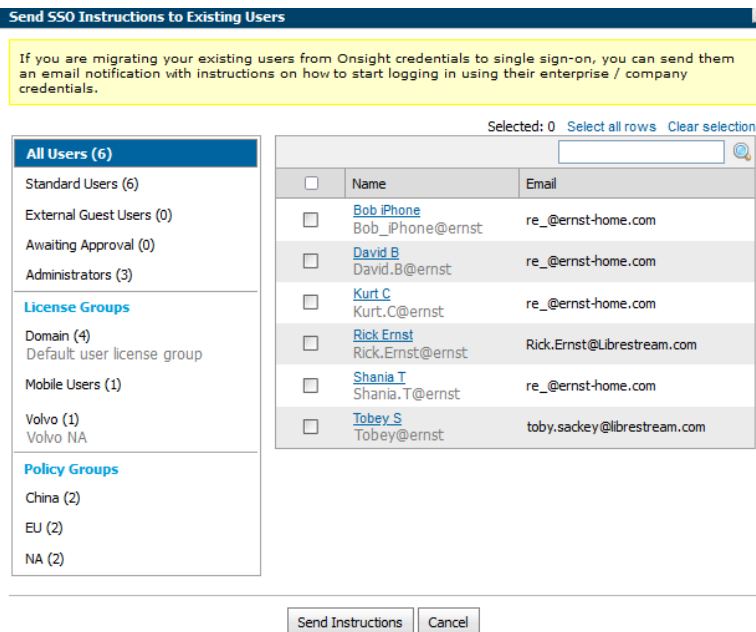


Figure 9-20 Send SSO Instructions to Existing Users

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

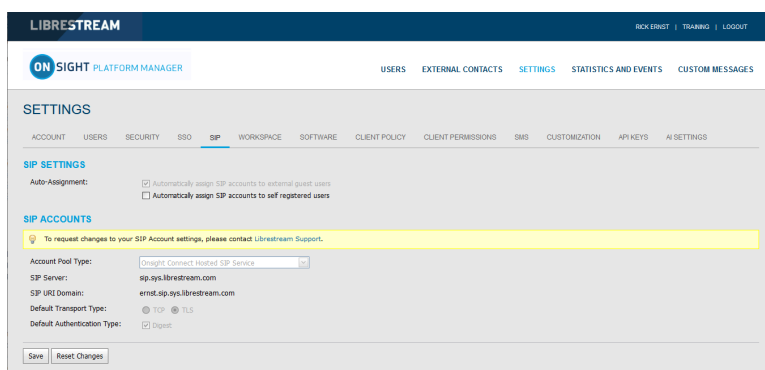


Figure 9-21 SIP Settings

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

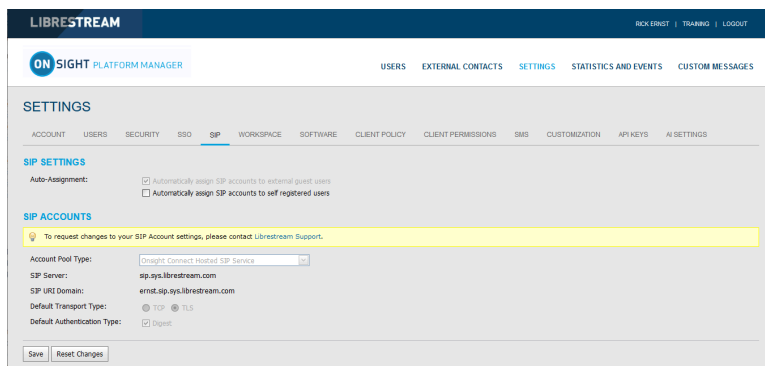


Figure 9-22 Auto-Assignment

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

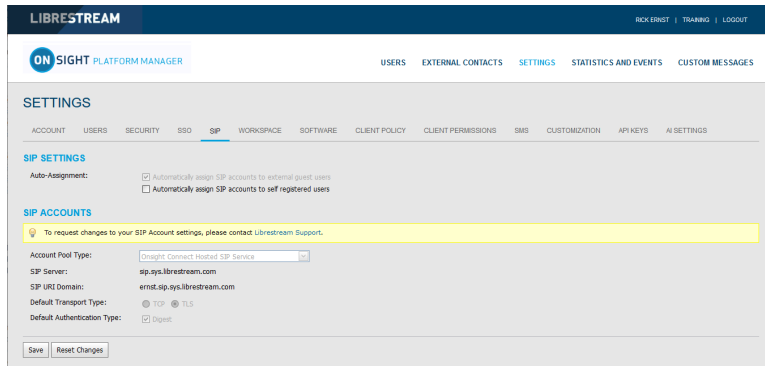


Figure 9-23 SIP Account

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

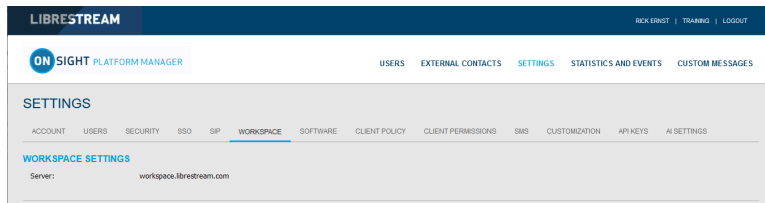


Figure 9-24 OnSight Workspace

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 reference

[Client Policy — Best Practices \(on page 117\)](#)

[Client Permissions — Best Practices \(on page 127\)](#)

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.

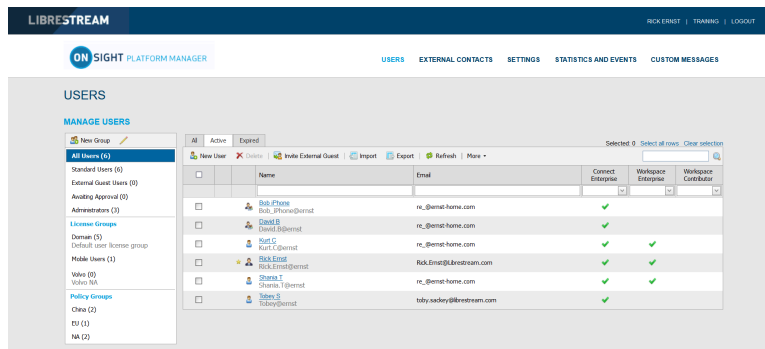


Figure 9-25 Users

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

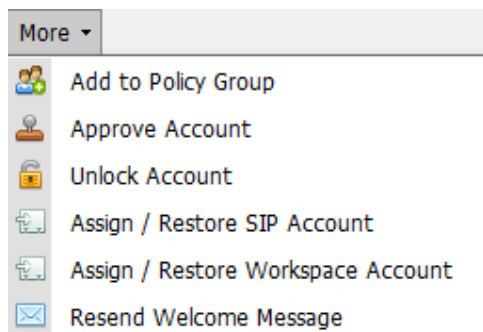




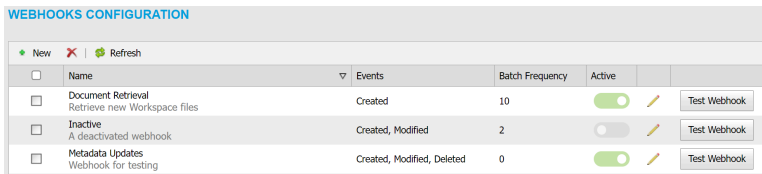
Figure 9-26 More drop-down menu

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 reference

- [Client Policy — Best Practices \(on page 117\)](#)
- [Client Permissions — Best Practices \(on page 127\)](#)

9.8. Workspace Webhooks



<input type="checkbox"/>	Name	Events	Batch Frequency	Active	
<input type="checkbox"/>	Document Retrieval Retrieve new Workspace files	Created	10	<input checked="" type="checkbox"/>	<input type="button" value="Test Webhook"/>
<input type="checkbox"/>	Inactive A deactivated webhook	Created, Modified	2	<input type="checkbox"/>	<input type="button" value="Test Webhook"/>
<input type="checkbox"/>	Metadata Updates Webhook for testing	Created, Modified, Deleted	0	<input checked="" type="checkbox"/>	<input type="button" value="Test Webhook"/>

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.

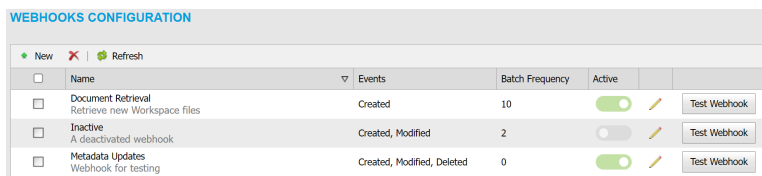
Workspace Webhooks are created and managed by an OPM Administrator when Workspace is enabled and configured for your account.

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.



<input type="checkbox"/>	Name	Events	Batch Frequency	Active	
<input type="checkbox"/>	Document Retrieval Retrieve new Workspace files	Created	10	<input checked="" type="checkbox"/>	<input type="button" value="Test Webhook"/>
<input type="checkbox"/>	Inactive A deactivated webhook	Created, Modified	2	<input type="checkbox"/>	<input type="button" value="Test Webhook"/>
<input type="checkbox"/>	Metadata Updates Webhook for testing	Created, Modified, Deleted	0	<input checked="" type="checkbox"/>	<input type="button" value="Test Webhook"/>

Figure 9-28 Webhooks Configuration

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

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.
- **Batch Frequency**: The maximum duration for webhook events that will be batched in a single notification in minutes. If 0, events will be batched within a minimum duration of 10 seconds.
- **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.

New Webhooks Configuration

Name:

Description:

Consumer URI:

HTTP Headers:

Administrator Email:

Batch Frequency:



User Name:

Password:

Active:

Events: Created
 Modified
 Deleted

Figure 9-29 New Webhooks Configuration

3. Enter all required fields and click **OK** to save the webhook configuration.
4. 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.
5. 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.
6. 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

LIBRESTREAM RICK ERNST | TRAINING | LOGOUT

ON SIGHT PLATFORM MANAGER USERS | EXTERNAL CONTACTS | SETTINGS | STATISTICS AND EVENTS | CUSTOM MESSAGES

SETTINGS

ACCOUNT | USERS | SECURITY | SSO | SP | WORKSPACE | **SOFTWARE** | CLIENT POLICY | CLIENT PERMISSIONS | SMS | CUSTOMIZATION | API KEYS | AI SETTINGS

SOFTWARE UPDATES

OS	Latest Published Version
Windows 7	<input type="text" value="Latest Published Version"/>
Windows 10/8.1/8	<input type="text" value="Latest Published Version"/>

Software Updates
Choose which version of software will be made available to new and existing users. Setting the version to Latest Published Versions will ensure your users are always offered the newest software release.

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 reference

[Software — Best Practices \(on page 116\)](#)

9.9.1. Onsite Connect for Windows

The OPM Administrator can select which version of Onsite Connect for Windows is available for download by Onsite 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 Onsite Connect for Windows.

Related reference

[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 Onsite 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 reference

[Software — Best Practices \(on page 116\)](#)

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

Librestream publishes the updates for the Onsite Cube and Collaboration Hub. These are available through Onsite 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 Onsite Platform Manager — Installation Guide for details on deploying update packages for Onsite Connect for Windows, Onsite 5000HD, and Onsite Collaboration Hub. Onsite mobile client updates are available in the App stores for on premises installations.

9.10. Client Policy & Permissions

The figure displays two screenshots of the Onsite Platform Manager settings interface. The left screenshot shows the 'CLIENT POLICY' settings page, and the right screenshot shows the 'CLIENT PERMISSIONS' settings page.

CLIENT POLICY settings include:

- Choose Settings (checked)
- Manage Media Configurations (checked)
- General settings: User Mode (Expert), Prompt for Permissions (As Required), Enable GPS in Video and Images (Enabled), Screen Sharing (Enabled), Show GPS Overlay (Enabled), Show Date/Time Overlay (Enabled), Copy Captured Image to Gallery / Camera Roll (Enabled), Text Location of Overlay (Bottom Left), Text Size of Overlay (Small), Image Capture Resolution (Low), Wait for Refresh on Last Video Frame (Enabled), Media Path (empty).
- Bandwidth Control: Enable Bandwidth Control (Disabled).

CLIENT PERMISSIONS settings include:

Domain Defaults	Description	Action	Calculated Permission
Client Administrators	General		
Standard Users	Enable GPS in Video and Images	Deny	Deny
External Guest Users	Show GPS Overlay	Allow	Allow
Domain	Show Date/Time Overlay	Allow	Allow
Mobile Users	Text Location of Overlay	Allow	Allow
Web	Text Size of Overlay	Allow	Allow
Policy Groups	Image Capture Resolution	Allow	Allow
China	Encoder Hardware Acceleration	Allow	Allow
EU	Media Path	Allow	Allow
NA	Copy Captured Image to Gallery / Camera Roll	Allow	Allow
	Allow Illumination	Allow	Allow
	Allow Flash	Allow	Allow
	Allow Laser	Allow	Allow
	Login		
	Auto Login	Allow	Allow

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 Onsite 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 reference

[Client Policy & Priority Precedence \(on page 107\)](#)

[Client Policy — Best Practices \(on page 117\)](#)

[Client Permissions — Best Practices \(on page 127\)](#)

9.10.1. External Guest Users

The screenshot shows the 'CLIENT POLICY' settings for 'External Guest Users' in the SIGHT Platform Manager. The interface includes a navigation menu on the left with categories like 'All Users', 'License Groups', and 'Policy Groups'. The main area contains a table of settings with columns for 'Description' and 'Value'. The settings are as follows:

Description	Value
Allow users to invite external guests	Enabled
Allow text message guest invitations	Disabled
SMS Max Message to User Length	100
Guest users must change temporary password on initial login	Disabled
Send 'Invitation Sent' confirmation to host (includes copy of invite)	Enabled
Disable recording of images and video	Enabled
Disable global directory access	Disabled
Epiry	1 days
User can choose expiry time when inviting guests	Disabled
Deactivate guest user account when removed from contact list	Disabled
Include option for guest to call host immediately	Enabled
From Email	Default
Custom Fields	<input type="checkbox"/> Department Required <input type="checkbox"/> GuestInUseStatus
Allow Setting User Mode while inviting guest	Disabled

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 Onsite 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 Onsite recordings or capturing Onsite still images. The **Default** option is **Enabled**, i.e., External Guest Users cannot record images and video.

i 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 reference

[Client Policy — Best Practices \(on page 117\)](#)

[Client Permissions — Best Practices \(on page 127\)](#)

9.10.2. External Guest Invitation Defaults

Description	Value
External Guest Users	
Allow users to invite external guests	Enabled
Allow text message guest invitations	Enabled
SMS Max Message to User Length	100
Guest users must change temporary password on initial login	Disabled
Send 'Invitation Sent' confirmation to host (includes copy of invite)	Enabled
Disable recording of images and video	Enabled
Disable global directory access	Disabled
Expiry	1 days
User can choose expiry time when inviting guests	Disabled
Deactivate guest user account when removed from contact list	Disabled
Include option for guest to call host immediately	Enabled
From Email	Default
Custom Fields	<input checked="" type="checkbox"/> Department <input type="checkbox"/> Required <input checked="" type="checkbox"/> Guest/Invitation <input type="checkbox"/>
Allow Setting User Mode while inviting guest	Enabled
User Mode	Expert

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 Onsite 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 reference

[Client Policy — Best Practices \(on page 117\)](#)

[Client Permissions — Best Practices \(on page 127\)](#)

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 reference

[Client Policy & Priority Precedence \(on page 107\)](#)

[Client Policy — Best Practices \(on page 117\)](#)

[Client Permissions — Best Practices \(on page 127\)](#)

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.

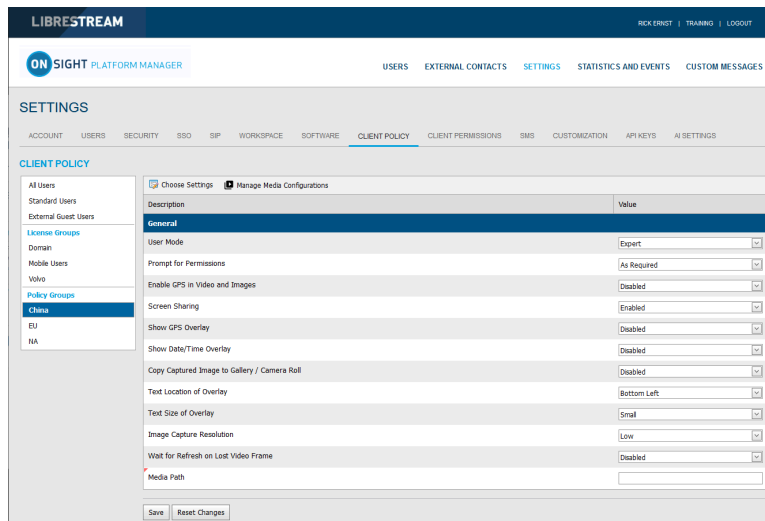



Figure 9-34 Group Client Policy

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

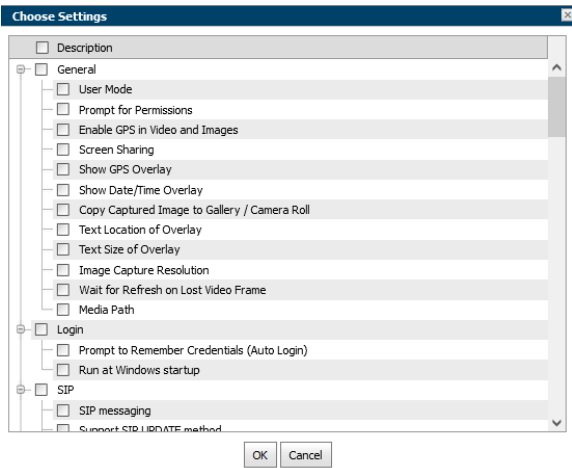


Figure 9-35 Choose Settings

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.

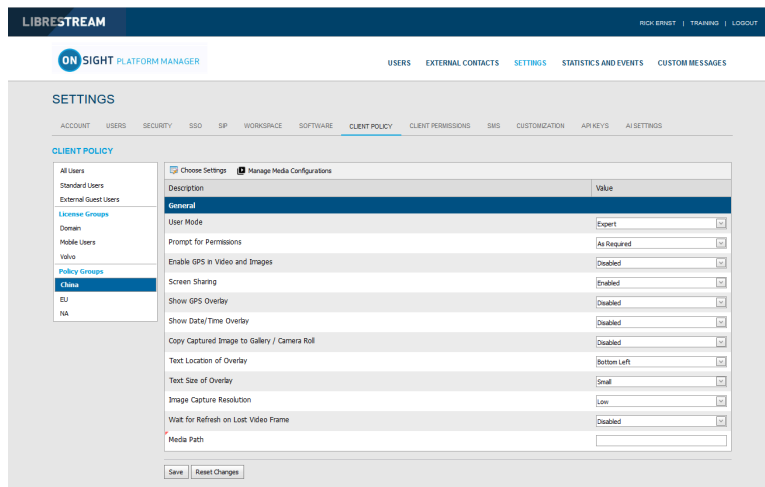


Figure 9-36 Setting Values

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 reference

[Client Policy — Best Practices \(on page 117\)](#)

[Client Permissions — Best Practices \(on page 127\)](#)

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.

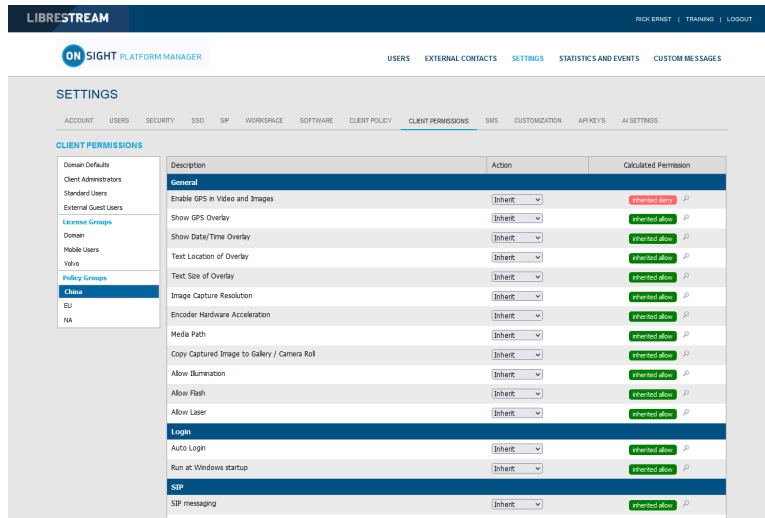


Figure 9-37 Setting Group Permissions

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 reference

[Client Policy — Best Practices \(on page 117\)](#)

[Client Permissions — Best Practices \(on page 127\)](#)

Related information

[Client Policy & Permissions \(on page 75\)](#)

9.10.4. Group Client Policy and Permissions

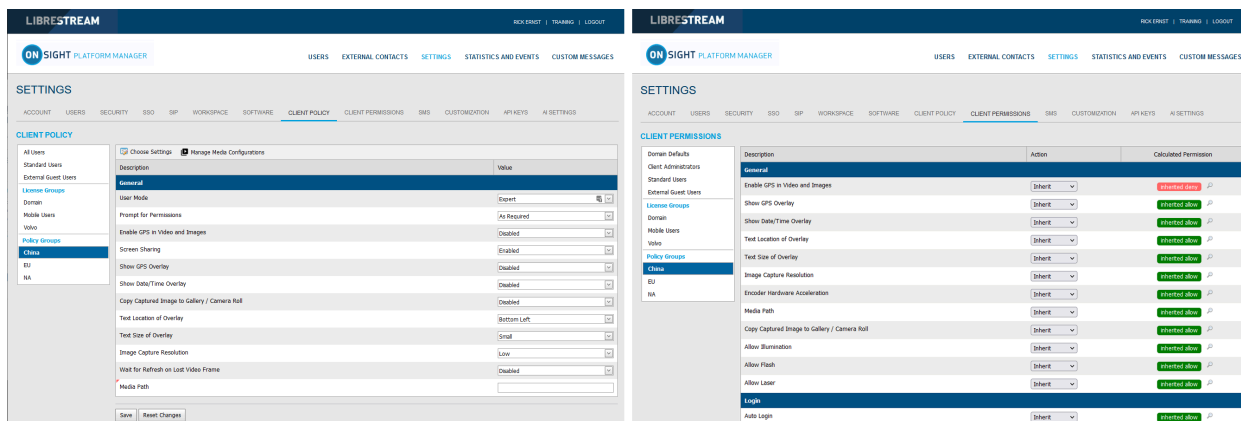


Figure 9-38 Group Client Policy & Permissions

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 reference

[Client Policy — Best Practices \(on page 117\)](#)
[Client Permissions — Best Practices \(on page 127\)](#)

Related information

[Client Policy & Permissions \(on page 75\)](#)

9.10.5. Remote Video Privacy

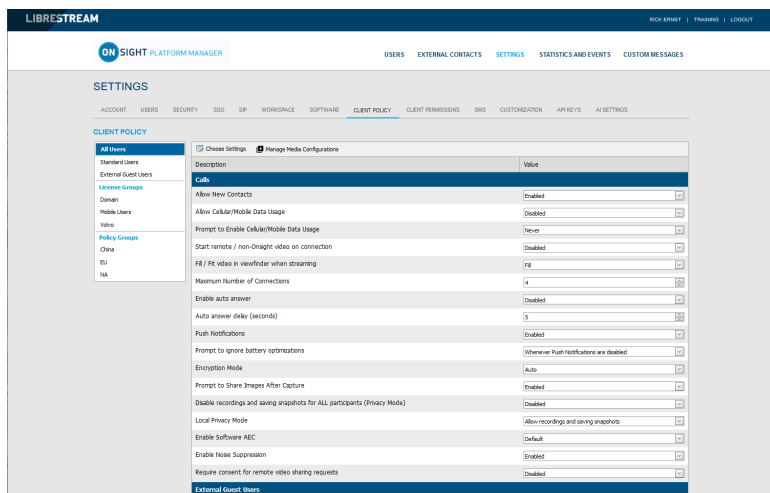


Figure 9-39 Privacy Settings

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.

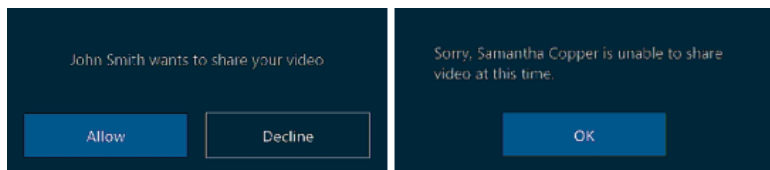


Figure 9-40 Requiring Consent

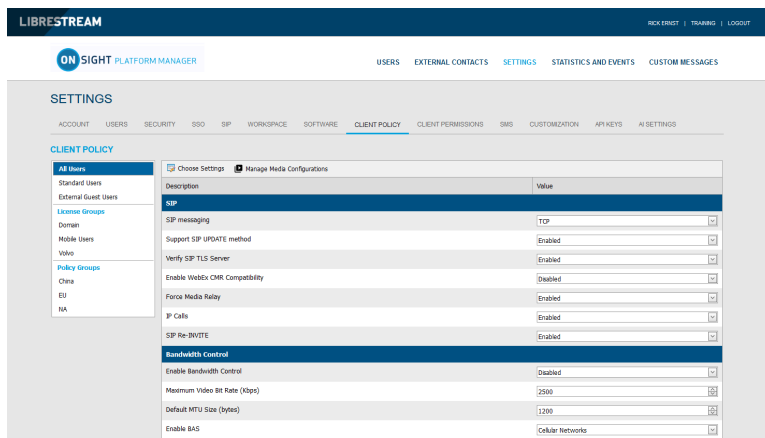
Video privacy is enhanced at sensitive locations by requiring users to provide consent before sharing video. Remote video privacy affects:

- **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 reference

[Client Policy — Best Practices \(on page 117\)](#)
[Client Permissions — Best Practices \(on page 127\)](#)

9.10.6. WebEx CMR Compatibility



The screenshot shows the Librestream Settings page with the 'CLIENT POLICY' tab selected. On the left, there is a sidebar with categories like 'All Users', 'Standard Users', 'External Guest Users', 'License Groups', 'Policy Groups', and 'NA'. The main content area shows a table of settings. The 'SIP' section is expanded, and the 'Enable WebEx CMR Compatibility' option is checked. Other settings include 'SIP messaging' (TZP), 'Support SIP UPDATE method' (Enabled), 'Verify SIP TLS Server' (Enabled), 'Force Media Relay' (Enabled), 'P Calls' (Enabled), and 'SIP Re-INVITE' (Enabled). The 'Bandwidth Control' section is also visible, with options like 'Enable Bandwidth Control' (Disabled), 'Maximum Video Bit Rate (Kbps)' (2500), 'Default MTU Size (bytes)' (1200), and 'Enable BAS' (Cellular Networks).

Figure 9-41 Client Policy

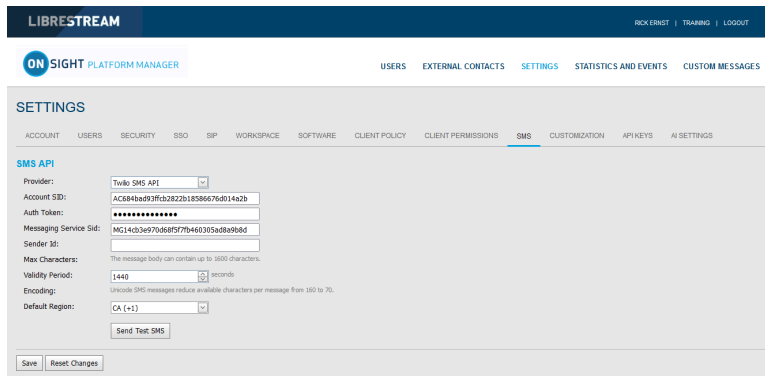
Access **Client Policy** and locate the **SIP** section to enable **WebEx CMR Compatibility**. **WebEx CMR Compatibility** enables Onsite Endpoints to call into WebEx Meeting rooms and act as a video/audio streaming endpoint. WebEx Meeting rooms will not accept calls from Onsite unless this feature is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

Related reference

[Client Policy — Best Practices \(on page 117\)](#)

[Client Permissions — Best Practices \(on page 127\)](#)

9.11. Short Message Service




The screenshot shows the Librestream Settings page with the 'SMS' tab selected. The 'SMS API' section is visible, with the following settings: 'Provider' (Twilio SMS API), 'Account SID' (AC848ba93f0c2822b18386676d014a2b), 'Auth Token' (masked with asterisks), 'Messaging Service Sid' (MG1403a97f066577b460305a08a9080), 'Sender Id' (empty), 'Max Characters' (The message body can contain up to 1600 characters), 'Validity Period' (1440 seconds), 'Encoding' (Unicode SMS messages reduce available characters per message from 160 to 70), and 'Default Region' (CA (+1)). There is a 'Send Test SMS' button and 'Save' and 'Reset Changes' buttons at the bottom.

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 \(on page 105\)](#)

9.12. Customization

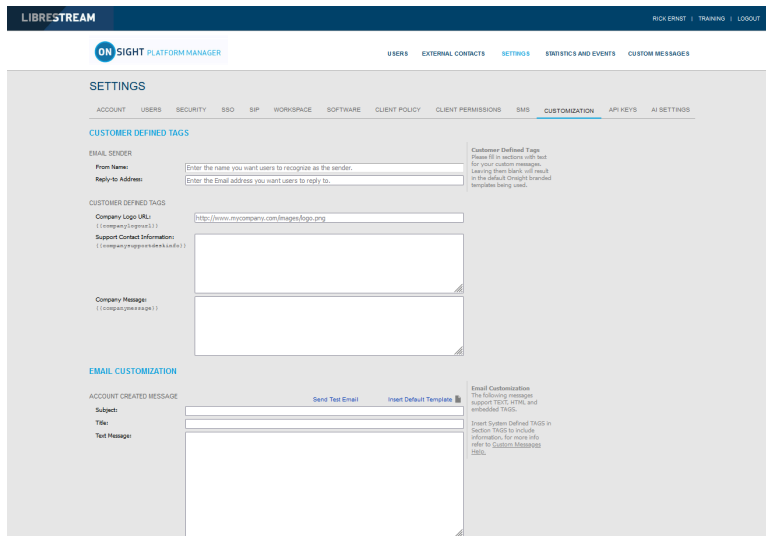


Figure 9-43 Customization

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

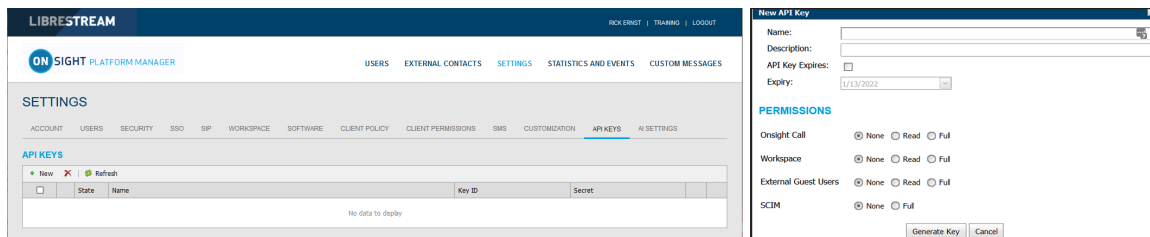



Figure 9-44 API Keys Page

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

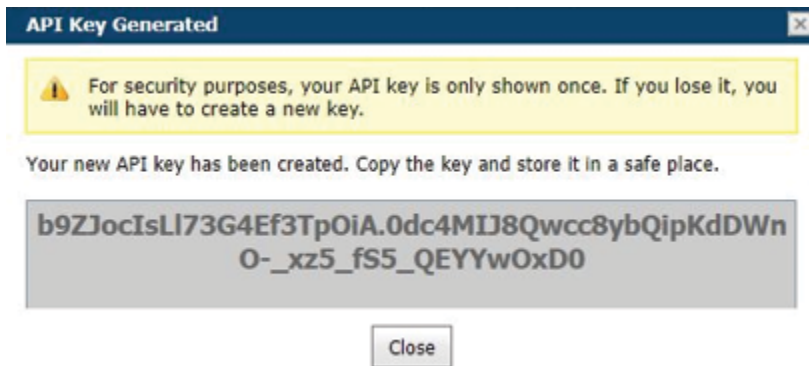


Figure 9-45 API Key Generated

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

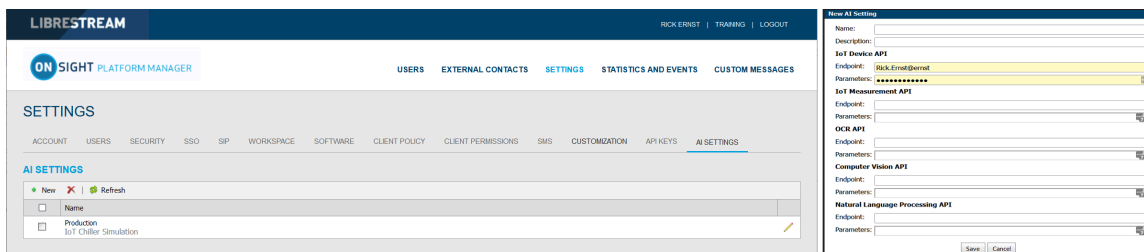




Figure 9-46 New AI Settings

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

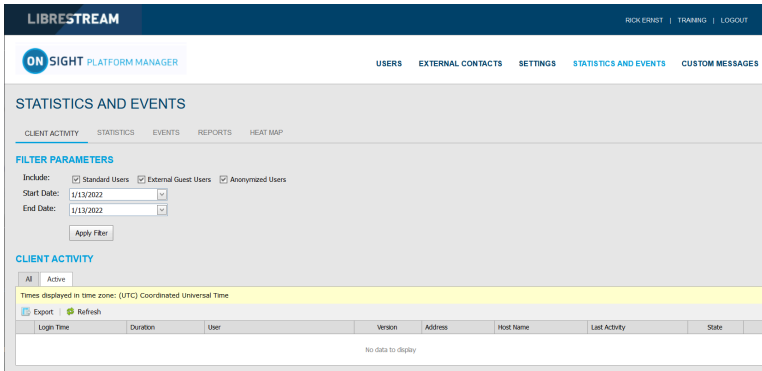


Figure 10-1 Statistics & Events

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

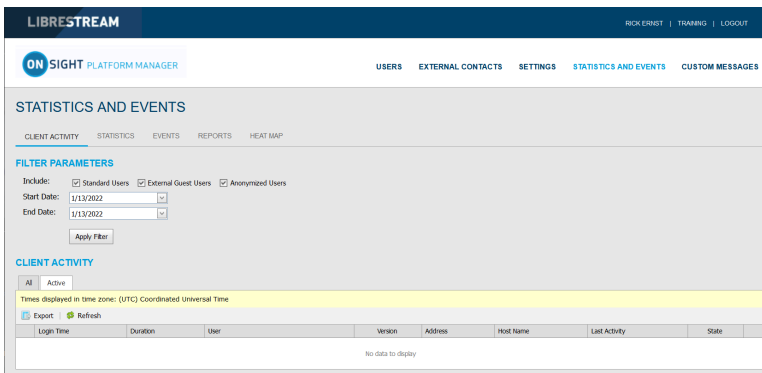


Figure 10-2 Client Activity

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**

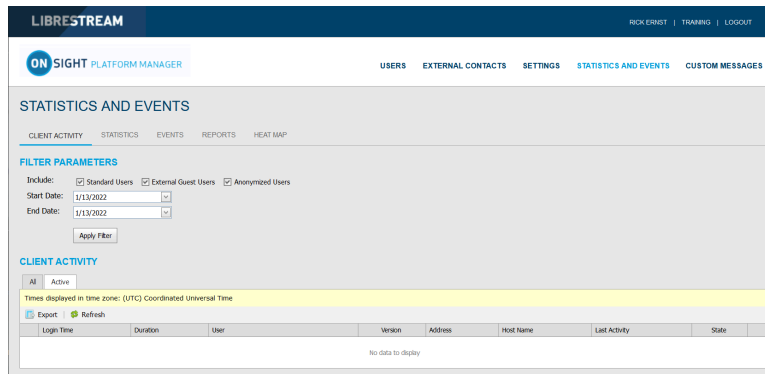


Figure 10-3 Filtering Users

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.

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**

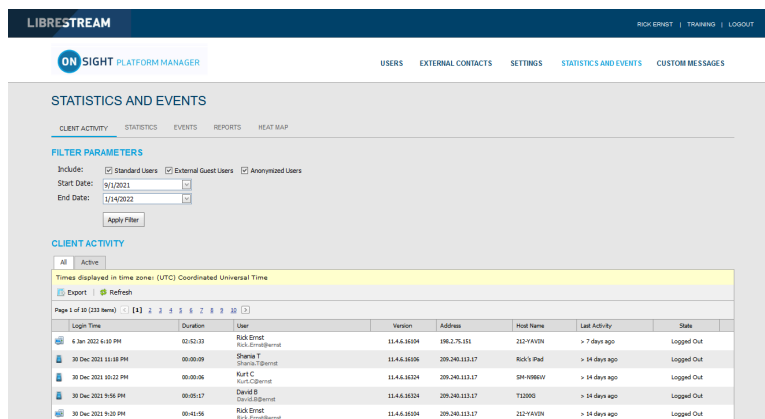


Figure 10-4 Client Activity Results

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

- 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**.

- 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

- Set your Date parameters. Click the drop-down menu and select a:
 - Start Date** using the Calendar pop-up menu.
 - End Date** using the Calendar pop-up menu.

3. Click **Apply Filter** to display results within the **CALLS** section.

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

- a. **Start Time**
- b. **Duration**
- c. **Calling Participant**
- d. **Calling User**
- e. **Called Participant**
- f. **Called User**

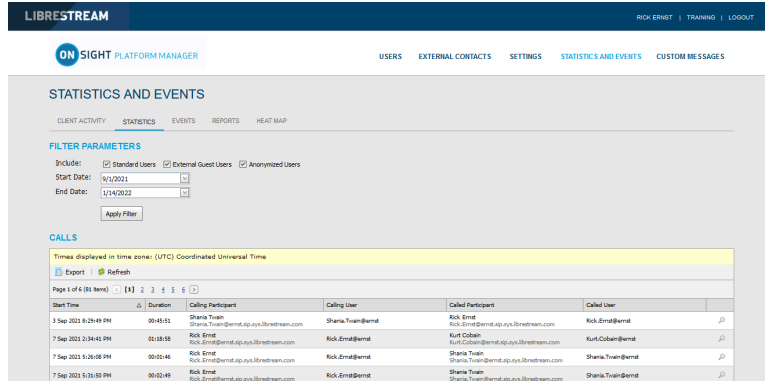


Figure 10-7 Statistic Report Results

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.

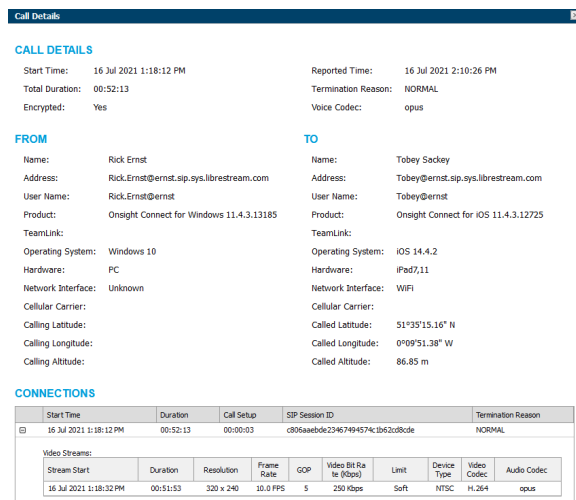


Figure 10-8 Statistic Call Details

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

The screenshot shows the 'STATISTICS AND EVENTS' page in the Librestream ON SIGHT Platform Manager. The page has a dark blue header with the Librestream logo and navigation links. Below the header is a navigation menu with 'STATISTICS AND EVENTS' selected. The main content area is divided into 'FILTER PARAMETERS' and 'EVENT LOG'. The 'FILTER PARAMETERS' section includes checkboxes for Severity (Information, Warning, Error, Fatal) and Include (Standard Users, External Guest Users, API Users). The 'EVENT LOG' section displays a table of events with columns for Time, User, API Key, Description, and Details. The events listed include user logins and a group policy update.

Time	User	API Key	Description	Details
13 Jan 2022 7:07 PM	Rick.Ernst@erast	-	User logged in successfully. [IP Address: 64.4.89.120]	Username: Rick.Ernst@erast, FullName: Rick Ernst
13 Jan 2022 9:34 PM	Rick.Ernst@erast	-	User logged in successfully. [IP Address: 198.2.75.151]	Username: Rick.Ernst@erast, FullName: Rick Ernst
13 Jan 2022 9:58 PM	Rick.Ernst@erast	-	User logged in successfully. [IP Address: 198.2.75.151]	Username: Rick.Ernst@erast, FullName: Rick Ernst
13 Jan 2022 2:19 PM	Rick.Ernst@erast	-	Group 'Chase' client policy updated.	
13 Jan 2022 2:05 PM	Rick.Ernst@erast	-	User logged in successfully. [IP Address: 198.2.75.151]	Username: Rick.Ernst@erast, FullName: Rick Ernst
13 Jan 2022 11:50 AM	Rick.Ernst@erast	-	User logged in successfully. [IP Address: 198.2.75.151]	Username: Rick.Ernst@erast, FullName: Rick Ernst
12 Jan 2022 10:15 PM	Rick.Ernst@erast	-	User logged in successfully. [IP Address: 198.2.75.151]	Username: Rick.Ernst@erast, FullName: Rick Ernst

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**

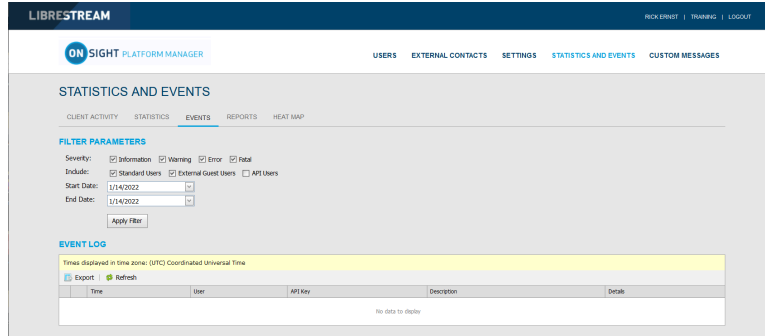


Figure 10-10 Filtering by Severity and Users

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.

5. The Event Log displays:

- a. **Time**

- b. **User**

- c. **API Key**

- d. **Description**

- e. **Details**

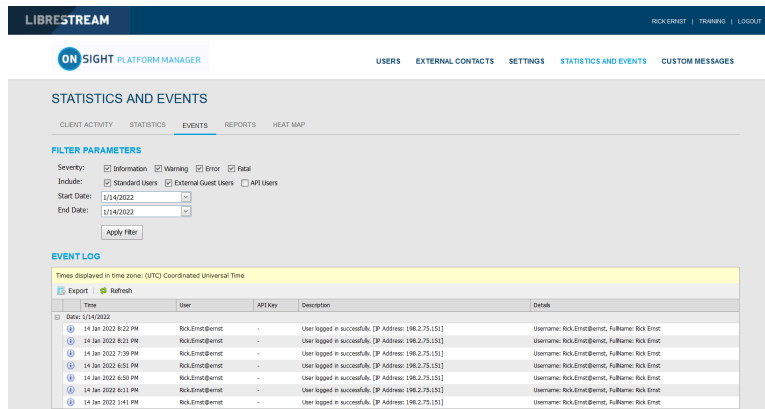


Figure 10-11 Statistics Report Results

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

The screenshot displays the 'REPORTS' tab in the SIGHT Platform Manager. The 'REPORT PARAMETERS' section includes dropdown menus for Report Name, Start Date, End Date, User Account Type, Groups, Country, and Custom Fields. It also features a 'Call Duration' dropdown, a 'Number of Results' dropdown, and a checked 'Include anonymous records' checkbox. A 'Run Report' button is located below these options. The 'RESULTS' section, titled 'TOP USAGE (CALLS)', shows a table with columns for Name, # of Calls, and Duration (mins). The table lists three users: Rick Ernst (92 calls, 74:07:28), Shana T (42 calls, 46:13:48), and Matt C (19 calls, 13:22:23).

Name	# of Calls	Duration (mins)
Rick Ernst rick.ernst@ernst	92	74:07:28
Shana T Shana.T@ernst	42	46:13:48
Matt C matt.c@ernst	19	13:22:23

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. 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.

The screenshot shows the 'REPORT PARAMETERS' form in the Librestream interface. The form is organized into several sections:

- Report Name:** A dropdown menu with 'Top Usage (Calls)' selected.
- Start Date:** A date picker showing '1/14/2022'.
- End Date:** A date picker showing '1/14/2022'.
- User Account Type:** A dropdown menu with 'Optional (default to All User Account Type)' selected.
- Groups:** A dropdown menu with 'Optional (default to All User)' selected.
- Country:** A dropdown menu with 'Optional (default to All Country)' selected.
- Custom Fields:** A dropdown menu with 'Add Custom Fields For Filtering' selected.
- Call Duration:** A dropdown menu with 'any' selected.
- Number of Results:** A dropdown menu with '10' selected.
- Include anonymous records:** A checked checkbox.
- Run Report:** A button at the bottom of the form.

Figure 10-13 Report Parameters

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

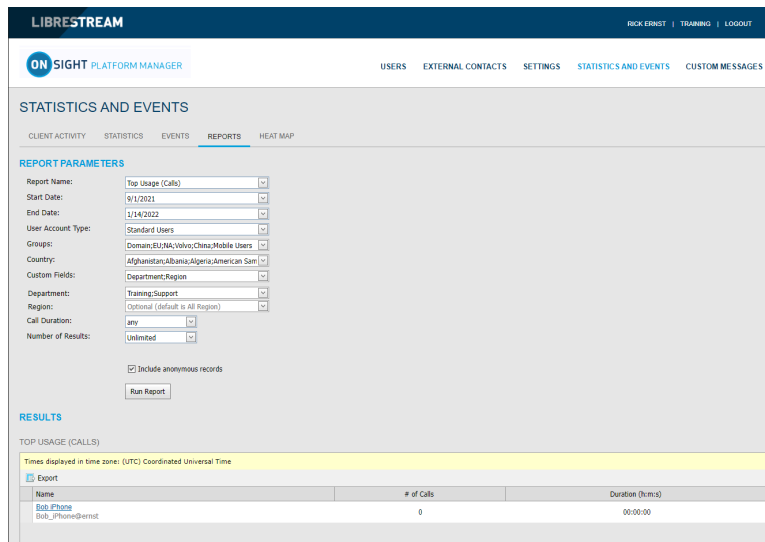


Figure 10-14 Report Results

- (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

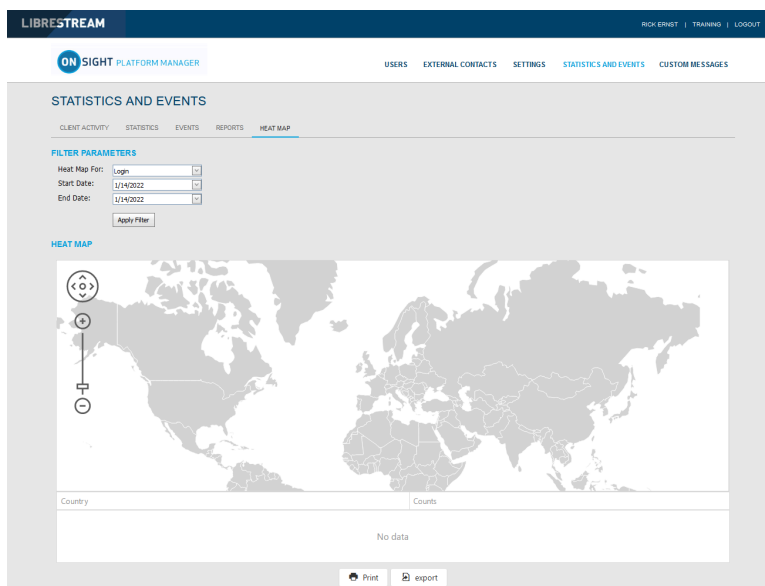



Figure 10-15 Heat Map Page

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**

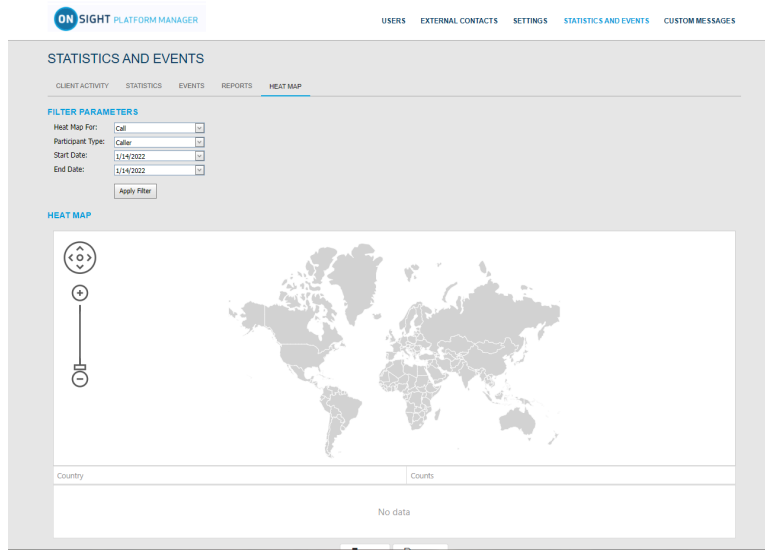


Figure 10-16 Heat Map Filter Parameters

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.

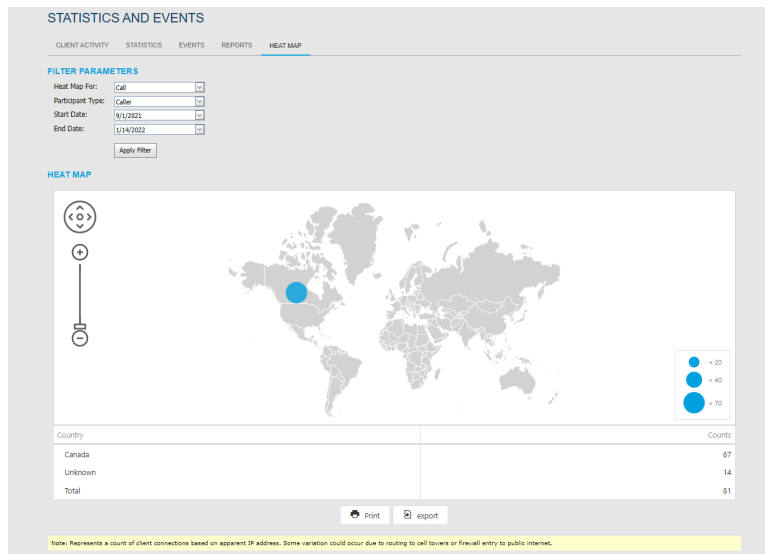


Figure 10-17 Heat Map Report Results

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**:

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

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

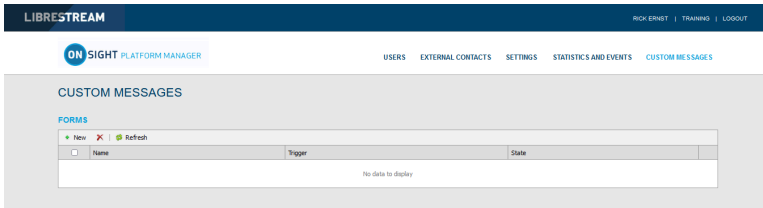



Figure 12-1 Custom Messages

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 Onsite 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.

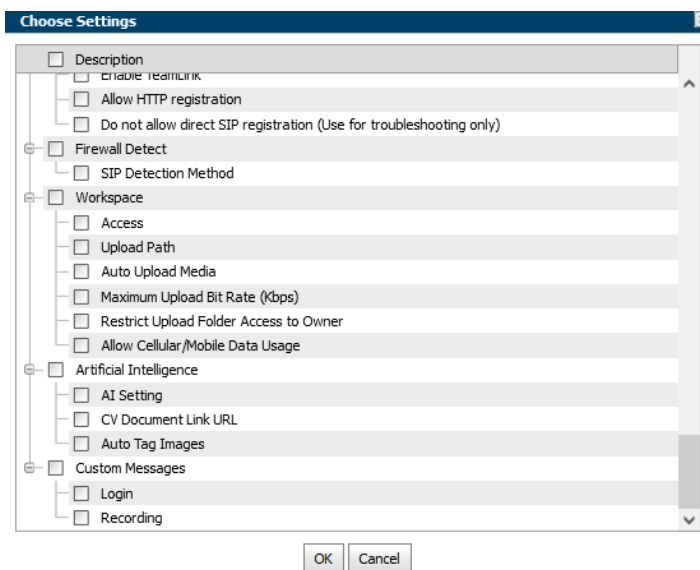


Figure 12-3 Choose Settings

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/termsfuse/>

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	<ol style="list-style-type: none"> 1. Field 2. Expert
Prompt for Permissions	<ol style="list-style-type: none"> 1. On Login 2. As Required
Enable GPS Location in Video and Images	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Show GPS Overlay	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Show Date/Time Overlay	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Copy Captured Image to Gallery / Camera Roll	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Text Location of Overlay	<ol style="list-style-type: none"> 1. Bottom Left 2. Bottom Right 3. Top Left 4. Top Right
Text Size of Overlay	<ol style="list-style-type: none"> 1. Large 2. Medium 3. Small
Image Capture Resolution	<ol style="list-style-type: none"> 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)	<ol style="list-style-type: none"> 1. Disabled 2. Enabled
Run at Windows startup	<ol style="list-style-type: none"> 1. FALSE 2. TRUE

Client Policy Item	Priority (High to low)
SIP	
SIP messaging	<ol style="list-style-type: none"> 1. UDP 2. TCP
Support SIP UPDATE method	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Verify SIP TLS Server	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Enable WebEx CMR Compatibility	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Force Media Relay	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Media Configurations	
Custom Media Configurations	Combined list from all groups
Bandwidth Control	
Enable Bandwidth Control	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Maximum Video Bit Rate (Kbps)	<ol style="list-style-type: none"> 1. Lower Value 2. Higher Value
Enable BAS	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Preferred Voice Codec	<ol style="list-style-type: none"> 1. Low Bandwidth (GSM) 2. Default (G.711)
Preferred Subject Audio Codec	<ol style="list-style-type: none"> 1. Disabled 2. Low Bandwidth (GSM) 3. Default (G.711)
Audio Efficiency	<ol style="list-style-type: none"> 1. Lower bandwidth 2. Mid 3. Lower latency
Calls	
Allow Cellular / Mobile Data Usage	<ol style="list-style-type: none"> 1. FALSE 2. TRUE

Client Policy Item	Priority (High to low)
Prompt to Enable Cellular / Mobile Data Usage	<ol style="list-style-type: none"> 1. On Every Login 2. On First Login 3. Never
Start remote / non-Onsight video on connection	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Fill / Fit video in viewfinder when streaming	<ol style="list-style-type: none"> 1. Fill 2. Fit 3. Actual Size
Maximum Number of Connections	<ol style="list-style-type: none"> 1. Lower Value 2. Higher Value
Enable auto answer	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Auto answer delay (seconds)	<ol style="list-style-type: none"> 1. Lower Value 2. Higher Value
Push Notifications	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Prompt to ignore battery optimizations	<ol style="list-style-type: none"> 1. Only when user disables Push Notifications 2. Whenever Push Notifications are disabled
Encryption Mode	<ol style="list-style-type: none"> 1. On 2. Auto 3. Off
Prompt to Share Images After Capture	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Disable recordings and saving snapshots for ALL participants (Privacy Mode)	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Local Privacy Mode	<ol style="list-style-type: none"> 1. Disable recordings and saving snapshots 2. Disable recordings 3. Disable saving snapshots 4. Allow recordings and saving snapshots
Networking	
Diffserv DSCP (Voice)	<ol style="list-style-type: none"> 1. Voice 2. Audio / Video / Guaranteed 3. Controlled Load 4. Best Effort

Client Policy Item	Priority (High to low)
Diffserv DSCP (Video)	<ol style="list-style-type: none"> 1. Voice 2. Audio / Video / Guaranteed 3. Controlled Load 4. Best Effort
Diffserv DSCP (Subject Audio)	<ol style="list-style-type: none"> 1. Voice 2. Audio / Video / Guaranteed 3. Controlled Load 4. Best Effort
Diffserv DSCP (Data Stream)	<ol style="list-style-type: none"> 1. Voice Audio 2. Video 3. Gauranteed Controlled Load Best Effort
TeamLink	
Enable TeamLink	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Allow HTTP registration	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Do not allow direct SIP registration (User for troubleshooting only)	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Firewall Detect	
SIP Detection Method	<ol style="list-style-type: none"> 1. SIP Server — Full 2. SIP Server — Basic 3. TeamLink
Workspace	
Access	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Upload Path	Undefined — This setting accepts the value for the last group in list.
Auto Upload Media	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Maximum Upload Bit Rate (Kbps)	<ol style="list-style-type: none"> 1. Lower Value 2. Higher Value
Restrict Upload Folder Access to Owner	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Allow Cellular / Mobile Data Usage	<ol style="list-style-type: none"> 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 \(on page 75\)](#)

[Policy Precedence \(on page 78\)](#)

Best Practices

15.2.1. Account — Best Practices

Table 15-2 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 15-2 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 \(on page 50\)](#)

15.2.2. Users — Best Practices

Table 15-3 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	<input checked="" type="checkbox"/> 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 \(on page 55\)](#)

15.2.3. Security — Best Practices

Table 15-4 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:	<input type="checkbox"/> 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 <input checked="" type="checkbox"/> 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/OamDev/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:	<input type="checkbox"/> default disabled	If Self Registration is enabled you can specify the license type	

Table 15-4 Security — Best Practices (continued)

Settings	Value	Description	Best Practices/Tips
Account Activation Method:	default enabled <input checked="" type="checkbox"/> 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 <input checked="" type="checkbox"/> Notify Administrators by email when an account is registered	OPM Admins will receive emails whenever a user registers.	
Email	default enabled <input checked="" type="checkbox"/> 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 \(on page 57\)](#)

15.2.4. Software — Best Practices

Table 15-5 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 \(on page 74\)](#)

15.2.5. Client Policy — Best Practices

Table 15-6 Client Policy — Best Practices

Settings	Value	Description	Best Practices/Tips
External Guest Users			
Allow users to invite external guests	<input checked="" type="checkbox"/> default enabled	Enables users to send guest invites	
Allow text message guest invitations	<input type="checkbox"/> 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	<input type="checkbox"/> default disabled		
Send 'Invitation Sent' confirmation to host (includes copy of invite)	<input checked="" type="checkbox"/> default enabled	Enables you to view a copy of the invitation	
Allow recording of images and video	<input checked="" type="checkbox"/> default enabled		
Allow global directory access	<input checked="" type="checkbox"/> default disabled	Not enabled for guest users	
Expiry	1	Day	
User can choose expiry time when inviting guests	<input type="checkbox"/> default disabled		
Deactivate guest user account when removed from contact list	<input type="checkbox"/> 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	<input checked="" type="checkbox"/> 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 Onsite 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.

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

Settings	Value	Description	Best Practices/Tips
Allow Setting User Mode while inviting guest	<input type="checkbox"/> 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.
General			
User Mode	Expert	Sets the mode the user operates in when logged in on an Onsite 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	<input type="checkbox"/> Disabled*	GPS meta data will be embedded in recordings and images	
Screen Sharing	<input checked="" type="checkbox"/> Enabled*	Enables Screen Sharing between participants.	
Show GPS Overlay	<input type="checkbox"/> Disabled*		
Show Date/Time Overlay	<input type="checkbox"/> Disabled*		
Copy Captured Image to Gallery/Camera Roll	<input type="checkbox"/> 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*		

* All default values are marked with an asterisk.

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



Settings	Value	Description	Best Practices/Tips
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 Onsite 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).	<p>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.</p> <p> Note: Gallery/Camera Roll Images are shared at their native resolution when the High-res button is pushed.</p>
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	<input type="checkbox"/> 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.	<p>This capability is ideal in situations where picture quality is more important than motion.</p> <p> Note: This setting requires that Onsite Connect Users download and install the latest Onsite Connect software and that they enable the Wait for refresh on packet loss setting. Within Onsite Connect, click SETTINGS > CALLS > Video and enable the Wait for refresh on packet loss option.</p>
Media Path	{ApplicationData}	Sets the default path for Onsite 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)	<input type="checkbox"/> Disabled*	Users can enter their login credentials to allow auto login when the app launches.	Not recommended for users who share devices.

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

Settings	Value	Description	Best Practices/Tips
Run at Windows startup	<input type="checkbox"/> Disabled*		
SIP			
SIP messaging	TCP*	The default transport for the SIP protocol.	
Support SIP UPDATE method	<input checked="" type="checkbox"/> Enabled*	A SIP compatibility feature used by some SIP Servers to update session parameters.	
Verify SIP TLS Server	<input checked="" type="checkbox"/> 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	<input type="checkbox"/> Disabled*	Required for compatibility with WebEx CMR.	When placing the Onsite 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, Onsite will immediately call back to connect to WebEx with the supported call parameters.
Force Media Relay	<input checked="" type="checkbox"/> 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	<input type="checkbox"/> Disabled*	When enabled it allows the Administrator to set the Maximum allowed Video bit rate for Media configurations on an endpoint.	

Table 15-6 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 Onsite 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	<input checked="" type="checkbox"/> 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 bandwidth 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 Onsite Collaboration Hub or with the 5000HD multi-port adapter.

Table 15-6 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	<input checked="" type="checkbox"/> 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	<input type="checkbox"/> 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	<input type="checkbox"/> 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	<input type="checkbox"/> 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 15-6 Client Policy — Best Practices (continued)


Settings	Value	Description	Best Practices/Tips
Push Notifications	<input checked="" type="checkbox"/> 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 Onsite Connect to be battery optimized by an Android device, if Push Notifications are disabled, Onsite 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.	<p>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 Onsite to remove it from the list of battery optimized apps on the device.</p> <p> 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.</p>
Encryption Mode	Auto*	The default should be Auto, this ensures that all Onsite 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	<input checked="" type="checkbox"/> 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)	<input checked="" type="checkbox"/> 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 15-6 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	<input checked="" type="checkbox"/> Enabled	Default On or Off	
Save Call Transcript	<input type="checkbox"/> Disabled*	Default Enabled	Enables all calls to be transcribed in the (Default) language.
Require consent for remote video sharing requests	<input type="checkbox"/> 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 Onsite call. Video privacy is enhanced at sensitive locations by requiring users to provide consent before sharing video.
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	<input checked="" type="checkbox"/> 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.	
Allow HTTP registration	<input type="checkbox"/> 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)	<input type="checkbox"/> 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.

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





Settings	Value	Description	Best Practices/Tips
Workspace			
Access	<input checked="" type="checkbox"/> Enabled*	Authorizes access to Onsite Workspace for the members of the group.	Only enable Onsite Workspace when users need to upload, view, and edit files when using Onsite 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	<input type="checkbox"/> Disabled*	When enabled any files captured during an onsite 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.
Restrict Upload Folder Access to Owner	<input type="checkbox"/> 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 Onsite 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	<input type="checkbox"/> 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 Onsite Workspace providing all required licenses and AI settings are correct.	Enabled.

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

Settings	Value	Description	Best Practices/Tips
Display Transcription Sentiment	Disabled	When enabled, sentiment analysis will display at the line level and for the complete transcript within Onsite 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.
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.
Auto Tag Images	<input type="checkbox"/> 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 15-7 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*	
Support SIP UPDATE method	Deny*	Allow*	Inherit*	Inherit*	Inherit*	

* All default values are marked with an asterisk.

Table 15-7 Client Permissions — Best Practices (continued)

Settings	Action					Best Practices/Tips
	Domain Defaults	Client Administrators	Standard Users	External Guest Users	Domain License Group	
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 15-7 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 Onsite 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-Onsite 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 15-7 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 Onsite 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 \(on page 75\)](#)

Index

Numerics

- 10/100 Ethernet 9
- 160 Characters Limit 76
- 443 9
- 5000HD 74, 75
- 802.11 a/b/g/n 9

A

- Access 71
- Access to Content 49
- Account 50
- Account Activation Method 59
- Account Created 83
- Account Deleted 83
- Account Expiry 25, 25
- Account Lockout Duration 59
- Account Owner 13, 13, 29, 50, 51, 51, 60
- Account Pool Type 70
- Account Registered 83
- Account Registered (HTML, Text) 99
- Account Type 25, 30
- ACS URL 61
- Action 75
- Active 73, 87
- Active Personal Data 54
- Active Users 11
- Add Members 33
- Add Selected Members 33
- Add to Contacts 14
- Add to List 46
- Add Users 25
- Adding/Removing External Contacts from Lists 46
- Adding/Removing Group Members 33
- Additional Administrators 30
- Address 43
- Address (SIP) 89
- Administration Privileges 30
- Administrator 13, 16, 23, 25, 30, 49
- Administrator Email 73
- Administrator must approve accounts register using the Self Registration Page 59
- Administrators 13, 60
- Advanced Reporting 53
- Advanced Reports 71
- AI Setting profile 84
- AI Setting Profile 84
- AI Setting Profiles 84
- AI settings 84
- All 87
- All Contacts 45, 45
- All Countries 94
- All Users 75, 78, 94, 94
- All Users Group 21
- Allow 35, 79, 80, 81
- Allow Cellular/Mobile Data Usage 71
- Allow New Contacts 25
- Allow Setting User Mode while inviting guest 77
- Allow text message guest invitations 76
- Allow users to invite external guest 76
- Allow users to invite guests 30
- Allowed Email Domains 59
- Always use TeamLink 52
- An absolute URI 28
- Android 28, 75
- Android devices 52
- Android Google Play Store 28
- Android smartphone 80
- Anonymize active user data 54
- Anonymize previously deleted users from your domain 54
- Anonymized 54
- Anonymized Data 54
- Anonymized Users 87, 89
- Anonymous Data 54
- Anonymous Data is Not Reversible 54
- Any 94
- API Generated Key 84
- API Key 92
- API Key Expires 83
- API Key Management 52, 52
- API KEYS 83
- API Users 92
- APIs 51
- App stores 75
- App Stores 75
- Application Programming Interface Keys 83
- Application Programming Interfaces (APIs) 52
- Apply Filter 87, 89, 92, 92, 96
- Approval Confirmation Email 42
- Artificial Intelligence (AI) 53
- Artificial Intelligence (AI) Settings 84
- Assets 19
- Assign / Restore SIP Account 25
- Assign Users to a Group 31
- Assign/Restore SIP Account 71
- Assign/Restore Workspace Account 71
- Assigning an Administrator to a Group 31
- Assigning Group Administrators 34
- Assigning Licenses 38
- Assignment Pool Type 70
- Attribute 63, 64, 64, 65
- Attribute Name 64, 64, 65
- Audio Codec 89
- Audit Capabilities 71
- Audit Content 71
- Audit Trail Requirements 71
- Authenticated 49
- Authentication 55
- Authentication Data 61
- Authentication Name 70, 70
- Authentication Password 70, 70, 70
- Authentication User Name 70
- Authorization Data 61
- Authorized 49
- Authorized Teams 71
- Auto Upload Media 71
- Auto-assignment Pool 69
- Auto-Assignment SIP Pool 25
- Auto-generate username 65
- Auto-tagging of Images/Video 54
- Automate The Login Process 27
- Automatic Updates 75
- Automatic Upload 71
- Automatic Versioning 71

Automatically assign a SIP account to this user 16, 25, 71
Automatically assign SIP accounts to new users 38, 39
Automatically assign SIP accounts to self-registered users 70
Automatically assign SIP Accounts to self-registered users 68
Available Connect Enterprise licenses 11
Available for Use 101
Available Licenses 21
Available Workspace Enterprise licenses 11
Average Duration 94

B

Back-office Systems 71
Bandwidth Control 52
Batch Frequency 73
Between 94
Both 96, 96
Button Styles 101

C

Call 96
Call Details 89
Call Duration 94
Call History 94
Call Librestream Support 50
Call Reports 94
Call Services 49
Call Setup 89
Call Statistics 53
Called Participant 89
Called User 89
Callee 96, 96
Caller 96, 96
Calling Altitude 89
Calling Latitude 89
Calling Participant 89
Calling User 89
Calls 89
Calls or Logins Quantities 96
Capture Content 19
Capture Mode 20
Capture Mode is no longer available 20
Captured Images 20
Captured Recordings 20
Category Section 78
Cell Towers 96
Cellular Carrier 89
Cellular Data Consumption 71
Challenge code 42
Change Account Owner 50, 51
Change Account Type 31
Change Password 13
Change Passwords 30
Change Settings 30
Check for Updates 75
Chinese (Simplified) 99
Choose Settings 35, 71, 78
Cisco VCS Expressway 69
Clear 75
Client Activity 87, 94
Client Activity Report 87
Client Administrator 25
Client Administrator Group Policy 25
Client Functionality 51, 52
Client Permissions 21, 23, 30, 33, 35, 53, 75, 79, 80, 80, 81
Client Policy 21, 21, 21, 23, 25, 30, 30, 33, 35, 49, 52, 52, 53, 56, 58, 71, 75, 78, 78, 79, 80, 81, 82, 101, 102
CLIENT POLICY 78
Client Policy Group 25

Client Settings 16, 25, 30
Collaborate 19
Collaboration Hub 74, 75
Column Headings 38
Comma Separated Value File (CSV) 38
Comma Separated Value list 59
Commit the Changes 49
Common Actions 13, 25, 27, 29, 31, 33, 34, 50, 50, 51
Company Name 50
Computer Vision (CV) 53
Computer Vision API 84
Conference Hosts 52
Configuring Your IdP Settings 61
Confirmation 76
Connect Enterprise 19, 19, 25, 39, 51, 89
Connect Enterprise License 16
Connect Enterprise with Workspace Contributor) 19
Connect Enterprise with Workspace Enterprise 19
Consent 81
Consumer URI 73
Contact List 56
Contact Lists 21
Contact Support 105
Contact Support QR Code 105
Contacts 14, 14
Contacts Lists 43
Contacts.csv 39
Contacts.xml file 39
Content 19, 71
Content Privacy 52, 52
Content Tagging 71
Contributor 19
Contributor license 71
Control Recording 52
Count of Client Connections 96
Country 16, 25, 25, 94, 94
Create a Duplicate 44
Create a New User 25
Create An External Contacts List 45
Create and Delete Users 30
Create New Contact List 45
Create New User 25, 25
Create Users 21
Created date 33
Creating New Users 38
CSV 41, 43, 63, 87, 89, 92, 94, 94, 96
CSV File 39
CSV Import Instructions 43
Cube 7, 20
Custom Email 53
Custom Field Name 57
Custom Field Value 57
Custom Fields 55, 57, 77, 94, 94, 94
Custom License Groups 21
Custom Media Configurations 53
Custom Message 101
Custom Messages 53, 101, 102
Custom Messages Help 83
Customer Created 50
Customer Defined Tags 83
Customer Domain 13, 50
Customer Expiry date 50
Customer Portal 68
Customization 53, 83

D

Dashboard 11, 13, 13, 19

- Data Anonymization 54, 94
- Data Anonymization of PII 54
- Data Privacy Compliance 54
- Data Retention Period (DRP) 54, 94
- Deactivate guest user account when removed from contact list 77
- Decline 81
- Default 76
- Default Authentication Type 69
- Default Contacts 38
- Default Language 55
- Default License Group 21
- Default Time Zone 55
- Default Transport Type 69
- Delete Group 33
- Deny 35, 79, 80
- Deny Super Administrator Access 50
- Department 16, 25
- Deploying Server Certificates 68
- Deploying Update Packages 75
- Description 23, 33, 73, 79, 83, 84, 84, 92
- Detailed Permission Controls 71
- Details 92
- Device Type 89
- Digest Algorithm 61, 62
- Digital Signature 68
- Disable global directory access 76
- Disabled 81
- Domain 21, 21, 41
- Domain Control 21
- Domain Level Configuration 76
- Domain License Group 16, 25
- Domain license management 21
- Domain Policy Group 16
- Domain Settings 30
- Don't show again 101
- Download 27, 29
- Download for iOS 28
- Download for Windows 28
- Download Import Template 38, 44
- Download SP Certificate 61, 68
- Duplicate Handling 44
- Duration 87, 89, 89, 89

E

- Edit 19, 84
- Edit Client Policy 75
- Edit Client Policy and Permissions 35
- Edit Group 31, 33, 35
- Email 16, 25, 42, 64
- Email Address 54, 63, 64
- Email addresses 29
- Email Customization 83
- Email Mapping 63, 64
- Email Requirements 29
- Email Verification Confirmation page 42
- EmailAddress 38
- Emails originating from OPM 99
- Enable Self Registration 59
- Enabled 76, 81
- Enabling Workspace Access 71
- Encrypted 89
- Encryption mode 78
- End Date 87, 89, 96
- End User License Agreement (EULA) 103
- Endpoint 52, 84
- English 99

- English Only 99
- Enterprise Customers 60, 61
- Enterprise license 71
- Enterprise security policy 9
- Enterprise SIP Account information 70
- Enterprise SIP server 70
- Enterprise SIP Server 69, 70
- Enterprise User 19
- Enterprise Users 39
- Entity ID 61, 61, 62
- Error 92
- Europe 54
- Event 73
- Event Log 92, 92
- Events 54, 73, 92
- Events Report 92
- Everything 37
- Expert Mode 52, 77
- Experts 52
- Expired Users 11
- Expiry 77
- Expiry Date 25, 83
- Export 39, 43, 87, 89, 92, 94, 96
- Export External Contacts 43
- Export SP Metadata 61
- Export Users 41
- Exported User Report 57
- Extended key usage set 68
- External Contact 43
- External Contact List 43
- External Contacts 38, 39, 43, 45, 46, 56
- External Contacts are public by default 56
- External Contacts list 46
- External Contacts List 44
- External Contacts page 44
- External Guest Confirmation 83
- External Guest Global Settings 55
- External Guest Invitation 83
- External Guest Invitation Defaults 77
- External Guest Invites 75
- External Guest User Permissions 49
- External Guest Users 11, 49, 51, 55, 56, 60, 76, 78, 83, 87, 89, 92, 94
- External Guests 30
- External or Third-Party Video Endpoints 56
- ExternalContacts.CSV 44

F

- Fatal 92
- Federated SSO Id 63
- Federated SSO ID 16, 39, 63, 64
- Federated SSO ID mapping 63
- Federated SSO ID Mapping 64
- Field Mode 52, 77
- File to Import 38, 39
- File Upload 39
- Filter Parameters 87, 87, 89, 92, 92, 94, 94, 96
- Filtered 37
- Firewall 52, 69
- Firewall Entry 96
- First Name 16, 25, 42, 65
- First-time Login 9
- FirstName 38
- Forgot Password 99
- Frame 89
- French 99
- From Email Address 77

Full 83

G

General 68
General Data Protection Regulation (GDPR) 54
Generate Key 83
Generate Temporary Password 16
Generating a Report 94
German 99
Global Contacts Directory 76
Global Directory 14, 33, 36, 37, 43, 43, 55, 56, 76
Global Directory Availability 37
Global Directory Availability Filters 37
Global Directory Filter 37, 38
GOP 89
Grant Access 59
Greater Or Equal 94
Green 76
Group 38, 78, 79
Group Administrator 25, 30, 31, 31
Group Administrator Permissions 30
Group Administrators 33, 33, 34
Group Client Permissions 80
Group Client Policy 71, 80
Group Details 33
Group Level Settings 30
Group membership 75
Group Permissions 30
Group Policy 30, 75
Group Type 23
GroupMembership 38
Groups 94, 94
Guest invite Status 76
Guest Invite Summary 94
Guest User Behavior 76
Guest User Confirmation (Text) 99
Guest User Invitation (HTML, Text, SMS) 99
Guest Users 29
Guest Users API 52
Guests 57

H

Hardware 89
Heat Map 96
Heat Map For 96
Heat Map Report 96
Historical Trends 94
Host Name 87
Hosted Features 51, 53
Hosted SIP Service 69
How Many Calls 94
HTTP Basic Authentication 73
HTTP Callbacks 73
HTTP Headers 73
HTTPS 9, 9, 55
HTTPS network protocol 9
HTTPS Tunneling of Data 52
Hub 7, 20

I

Identity Mapping 39, 63
Identity Provider (IdP) 60, 61
IdP Certificate 61, 61
IdP metadata 61
IdP Metadata 61
IdP Metadata file 61
IdP Public Certificate 61
If a valid email is configured 29

IIS configuration 9
Images 19
Import 39, 43, 44, 44
Import File 38
Import From File 44
Import IdP Metadata 61
Import Mode 39
Import Results 39, 44
Import Template 38, 39
Import Users 39, 44
Import Users from a File 25
Imported User list 63
Importing a Users Import Template 38
Importing Metadata 61
Improve Reporting Data 57
Include anonymous records 94
Include option for guest to call host immediately 77
Individual Members 38
Individuals 71
Information 92
Inherit 35, 75, 79, 80
Initial Password 42
Insert Default Template 83
Install 27, 29
Instrument Visualization 54
Internal 69
Internet of Things (IoT) 54
Invite An External Guest 49
Invite Email 60
iOS 75, 80
iOS App Store 28
IoT Device API 84
IoT Measurement API 84
IoT services 54
IoT Services 84
IP Address 87, 96
iPhone 7
Italian 99
Item Created 73
Item Deleted 73
Item Modified 73

J

Japanese 99

K

Key 59
Key Encipherment 68
Knowledge Management 71
Korean 99

L

Language 16, 25
Last Activity 87
Last Modified 33
Last Name 16, 25, 42, 65
LastName 38
Latest Published Version 75, 75
Least Usage 94, 94, 94
Less Or Equal 94
Librestream Support 50
License and Overall Usage Summary 94
License and Policy Group Management 21
License Features 51
License Group 21, 23, 39
License Group for New Users 39
License Group Management 21
License Group Membership 25, 25

- License Groups 25, 30, 51
- License Options 19
- License totals 33
- License type 25
- License Types 21, 39
- License Usage Summary 94
- Licensed Add-on 61
- Licenses 13, 49, 50, 51, 52, 52, 59
- Limit 89
- Local Service Provider 61
- Local Service Provider Certificate SHA1 68
- Local Service Provider Settings 62
- Locally Authenticated for 30 Days on the Client 49
- Location and Quantity Of Calls/Logins 96
- Lock 84
- Login 14, 20, 29, 49, 96, 101, 102
- Login Policy 57, 59
- Login Time 87
- Login to Onsite Connect 27, 28
- Loss of Network Connectivity 49

M

- Make Calls 19
- Manage 19
- Manage Data 71
- Manage External Contacts 45
- Manage Images 71
- Manage Privacy Settings 78
- Manage Recordings 71
- Manage User Licenses 21
- Manage Users 23, 33, 33, 34
- Managing group administrators 31
- Manual Upload 71
- Manually Add a Group 23
- Manually Add An External Contact 43
- Manually Assigning SIP Accounts 71
- Manually Configure Your IdP Settings 62
- Manually Create a New User 25
- Mapped IdP Attribute 39, 63, 63, 64, 64
- Master License 30
- Maximum Bad Login Attempts 59
- Maximum Upload Bit Rate (Kbps) 71
- Maximum Video Bit Rate 52
- Media 52
- Media Configurations 52
- Member Of 39
- Membership Type 33
- Mentorship/Coaching 94
- Merge Groups 39
- Message 101
- Message Options 101
- Microsoft Excel 38
- Minimum Capital Letters 58
- Minimum Length 58
- Minimum Non-Alpha Characters 58
- Mobile Client Link 66
- Mobile Device 20
- Modify Group 33, 34, 35, 71
- Modify Users 30
- Multiparty Calling 52
- Multiple Accounts 69, 69, 70, 70, 70
- Multiple Administrator Accounts 13
- Multiple Groups 75
- Multiple License 19
- Multiple Participants 52
- Multiple SIP Accounts 70
- My Profile 13

N

- Name 23, 33, 43, 45, 73, 83, 84, 84, 89
- NameID 63
- Natural Language Processing (NLP) 53
- Natural Language Processing API 84
- Network Access is Not Available 60
- Network Interface 89
- Network Requirements 9
- New Contact 43
- New Group 23
- New List 43, 45
- New Release Notifications 75
- New User 16, 25, 25
- Next Login 71
- Next Update 71
- None 83
- Notification 11, 59, 65
- Notification Emails 29
- Notify Administrators by email when an account is registered 65
- Notify Existing Users 67, 67
- Number of Licenses Per Type 51
- Number of Results 94

O

- OamClientWebService 28, 28
- OCR API 84
- Offline Login 60
- On Premises 9, 9, 11, 50, 52
- On Premises — Installation Guide 68
- On-premises 68, 73, 75
- On-Premises Welcome Email 27
- Online Service 49
- Onsite 5000HD 75
- Onsite Account Credentials 60
- Onsite Account Domain 51
- Onsite Account Field 63, 63, 64
- Onsite Account Fields 63
- Onsite accounts 42
- Onsite Administrator 42
- Onsite API guides 84
- Onsite Augmented Reality Platform Architecture 7
- Onsite Call 20
- Onsite Call API 52
- Onsite Call Services 19
- Onsite Client 56
- Onsite Collaboration Hub 75
- Onsite Collaboration Hub Updates 52
- Onsite Connect 42, 60
- Onsite Connect client 7
- Onsite Connect Client 13
- Onsite Connect Endpoint Licenses 13
- Onsite Connect for Windows 99
- Onsite Connect Viewer 20
- Onsite Credentials 60
- Onsite Cube 74, 75
- Onsite domain 50
- Onsite Domain Name 61
- Onsite Endpoint 43, 75
- Onsite Endpoints 49
- Onsite Mobile Client Updates 75
- Onsite Platform Manager — Installation Guide 75
- Onsite Platform Manager Administrator Privileges 51
- Onsite Platform Manager's URL 27
- Onsite Smart Camera 80
- Onsite Translator 53
- Onsite User Account 69

- Onsight User Accounts, 39
- Onsight Users 51
- Onsight Users section 51
- Onsight Workspace 71
- Onsight Workspace Webhooks Guide 73
- Open Standard 61
- OpenOffice Calc 38
- Operating System 89, 89
- OPM Administration login 9
- OPM Administrator 51, 75
- OPM host and path 28
- OPM host only 28
- OPM Manuals and Guides 80
- OPM Reports and Call Statistics 54
- OPM scheme and host 28
- OPM.com\user@domain 27
- Optional 29, 60
- Overall Usage Summary 94
- Override the Password of Existing Users 39
- Override, 75
- Overwrite Groups 39

P

- Parameters 84
- Participant Type 96
- Partner Identify Provider setting 61
- Partner Service Provider 61
- Partner Service Provider Settings 61
- Password 9, 13, 27, 70, 73, 76
- Password Changed Confirmation 83
- Password Expiration 57
- Password Policy 57, 58
- Password Reset Request 83
- Password Reset Request (Text, SMS) 99
- Passwords 38
- Permission Controls 71
- Personal Identifiable Information (PII) 54
- Personal Settings 13, 13, 14
- Policy Group 23, 25, 25, 25
- Policy Group Membership 25, 39
- Policy Groups 25
- Policy Precedence 78
- Portuguese (Portugal and Brazil) 99
- Potential Leaders 94
- Precedence 75
- Primary Administrator 13
- Primary SIP Account 69
- Print 96
- Privacy Settings 81
- Private 37, 45, 69, 70
- Private Server 69, 70
- Private SIP Server settings 38
- Profile 16, 25, 29, 57
- Promoting a Standard User 31
- Prompt 29
- Prompt on First Login 65
- Public 37, 45, 69, 70
- Public Internet 96
- Public Internet Access 52
- Public Server 69, 70, 70
- Public SIP Settings 69

Q

- Quick Search And Retrieval 71

R

- Re-authenticate 49
- Read 83
- Read/Write access 83
- Recording 102
- Recordings 19, 101
- Red 76
- Refresh 89
- Region 16, 25
- Register for an Account 99
- Register For An Account 42
- Registration Key 59
- Remember Me 27
- Remote Endpoints 9
- Remote Video Privacy 81
- Remote Video Sharing Requests 81
- Remove Contact from List 46
- Remove Members 33
- Report Name 94
- Reported Time 89
- Reports 94, 94
- Require Email Address for Self-registered Accounts 59
- Require Email Address for Self-Registered Accounts 29, 65
- Require Encrypted Assertions 61, 62
- Require Signed Assertions 62
- Require Signed Responses 61
- Require Signed Responses. 62
- Required 60
- Required Email 59
- Required Signed Assertions 61
- Resend Welcome Email 29
- Resend Welcome Message 27
- Reset Changes 49
- Reset Password 99
- Resolution 89
- REST API Endpoints 84
- Restrict Upload Folder Access to the Owner 71
- Results 94
- Right to be Forgotten (RTBF) 54
- Run Report 94
- Russian 99

S

- SAML Assertion 63
- SAML Configuration 60, 61, 61, 61, 62, 62, 63
- SAML encryption 68
- SampleUserImport.csv 38
- Save 49
- Scheduled Anonymization 54
- SCIM API 52
- Screen Sharing 52
- Search 14
- Secure Architecture 71
- Security 49, 57, 58, 59, 69
- Security and SSO Settings 29
- Security Assertion Markup Language (SAML) 60
- Security Assertion Markup Language Configuration 61
- Select All Rows 67
- Self Registration 57, 59
- Self Registration URL 59
- Self-registration 25
- Self-Registration 68
- Self-Registration Auto-Assignment 68
- Self-Registration Key 42
- Self-registration page 29
- Self-registration Page 42
- Self-Registration Web Page 25
- Send Instructions 60, 67
- Send User Notification if Password Changes 39
- Send Welcome Email 16

- Send Welcome Email if Email Address Changes 39
- Send Welcome Email to New Users 39
- Server Address 70, 70
- Server Setting 68
- Service Provider (SP) 61, 61
- Session Initiation Protocol (SIP) 7, 14, 68
- Setting Client Permissions 79
- Setting Client Policy 78
- Settings 29, 49, 50
- Setup 50
- Severity 92
- SHA1 thumbprint 68
- Share Audio 7
- Share Content 19
- Share Data 71
- Share Images 7, 71
- Share Recordings 71
- Share Video 7
- Shared Account 69, 69, 70, 70, 70
- Short Message Service 82
- Sign Authentication Requests 61, 62
- Sign-on Binding type 62
- Signature Algorithm 61, 62
- Single License 19
- Single License Pool 21
- Single Sign On 60
- Single Sign ON 60
- Single Sign On (SSO) 16
- Single Sign-on URL 62
- SIP 25, 49, 52, 82
- SIP Account 68, 70
- SIP Account Information 70
- SIP Accounts 69
- SIP ACCOUNTS 68
- SIP Address 14, 69
- SIP Capable Device 43
- SIP Domain 70
- SIP Pool 70, 70
- SIP ports 52
- SIP Server 69, 69, 70
- SIP Server Address 70
- SIP Server Administrator 70
- SIP Server Set Up Options 69
- SIP Session ID 89
- SIP Settings 39, 70
- SIP URI 14, 70
- SIP URI Domain 69, 69, 70, 70
- SIP URI format 43
- SIP URI Format 43
- Site Administration 68
- Skip Duplicates 44
- Skip Duplicates (Keep Existing Records) 39
- Smartphones 99
- SMS 53, 53, 60, 82
- SMS API 82
- SMS Customization 83
- SMS guest invites 82
- SMS Max Message to User Length 76
- SMS Message 76
- Software 49
- Software Distribution 74
- Software Updates 74, 75
- Software Updates Page 75
- SP Certificate 61
- Spanish 99
- Special Cases 38

- Specific Version 75
- Spreadsheet Application 38
- SSO 38, 39, 53, 60, 60, 62, 63, 63, 64, 64, 65, 66, 67, 99
- SSO Attribute 29
- SSO binding 61
- SSO Certificate Setup 68
- SSO Client Login 66
- SSO Credentials 65
- SSO Domain 61
- SSO Enabled Instructions 83
- SSO Identify Provider 61, 61
- SSO Identity Provider (IdP) 61
- SSO Self Registration 65
- SSO Settings 39
- SSO URL 61
- SSO Users 29
- Standard User 25, 30, 30, 31
- Standard User Permissions 30
- Standard Users 60, 87, 89, 92, 94
- Start Date 87, 89, 96
- Start Time 89, 89
- State 87
- Statistics 89
- Statistics and Events 89
- Still Image Capture 52
- Stream Start 89
- Subject Name ID 63
- subscription-based service 7
- Super Administrator Access 50
- Super Administrator Access status 50
- Super Administrators 50
- Supported File Formats 43
- Swedish 99
- System Notifications 38

T

- Tablets 99
- TCP 9, 69, 69, 70, 70
- TeamLink 52, 89
- TeamLink firewall traversal capabilities 52
- TeamLink Registration 52
- Telestration 7
- Temporary Administrator 16
- Termination Reason 89, 89
- Terms of Use 101
- Third-party Video Endpoint 7
- Third-party Video SIP Endpoints 43
- Time 92
- Time Stamp Data 55
- Title 101
- TLS 69, 69, 70, 70
- Top and Least Usage 94
- Top Usage 94, 94, 94
- Total and Available Licenses 11
- Total Connect Enterprise licenses 11
- Total Duration 89, 94
- Total Users 11
- Total Workspace Contributor licenses 11
- Total Workspace Enterprise licenses 11
- Trigger 101
- Troubleshooting 50

U

- Unique Authentication Name 70
- Unique SIP URI 70
- Universal Time Coordinated (UTC) 55
- Update existing records 39
- Update Existing Records 44

- Updates 75
- Upload 39, 44, 61
- Upload Content 19
- Upload Data 71, 71
- Upload Folder 19
- Upload IdP Certificate 61, 61
- Upload Images 71
- Upload Path 71
- Upload Recordings 71
- URI 70
- URL 9, 59
- Usage Statistics 41, 94
- User 87, 92
- User Account 55
- User Account Expires 25, 25, 25
- User Account Types and Permissions 30
- User and Groups 71
- User Client Policy 75, 75, 75
- User Expiry 51
- User Identity Federation 60, 62, 63, 64, 65, 66
- USER Identity Federation 63
- USER IDENTITY FEDERATION 64
- User Identity Mapping 64
- USER IDENTITY MAPPING 64
- User licenses 19
- User Management 30
- User Mode (Expert/Field) 52
- User Name 9, 16, 27, 42, 63, 65, 89
- User Name/ 73
- User Password Changed (Text, SMS) 99
- User Provisioning Links 66
- user@domain.com 9
- user@sipdomain.com 14
- Username 31, 54, 63
- UserName 38
- Username Mapping 63, 63
- Users 11, 16, 23, 25, 25, 41, 55
- USERS 31
- Users and Groups 56
- Users Awaiting Approval by an administrator 11
- Users Client Settings 25
- Users Import template 38

V

- Value 35
- Verify your Email Address 42
- Version 87
- Video Bit Rate 89
- Video Codec 89
- Video Conference Rooms 43
- Video Privacy 81
- Video Sharing 81
- View Data 71
- View Images 71
- View Recordings 71
- View Report 44
- Visualization 54
- Voice Codec 89

W

- Warning 92
- Web Proxy 9
- Web Service interface 9
- WebEx CMR Compatibility 82
- WebEx Meeting Rooms 82
- Webhook Configuration 73
- Webhook Notification Mechanism 73
- Welcome Email 9, 16, 27

- Welcome Emails 75
- Welcome Message 28
- Welcome to Onsite email 42
- Wild Card Sip Accounts 70
- Windows 74, 75, 75, 99
- Windows Client Download 66
- Windows PC 7, 20, 80
- Windows PCs 52
- Windows Users 75
- Wired Network 9
- Wireless Network 9
- Workspace 20, 83
- Workspace Access 19
- Workspace Account 54
- Workspace API 52, 71
- Workspace Assets 73
- Workspace Contributor 19, 25, 39, 51
- Workspace Contributor) 19
- Workspace Data Collection 71
- Workspace Enterprise 19, 19, 25, 39, 51
- Workspace Enterprise License 71
- Workspace Key Features 71
- Workspace License Types 19
- Workspace server 71
- Workspace Webhooks 73

Y

- Yellow 76