



ONSIGHT PLATFORM MANAGER ADMIN GUIDE



Librestream
Onsight Platform Manager Guide
Doc #: 400199-24, rev. E

v11.4.6
November 2021

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 © 2004-2021 Librestream Technologies, Incorporated.
All rights reserved.

Name of Librestream Software Onsight Connect

Copyright Notice: Copyright 2004-2021 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 Hub, Onsight Smartcam, Onsight Platform Manager and Onsight Tealink 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

OVERVIEW	5
ONSIGHT AUGMENTED REALITY PLATFORM ARCHITECTURE	5
NETWORK REQUIREMENTS	5
FIREWALL CONFIGURATION	5
LOGGING INTO OPM FOR THE FIRST-TIME	5
DASHBOARD	6
ADMINISTRATOR'S SETTINGS	6
CHANGING THE ADMINISTRATOR'S PASSWORD	6
CHANGING THE ADMINISTRATOR'S PERSONAL CONTACTS.....	6
ADDING ADMINISTRATORS TO OPM	6
USER LICENSES	7
LICENSE OPTIONS	7
CAPTURE MODE	7
MANAGING USERS AND GROUPS	7
DOMAIN LICENSE AND POLICY MANAGEMENT.....	7
LICENSE GROUP MANAGEMENT.....	7
CREATING USERS AND GROUPS	8
ADDING USERS AND GROUPS	8
ADD A GROUP	8
ADD A USER.....	8
WELCOME EMAIL	9
ON PREMISES - URL FORMATS	9
USER EMAIL REQUIREMENT	10
USER ACCOUNT TYPES AND PERMISSIONS	10
CREATE AND ASSIGN GROUP ADMINISTRATOR	10
EDIT GROUPS.....	10
ASSIGN GROUP ADMINISTRATORS	10
ADD OR REMOVE GROUP MEMBERS	11
EDIT CLIENT POLICY AND PERMISSIONS.....	11
GLOBAL DIRECTORY	11
GLOBAL DIRECTORY AVAILABILITY	11
GLOBAL DIRECTORY FILTER	11
DEFAULT CONTACTS	11
IMPORT/EXPORT USERS	11
CREATE AN IMPORT FILE.....	11
IMPORT FILE - BEST PRACTICES.....	12
IMPORT USERS	12
SELF-REGISTER USERS.....	13
EXTERNAL CONTACTS	13
ADD AN EXTERNAL CONTACTS LIST	13
ADD/REMOVE EXTERNAL CONTACTS FROM LISTS	13
SETTINGS	13

ACCOUNT	14
USERS.....	15
SECURITY	16
SSO	16
SIP	18
SIP SETTINGS	18
SIP ACCOUNT.....	18
ONSIGHT WORKSPACE.....	19
WORKSPACE WEBHOOKS	20
CLIENT POLICY AND PERMISSIONS	21
GROUP CLIENT POLICY AND PERMISSIONS.....	23
SMS.....	23
CUSTOMIZATION	24
API KEYS.....	25
AI SETTINGS	25
STATISTICS AND EVENTS.....	26
CLIENT ACTIVITY	26
STATISTICS	26
EVENTS.....	26
REPORTS	27
HEAT MAPS.....	27
LANGUAGE SUPPORT	28
CUSTOM MESSAGES	28
CUSTOM MESSAGES - FORMS.....	28
CUSTOM MESSAGES - CLIENT POLICY	28
END USER LICENSE AGREEMENT.....	29
CONTACT SUPPORT	29

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:

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

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.

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

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.

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/

NETWORK REQUIREMENTS

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

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.

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 1

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.

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

LOGGING INTO OPM FOR THE FIRST-TIME

You will receive your OPM Administration login information from Librestream via 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:

User Name: user@domain.com
Password: Password

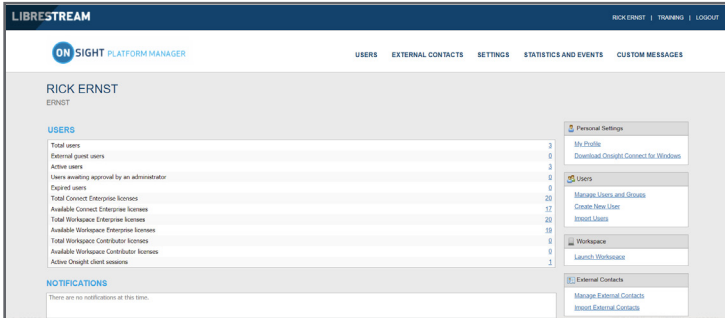
To avoid unauthorized access to the software, you should change this password immediately after logging in for the first time, as described in Changing the Administrator's Password in paragraph 4.1.1, on page 8.

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

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.

DASHBOARD

The dashboard includes the table of user totals, a list of notifications and links.



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

ADMINISTRATOR'S SETTINGS

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, **My Profile** allows 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.

CHANGING THE ADMINISTRATOR'S PASSWORD

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

CHANGING THE ADMINISTRATOR'S PERSONAL CONTACTS

1. Go to **MY PROFILE**.
2. Choose the **CONTACTS** tab.
3. Click the **Global Contacts** button to search for a contact to add to your Contacts list.
4. Enter a name to search and press the search button; or you may just press the search button to see a list of all users.
5. To Enter a contact manually, click the **New** button. This is only necessary if you need to add a 3rd party contact.
6. Enter the Name, Address, and Type for the contact. You may enter an optional Address 2. Note: the address must be in the SIP URI format, e.g., user@sipdomain.com.
7. Click **OK** to save.

ADDING ADMINISTRATORS TO OPM

As the OPM Administrator you can add additional Administrator accounts. The additional Admin accounts will not consume licenses unless you specifically assign a license to the administrator accounts.

To add additional Administrators:

1. Select the **USERS** tab.
2. Press the **New User** button.
3. Enter the **PROFILE** settings:
 - User Name
 - First Name
 - Last Name
 - 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 uncheck **Generate Temporary Password**. You will need to notify the new admins of their User Names and passwords.
 - 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. **Automatically assign a SIP account to this user** is selected by default. 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.

USER LICENSES

Onsight Platform manager supports 3 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 can not 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).

LICENSE OPTIONS

The following table outlines the valid license type assignment combinations:

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.

CAPTURE MODE

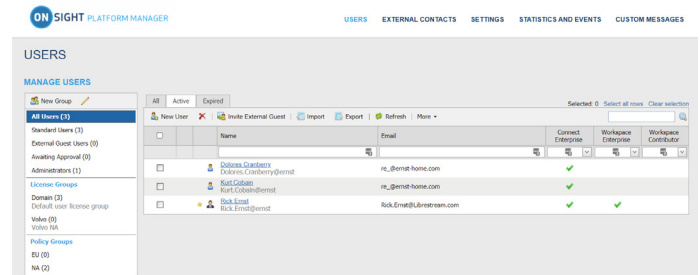
Capture Mode provides offline use of Onsight Connect without requiring a login. From the login screen, users can press the Capture Mode button to enter the Onsight Connect Viewer. This allows access to video sources like mobile device cameras as well as Onsight devices such as the Cube and Hub without 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 get 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 screen. An Onsight login must be used to gain access to the application from that point on.

MANAGING USERS AND 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 enables you to affect:

- Domain license management
- License group management

DOMAIN LICENSE AND POLICY MANAGEMENT

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.

LICENSE GROUP MANAGEMENT

License Group management is an optional method of managing licenses, it is enabled by request only. It allows 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.

CREATING USERS AND GROUPS

OPM administrator can create 2 types of groups: Policy and License.

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.

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

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.

The use of License Groups is optional and must be requested to 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 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, you can set client policy for all users by editing the Standard Users client policy.
- If External Guests is enabled, 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, 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.

There are three ways the Administrator can add Users:

- Manually create a new user.
- Import users from a file (e.g., SampleUserImport.csv).
- Self-registration using the OPM Self-Registration webpage.

The default groups listed in 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.

Default groups cannot be deleted.

ADDING USERS AND GROUPS

ADD A GROUP

1. Select the **USERS** page.
2. To add a custom group, click the New Group button in the MANAGE USERS panel.
 - Enter the Name, Description, and Group Type: Policy or License, then click OK.
 - 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.

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

ADD A USER

1. To add a new user, click the **New User** button. You will be presented with the CREATE NEW USER screen.
Note: If the **New User** button is missing, then you are unable to add new users. Revisit your **Client Policy** setting for **Allow New Contacts** as required.
2. Enter the PROFILE for the user. By default, the **Send Welcome Email** and **Generate Temporary Password** options are selected.
3. Within CLIENT SETTINGS, select the Account Type: **Standard User**, **Administrator**, or **Group Administrator**.
4. 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.

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

Note: both License groups and Policy groups have client policy and permissions 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 **Create New User** button at the bottom of the screen.
- To set a user as Client Administrator, click on the user's name in the list on the USERS page. Select the **Client Administrator** checkbox. The user is now able to edit all settings on an endpoint.

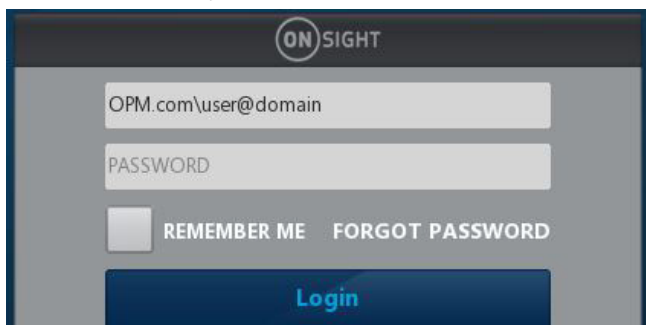
*The Client Administrator setting for user accounts is deprecated. It is recommended that users be added to policy groups to control client permissions. However, users who currently have Client Administrator enabled for their user account can be managed through the Client Administrator group policy.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

WELCOME EMAIL

The Welcome email notifies new users of their Onsight Connect account and how to download and install Onsight Connect. The Welcome message can be resent, if necessary, select the user from the user list. Next, click the More menu and then click Resend Welcome Message.

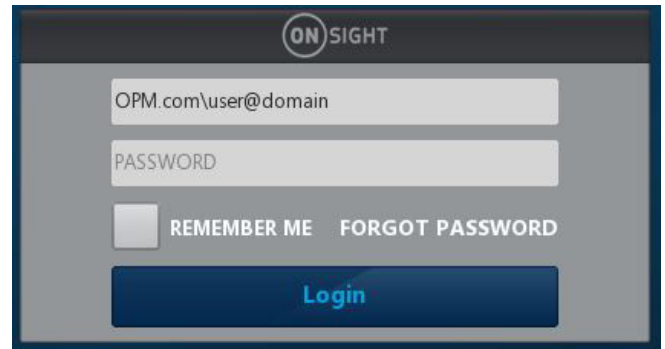
ON PREMISES: Welcome emails will contain a **Login to Onsight Connect link** which will launch Onsight Connect and direct it to your Onsight Platform Manager's URL. The URL in the link will match the URL that was configured during installation your On-premises server installation.

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



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

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



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

ON PREMISES - URL FORMATS

When specifying the OPM path in the user name field at log in, shortened formats are accepted. Typical hardcoded 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:

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

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

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

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

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, 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.

The email requirement for self-registered users (either through the self-registration page or provisioned through SSO), is configurable on the **SETTINGS-SECURITY** and **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. **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. **Require Email Address for Self-registered Accounts** can be unchecked.

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.

USER ACCOUNT TYPES AND PERMISSIONS

The **Account Type** indicates the level of access the User has to Onsight Platform Manager. The licenses assigned to the user determines the features the user has access to in Onsight Connect and Workspace. Client policy and client permissions dictate the users access to settings on the client apps.

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.

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.

CREATE AND ASSIGN GROUP ADMINISTRATOR

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.

1. Assign the user Group Administrator privileges.
 - a. Go to Users and Groups, click on User.
 - b. In the Common Actions area click on Change Account Type.
 - c. Select Group Administrator from the Account Type; click the Change Account Type to apply the change.
2. To assign the group administrator to a Group.
 - a. Go to Users and click on the group to which you wish to assign the group administrator.
 - b. Press the Pencil button to edit.
 - c. In the Common Actions area click on Group Administrators.
 - d. Select the Group Administrator(s) from the list; click OK to apply the change.
 - e. Press Save

EDIT GROUPS

To edit a group, go to the USERS tab and select it in the MANAGE USERS panel. Press the Pencil button to open the edit page.

The group details page lists the following:

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

ASSIGN GROUP ADMINISTRATORS

To assign a group administrator in the Common Actions area.

1. Click on Group Administrators and a list of users with group administrator privileges is displayed.
2. Select the Group Administrator(s) you wish to assign to the group. Press OK.

ADD OR REMOVE GROUP MEMBERS

To assign a group administrator in the Common Actions area.

1. Select the **Members** tab, press add (+) to add members to the group.
2. Select the users you wish to add and press the **Add Selected Members** button.
3. To remove members, select them from the MEMBERS list and press the **Remove Members** button.

EDIT CLIENT POLICY AND PERMISSIONS

1. Select the CLIENT POLICY tab to configure endpoint settings.
 - a. Press **Choose Settings** to add the settings you wish to control. Select the categories and press **OK**.
 - b. Set the Value for each category and press **Save**.
2. Select the CLIENT PERMISSIONS tab.
 - a. Set the action as **Inherit**, **Allow**, or **Deny** for each setting. 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.

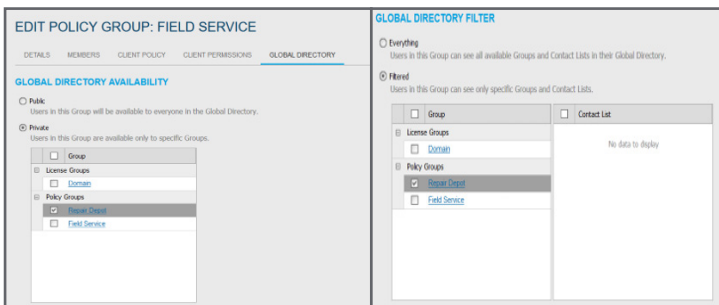
See the Client Policy and Client Permissions section for a detailed description of the actions.

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

GLOBAL DIRECTORY GLOBAL DIRECTORY AVAILABILITY

Global Directory Availability **controls whether the current group is visible** in the Global Directory. (Think of this as, who can search for me?)

1. Select the **Global Directory** tab to view the global directory availability and filter controls.
2. Select **Public** to make the members of the group visible to all groups in the Global Directory.
3. 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.



GLOBAL DIRECTORY FILTER

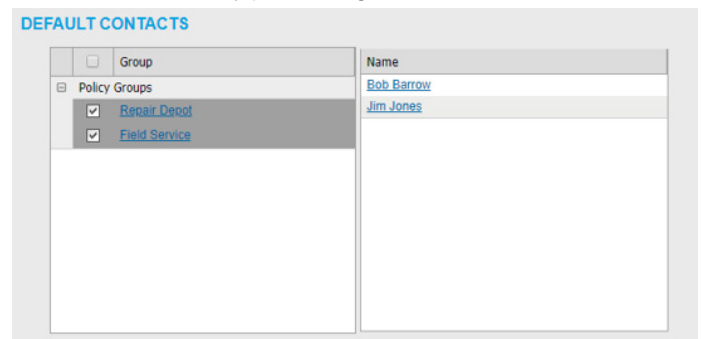
Global Directory Filter **controls who is visible to the current group** in the Global Directory. (Think of this as, for whom can I search?)

1. Select **Everything** if you want the group to be able to view all groups and contacts in the Global Directory.
2. Select **Filtered** to limit search visibility for the current group. Select the groups and contact lists you wish 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.

DEFAULT CONTACTS

Default contacts controls which contacts are automatically included in a group member's contact list when they log into the OnSight Connect application.

1. Select the group or individual members of the group you wish 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.

IMPORT/EXPORT USERS

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

CREATE AN IMPORT FILE

On the USERS page click the Import button.

- To create the OnSight Users file, download the import template by clicking the Download Import Template button.
- Once downloaded, open the file, SampleUserImport.csv.
- Follow the format outlined in the OPM CSV Import Instructions. Sample data is included in the instructions.
- On the Import from File page, click CSV Import Instructions to view the instructions. They provide the CSV file format details and provide examples.

IMPORT FILE - BEST PRACTICES

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

- UserName
- FirstName
- LastName
- EmailAddress (optional but is required when you wish to use system notifications and features such as password change.)
- GroupMembership (this is 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:

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

IMPORT USERS

1. Go to **USERS**, click on **Import**.
2. Select **Users** from the Import Mode drop down list.
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. Select the File to Import; click **Browse** to find the Onsight Users file you created from the import template.
4. Click **Upload** to import the file.
5. You will be presented with the Import Users dialog screen.

6. Determine how you would like to handle duplicates:
 - a. Skip Duplicates (Keep Existing Records) or
 - b. Update existing records.
7. In the Password section, determine how you would like to import passwords:
 - a. Override the Password of Existing Users.
 - b. Send User Notification if Password Changes.

8. In the Email section, select the relevant options:
 - a. Send Welcome Email to New Users.
 - b. Send Welcome Email if Email Address Changes.
9. Select SIP Settings – This automatically assign SIP accounts to new users. This is an important step in configuring users accounts to ensure they are ready to make Onsight Calls.
10. The License Group for New Users is specified within the CSV file.
11. Licenses – Enable the appropriate option:
 - a. Create new users if license assignment is missing.
 - b. Update licenses of existing users.
Note: License types you are assigning to each user (licenses must be available in the chosen license group).
 - i. Connect Enterprise
 - ii. Workspace Enterprise
 - iii. Workspace Contributor
12. In the Policy Group Membership section, select how you would like to assign group membership to existing users. In this case, you are importing an Onsight User's file to reconfigure the existing users accounts. Select from:
 - a. Merge Groups results in users who are 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 screen appears.

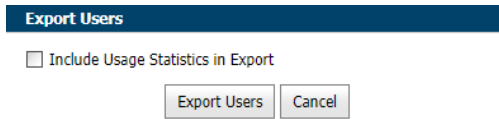
Note: You must use the License Group for New Users field to assign license group membership when importing users and assigning licenses. This means only members of the same License Group can be imported by the specified user file. The GroupMembership field of SampleUserImport.csv file cannot be used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

When importing users into a License group there must be enough available licenses of 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.

Export users

Go to **USERS**, 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.



SELF-REGISTER USERS

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

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

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

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

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

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**.

To manually add an External Contact to the Global Directory:

1. On the EXTERNAL CONTACTS page, click the **New Contact** button.
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 to which you would like the external contact added.
4. Click **OK**.

You will now be able to see the **External Contact** when searching the Global Directory from an Onsight endpoint.

To import an **External Contacts** file:

1. On the EXTERNAL CONTACTS page, select **More** → **Import**.
2. Create a Contacts.csv* file to import. Refer to the CVS Import Instructions for details on column names, required fields, and format.
Note: the addresses you enter must be in the SIP URI format, e.g., videoroom@sipdomain.com.
3. Select the File to Import, press the **Browse** button.
4. Press **Upload**.
5. You will be presented with the Import External Contacts dialog screen.
 - a. Select the Duplicate Handling option appropriate for your situation:
 - b. Skip Duplicates (Keep Existing Records)
 - c. Update Existing Records
 - d. Create a Duplicate
6. Press **Import**.
7. When the import is complete you will be presented with the Import Results screen.
8. Press **View Report** for details.
9. Press **Close**.
10. Return to the EXTERNAL CONTACTS page to view the imported contacts.

***Note:** On the EXTERNAL CONTACTS page, you may press **More** → **Export** to download a contact's file template.

ADD AN EXTERNAL CONTACTS LIST

1. Click the **New List** button below the MANAGE EXTERNAL CONTACTS title. You will be presented with the Create New Contact List screen.
2. Enter a Name for the list and a Description.
3. Select **Public** or **Private** to set the accessibility level for the list. If selecting Private, select the Groups that will have access to the list.

ADD/REMOVE EXTERNAL CONTACTS FROM LISTS

1. On the EXTERNAL CONTACTS page, select the External Contacts you wish to add to the list.
2. Press **More** → **Add to List**.
3. Select the list to which you want the contacts to be added.
4. Click the Contact list name to confirm the contacts are listed.
5. You may remove contacts from a list by selecting the list, then the contacts you want to remove. Next, press More-Remove from List.

SETTINGS

An OPM Administrator can configure the 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 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.
- SIP Settings are assigned from the Auto-Assignment Pool.
- Onsight Connect version settings can be selected.

- Client Policies are selected for each endpoint, e.g., Encryption mode.
- Security settings are assigned such as 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 making changes to a settings page you must press **Save** to commit the changes. Press **Reset Changes** to return the prior saved settings on the page.

AUTHENTICATION TIME-OUT

To allow access to content and call services if the loss of network connectivity occurs, users remain locally authenticated for 30 days on the client after their initial online authentication occurs. Clients must re-authenticate to the online service once every 30 days.

ACCOUNT

Your company’s OPM account information is displayed on the Account page.

- Choose the **SETTINGS** tab and then **ACCOUNT**.
- ACCOUNT INFORMATION is listed including your Company Name, Customer Domain, Account Owner, Customer Created date, Customer Expiry date and Super Administrator Access status.
- The LICENSES section includes Onsight Users, Client Functionality, and Hosted Features.

SUPER ADMINISTRATOR ACCESS

In the Common Actions panel, you can Grant or Disable **Super Administrator Access** to Librestream Support. This allows 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. Call Librestream Support if assistance is required.

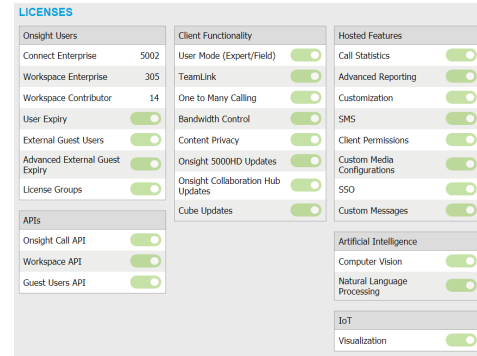
CHANGE ACCOUNT OWNER

In the **Common Actions** section, you can use **Change Account Owner** to specify the primary OPM Administrator for your Onsight Account Domain.

Change Account Owner allows an Onsight Platform Manager Administrator to assign another user as the Account Owner. The user must have Onsight Platform Manager Administrator privileges before they can be assigned as the Account Owner.

DOMAIN LICENSES

The licenses enabled in your Onsight domain are listed in the **LICENSES** section. They are divided into 4 main categories: Onsight Users, Client Functionality, APIs and Hosted Features.



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.

APIS

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.

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: allows user accounts expiry dates.
- External Guest Users: allows guest invites.
- License Groups: allows license pool management on a per group basis.

CLIENT FUNCTIONALITY

User Mode (Expert/Field): enables the capability to define user accounts as Expert or Field. 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 allows HTTPS tunneling of all 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 **‘Always use TeamLink’**, 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. Librestream recommends that ‘Always use TeamLink’ be disabled and only be used on a per endpoint basis for troubleshooting purposes.

ON PREMISES:

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

Multiparty Calling: enables the capability to set Windows PCs and Android devices as conference hosts. When enabled, the device may host a conference call with multiple participants. The limitation on the number of participants is dependent on the hardware and network resources available to the device. 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 via Client Policy.

Onsight Collaboration Hub Updates: enables the ability to deploy software updates to Onsight Collaboration Hubs via either iOS or Android clients.

HOSTED FEATURES

Call Statistics: enables the capability to capture Call Statistics from Onsight endpoints.

Advanced Reporting: enables the capability to generate an 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.

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.

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

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

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

Data Anonymization of PII occurs when:

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

Note: Onsight Workspace content is the property of the customer. As such, the company is responsible for all content. When a user is deleted, the Workspace account is also automatically deleted. The customer must choose to delete the user's content as 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.

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.

ARTIFICIAL INTELLIGENCE

Computer Vision: enables access to the CV features including OCR, Object classification and location, and auto-tagging.

Natural Language Processing: enables access to the NLP feature - Onsight Translator.

IOT

Visualization: enables access to IoT services, instrument visualization and auto-tagging.

USERS

Set the user and external guest user related global settings for the domain on the USERS page.

USER ACCOUNTS

Set the **Default Time Zone** for all User Accounts by selecting the desired zone from the drop-down list.

All data reported by Onsight clients to OPM is based on UTC however, the Default Time Zone setting will adjust the time stamp data within OPM for display purposes only.

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.

EXTERNAL GUEST USERS

All External Guest Settings are moved to Client Policy.

GLOBAL DIRECTORY

This setting controls how External Contacts are displayed in 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, such as external or third-party video endpoints.

External Contacts are public by default: controls 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 user setting - Disable global directory access**, this controls standard user access to External Contacts in the global directory.

CUSTOM FIELDS

Custom fields can be added for use on the user profile page.

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.

Note: custom fields will be included in the exported user report.

SECURITY

Set security so that each OnSight Connect clients complies with your password and login policies.

PASSWORD POLICY

Set the Minimum Length, Minimum Capital Letters and Minimum Non-Alpha Characters for your domain and client policy.

PASSWORD EXPIRATION

Enable Password Expiration: enables password expiry on the clients and OPM login.

Password Expires: set the length in days.

Minimum: 1 day, Maximum: 365 days.

Warn Users Before Expiration: set the length in days.

Minimum: 0 day, Maximum: 365 days.

LOGIN POLICY

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. 5, 15, 30 minutes, or forever (requires the administrator to unlock the account to grant access).

SELF REGISTRATION

This setting allows user to self-register for an account by going to the self registration URL. The URL must be distributed by the administrator and may be protected by a self registration key.

Enable Self Registration: allows 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 unauthorized access to the 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: When enabled, the administrators will be 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 list of allowed email domains for self-registered users. Use in combination with the 'Required Email' setting to restrict access to self-registered accounts.

SSO

Single Sign-On (SAML v2.0) is supported by OnSight Platform Manager as a licensed add-on for Enterprise customers. SAML 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 to select to which users you would like to notify and have instructions sent. You can select individual users or groups. They will receive an email with the login instructions.

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.

SINGLE SIGN-ON

Enable Single Sign-On to turn on SSO support.

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 with their OnSight Account (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 IdP, they would still be able to log in to OnSight Connect.

SAML CONFIGURATION

Local Service Provider

These settings describe OnSight Platform Manager as the Service Provider (SP) to your Identity Provider (IdP).

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

To configure your IdP settings:

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 Identify Provider (**IdP**).
3. Download the **IdP metadata file** from your **IdP**.

Local Service Provider (cont'd)

If you require encrypted communication between OPM and your IdP, you will need to import the OPM SP Certificate into your IdP.

1. Press the **Download SP Certificate** button to download the Service Provider (SP) public certificate file.
2. Upload the **SP Certificate** file to your SSO Identify Provider (**IdP**).

Partner Identity Provider Settings

These settings will tell OPM 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 Provider Settings.

Importing the metadata will provide the:

- 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.

Press **Import IdP Metadata** to import the IdP metadata file that you downloaded from your Identity Provider. The metadata file will normally contain the IdP Public Certificate.

Press **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.

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**.

USER IDENTITY FEDERATION

User Identity Federation defines how SSO enterprise users map to OnSight user accounts.

User Identity Mapping

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

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

Choose one of the following mapping methods:

Username mapping:

1. Select the **Onsight Account Field** to be compared to the **Mapped IdP Attribute**:
 - a. **User Name** – OnSight Account User name
 - b. **Email Address** – OnSight Account Email Address
 - c. **Federated SSO Id** – OnSight user's associated Federated SSO Id. This is defined by the OnSight Administrator and can be included as part of the Imported User list. This may be mapped to either the **Subject Name Id** or an **Attribute** of the SAML Assertion.
2. Select the **Mapped IdP Attribute** to be compared to the **Onsight Account Field**:
 - a. **Subject Name ID**
 - b. **Attribute** – set the **Attribute Name** of the **Attribute** to be compared to the **Onsight Account Field**

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.

Email mapping:

1. Select the **Onsight Account Field, Email Address**.
2. Select the **Mapped IdP Attribute, Attribute**.
3. Enter the **Attribute Name**, e.g., **Email**.

Federated SSO ID mapping:

1. Select the **Onsight Account Field, Federated SSO ID**.
2. Select the **Mapped IdP Attribute, Attribute**.
3. Enter the **Attribute Name**, e.g., **OPMUSER**. (You may define which ever attribute name you wish).

SSO SELF REGISTRATION

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

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.

Set your notification and Email preferences:

- **Notification:** Notify Administrators by email when an account is registered.
- **Email:** Require Email Address for Self-Registered Accounts.

Set the method you would like to use for **User Name** creation:

- **Auto-generate:** Creates the Onsight username.
 - **Prefix:** Set the prefix for auto-generated Onsight usernames.
- **Attribute:** Uses the mapped attribute as the Onsight username.
 - **Attribute Name:** Set the attribute name that will be used as the Onsight username.
- **Prompt on First Login:** Prompts the user to enter an Onsight username.

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.
- Or select **Prompt on First Login**, which will require the user to enter their email address the first time they log in to Onsight Connect.

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

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.

Set the **Password** creation option:

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

USER PROVISIONING LINKS

These links are provided for reference. You may include the links in your Onsight account deployment instructions email to your users.

SSO Client Login: The link to the SSO login page.

Windows Client Download: The download link for Onsight Connect for Windows.

Mobile Client Link: The link to the Onsight Connect for mobile devices download page.

NOTIFY EXISTING USERS

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.
2. Select the users you wish 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.

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.

SIP

SIP (Session Initiation Protocol) 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.

SIP SETTINGS

Self-Registration Auto-Assignment

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.

SIP ACCOUNT

There are three SIP Server set up options:

- Onsight Connect Hosted SIP Service
- Shared Account (Enterprise SIP Server)
- 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 (a.k.a. the 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, 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.

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 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.

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.

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.
 - a. 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.

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.

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, Authentication Password**.
2. In the SIP Settings section, select **Automatically assign SIP accounts to self-registered users**.
3. Set the **Assignment 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, Authentication Password**.
8. Repeat steps 3 to 7 on the **Private Server** tab if required.
9. **Save** the changes.

MANUALLY ASSIGNING SIP ACCOUNT TO USERS

SIP Accounts are assigned when a new User Account is created. The **Automatically assign a SIP account to this user** checkbox 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).

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.

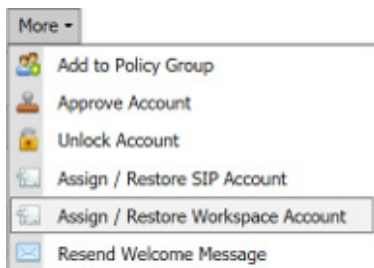
Workspace integrates with the full OnSight platform by providing a practical solution to aid in knowledge management and audit trail requirements. The solution features:

- 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

ENABLING WORKSPACE ACCESS FOR USERS

When Workspace is enabled for an existing domain, existing users have to be assigned a Workspace account. (Any new users added are assigned a Workspace account automatically).

1. On the Users page, select the users you want to have Workspace access.
2. Then select **More → Assign/Restore Workspace Account**.



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 press the **Modify Group** button (pencil icon).
6. Select the CLIENT POLICY page.
7. Select **Choose Settings**.

8. Select the Workspace settings to the Client policy including:
 - **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. Press **OK**.
10. In the Workspace Section set the desired Values.

Description	Value
Workspace	
Access	Enabled
Upload Path	~/CustomUploadFolderName
Auto Upload Media	Disabled
Maximum Upload Bit Rate (Kbps)	0
Restrict Upload Folder Access to Owner	Disabled
Allow Cellular/Mobile Data Usage	Enabled

WORKSPACE 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.

To create or Modify a Webhook configuration, you must:

1. Login as an Administrator to OPM. Click **Settings → Workspace**.
2. The **WEBHOOKS CONFIGURATION** table displays a list of webhooks.

WEBHOOKS CONFIGURATION					
Name	Events	Batch Frequency	Active		
<input type="checkbox"/> Document Retrieval Retrieve new Workspace files	Created	0	<input checked="" type="checkbox"/>		Test Webhook
<input type="checkbox"/> Inactive A deactivated webhook	Modified, Deleted	0	<input type="checkbox"/>		Test Webhook
<input type="checkbox"/> Metadata Updates Webhook for testing	Created, Modified, Deleted	5	<input checked="" type="checkbox"/>		Test Webhook

3. Click the **New** button to add a webhook configuration. The New Webhook Configuration form appears.

New Webhooks Configuration

Name:

Description:

Consumer URI:

HTTP Headers:

Administrator Email:

Batch Frequency:



User Name:

Password:

Active:

Events: Created Modified Deleted

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 - If 0, each event will result in a notification being sent
 - **User Name/Password**: If set, the notification will use HTTP Basic authentication with these credentials
 - **Active**: If unchecked, no notifications will be delivered for this webhook
 - **Events**: The Types of events that will trigger webhook notifications for this configuration - You must select one event
4. Enter all required fields and click **OK** to save the webhook configuration.
 5. Click the **Edit**  icon to show the Edit Webhook Configuration pop-up. This is identical to the New Webhook Configuration pop-up and it enables you to make changes to an existing configuration.
 6. Select one or more webhook configurations from the table and click the **Delete**  icon to permanently remove webhook(s). After deletion, no further notifications will be sent to consumer services for those configurations.
 7. Click the **Test Workbook** button from within the WEBHOOK CONFIGURATIONS table or New/Edit Webhook Configuration pop-up to test the configuration.
 - A **test** event notification triggers immediately and is sent to the **Consumer URI** from Workspace
 - OPM will display test results including the test duration and status code returned to Workspace from your consumer service

SOFTWARE UPDATES

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

ONSIGHT 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.

Based 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.

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 screen 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.

UPDATES FOR ONSIGHT 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.
- SETTINGS-COLLABORATION HUB-CHECK FOR UPDATES.

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.

CLIENT POLICY AND PERMISSIONS

Client Policy and Permissions configured under the SETTINGS-CLIENT POLICY or CLIENT PERMISSIONS pages 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 more restrictive 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 most restrictive 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.

To edit the Client Policy for a user, select the User, 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.

EXTERNAL GUEST USERS

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. Default: Enabled.

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

Confirmation: controls whether the inviter will receive an email confirmation when the invite was sent. It will include a copy of the invite message.

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

Yellow – invite sent, status unknown. This usually indicates the guest's email or SMS service provider has not acknowledged the receipt of the message.

Green – invite received by guest.

Red – invite not delivered.

Permissions: set **Disable recording of images and video** to prevent a Guest from making OnSight recordings or capturing OnSight still images. Default: Enabled, i.e., External Guest Users cannot record images and video.

If desired, set **Disable 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.

EXTERNAL GUEST INVITATION DEFAULTS

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. Default: 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.

Default: 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.

- OnSight Platform Manager: no-reply@librestream.com
- Inviter's Email Address

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: Set the guest's mode as Expert or Field.

POLICY PRECEDENCE

Users who belong to multiple Groups will have configuration settings applied giving precedence to the more restrictive setting. For example, 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 Encryption: Auto. In order for Bob to receive a client policy configuration of Encryption: 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

would now be Encryption: On, since it is more restrictive 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 less restrictive Encryption setting would be to Override it in Bob's User Client policy settings.

SETTING CLIENT POLICY

1. On the SETTINGS page, select the CLIENT POLICY tab.
2. Select the Group to which you wish to apply a policy.
3. Click the **Choose Settings** button. You will be presented with the **Choose Settings** screen.
4. Under each category, select each setting you would like to manage, or click **Description** to select all. Next, click **OK**.
5. When you are returned to the Client Policies page, set the appropriate Value for each Category.
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** allowing you to manage privacy settings.

SETTING CLIENT PERMISSIONS

1. On the SETTINGS page, select the CLIENT PERMISSIONS tab.
2. Select the Group you want to manage.
3. For each setting under **Description**, apply the **Action** you want applied for the permission.
 - a. **Allow** – let users edit the setting.
 - b. **Deny** – do not allow users to edit the setting.
 - c. **Inherit** (available only if the group is a child of a parent group).
4. Click **Save**.

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

GROUP CLIENT POLICY AND 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 Onsite Connect endpoint. Whether users are logging in to a Windows PC, iOS or Android smartphone, or an Onsite Smart Camera their assigned client policy will be applied.

The **Onsite 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 Onsite Support website.

Group Client permissions determine authorization for user access to settings on an Onsite 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 Onsite 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 **Policy Precedence section** for details.

LOCAL PRIVACY

Onsite Privacy settings allow control over which users can capture still images or recordings during a call. Disable recordings and saving snapshots for ALL participants (Privacy Mode) prevents the capture of any video or images by any participant in a call when it is enabled. This is the most restrictive privacy setting for streaming media during a call.

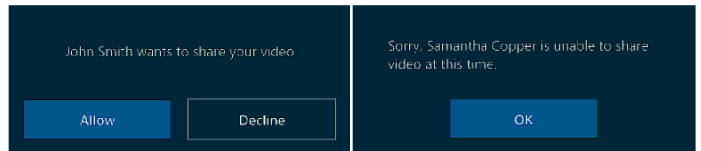
To control privacy for groups and individual users, use Local Privacy Mode instead. Select the appropriate privacy setting for the group policy (or user policy):

- Allow recordings and saving snapshots
- Disable saving snapshots (but allow recordings)
- Disable recordings (but allow snapshots)
- Disable recordings and saving snapshots

Example, you have a location where you do not want any users to save still images or recordings. Apply **Disable recordings and save snapshots** to the Group's **Client Policy**.

REMOTE VIDEO PRIVACY

Onsite privacy settings require consent for remote video sharing requests during an Onsite 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.



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

Remote video privacy affects:

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

WEBEX CMR COMPATIBILITY

Enabling WebEx CMR Compatibility allows 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.

SMS

The SMS page lists the SMS API configuration for the messaging service. This is included as part of the Enterprise and Pro platform subscriptions.

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

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.

CUSTOMIZATION

Customization allows you to customize the 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

System 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, press **Insert Default Template** beside the message text box. You may edit the default message template or create your own messages. Press **Save** to keep your changes.

EMAIL CUSTOMIZATION

Email Custom messages will contain both the text and HTML versions of the message (if you choose to include both). The User's email reader will determine which version to display, e.g., If HTML is not supported by the email program, the TEXT version will be displayed.

CUSTOMER DEFINED TAGS

Customer defined tags are used to identify your company's resources such as custom messages, logos, and support desk information.

1. EMAIL REPLY-TO-ADDRESS: Enter the Reply-to-address to which you would like the user to Reply.
2. CUSTOMER DEFINED TAGS:
 - a. Company Logo URL: add your company's logo to the Onsight email notifications.
 - i. Tag name: {{companylogourl}}
 - b. Support Contact Information: add information on how to contact your Company's Support desk.
 - iii. Tag name: {{companysupportdeskinfo}}
 - d. Company Message: add a custom message for your Onsight domain users.
 - v. Tag name: {{companymessage}}

SYSTEM DEFINED TAGS

System defined tags let you access OPM generated information for use in your custom messages. This information is for

reference only and cannot be edited.

LIBRESTREAM DEFINED TAGS

These tags allow you to access Librestream web resource URLs including OPM login, license agreement, and support and training. They cannot be edited.

SECTION TAGS

Section Tags are used to define a section within an email template. Both System and Customer defined tags are enclosed in Section tags within the Email Message Templates.

Sections are included in an email message if the corresponding tag is defined.

For example, if the {{companymessage}} tag has been defined by the Customer then the {{companymessage}} will be included within the [[companymessage]] section when the email message is sent. If {{companymessage}} has been left blank the [[companymessage]] section will not be included when the email message is sent.

If you do not wish to include a particular section in an Email message, remove the section tags (and the text it encloses) from the Message template.

EMAIL CUSTOMIZATION (HTML AND TEXT)

Fill in sections with text for your custom messages. Leaving them blank will result in the default Onsight branded templates being used.

Press the Send Email Test link to send a test copy of the message to an email of your choice.

The following messages support TEXT, HTML and the customer defined embedded TAGS. Insert Customer, System and Librestream Defined TAGS in Section TAGS to include information, for more info refer to Custom Messages Help.

Define the Subject, Title, Text, and HTML message from each message type.

1. Account Created Message
2. Account Registered Message
3. External Guest Invite Message
4. SSO Enabled Instructions Message

EMAIL CUSTOMIZATION (TEXT ONLY FORMAT)

Define the Subject and Text Message for each message type.

1. Account Deleted Message
2. Guest Confirmation Message
3. Password Reset Request
4. Password Changed Confirmation

SMS customization: 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.

Press the **Send SMS Test** link to send a test copy of the message to a phone number of your choice.

SMS Custom messages are sent when Onsight users use the SMS service to perform the following tasks:

1. External Guest Invitation
2. Password Reset Request
3. Password Changed Confirmation

For details on Message Customization, please refer to the [Custom Messages Help](#) link on the CUSTOMIZATION page.

SMS CUSTOMIZATION

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.

Press the **Send SMS Test** link to send a test copy of the message to a phone number of your choice.

SMS Custom messages are sent when Onsight users use the SMS service to perform the following tasks:

1. External Guest Invitation
2. Password Reset Request
3. Password Changed Confirmation

For details on Message Customization, please refer to the [Custom Messages Help](#) link on the CUSTOMIZATION page.

API KEYS

The API Keys page allows management for access to the Onsight Call and Workspace REST APIs.

Press the **NEW** button to generate a new API authorization key.

Enter the following information:

1. Name
2. Description
3. API Key Expires
 - a. Expiry Date
4. Set the permissions (**None, Read, Full**) for:
 - a. Onsight Call
 - b. Workspace
5. Press **Generate Key**.

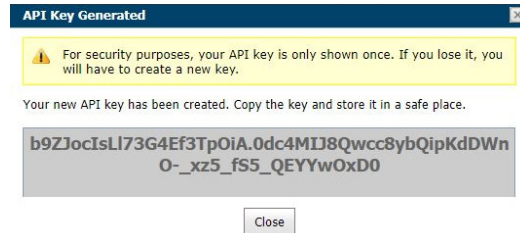
API GENERATED KEY

Once the Key is generated the API Key Generated dialog will be displayed. 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.

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



Once created the key cannot be viewed again but you may edit its associated properties such as the Name, Description, Expiry or Permissions. Press the edit button to change API key properties. You may 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.

AI SETTINGS

Use the 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, OCR, IoT, and NLP**.

Press the **NEW** button 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.

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 it can be configured, press the Choose Setting button 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 an AI setting profile if you wish to have members of a group access more than one AI service.

AUTO TAG IMAGES

When configuring client policy, you may choose to enable 'Auto Tag Images'. This will automatically process images and tag them with the Computer Vision (CV) results for Optical Character Recognition (OCR) and Object detection. These tags are searchable within OnSight Workspace.

STATISTICS AND EVENTS

Client Activity and Events can be viewed on the STATISTICS AND EVENTS page.

CLIENT ACTIVITY

The Client Activity page tracks user activity on the OnSight Connect Service. The Administrator can see who is actively logged in as well as the history of activity.

1. Set the FILTER PARAMETERS and click **Apply Filter** to display the Client Activity.
 - a. Standard Users and/or External Guest Users.
 - b. Start/End date.
2. You are shown a view of the following:
 - a. Login Time
 - b. Duration
 - c. User
 - d. Version of endpoint software
 - e. IP Address
 - f. Host Name
 - g. Last Activity
 - h. State
3. Click **Refresh** to update the list.
4. Click **Export** to save a comma separated file, csv, of the report.

To view the Client Status details:

1. To view a user's details, click on the **Details** button.
2. The Client Status page reports:
 - a. SIP STATUS
 - b. TEAMLINK STATUS
3. Exit the page when done viewing.

STATISTICS

The Statistics page provides call related statistics. Call related stats are available for Connect Enterprise licensed users.

1. Set the **Filter Parameters** and click **Apply Filter** to display the Calls activity.
 - a. Standard Users and/or External Guest Users.
 - b. Start/End date.
2. You are shown a view of the following:
 - a. Start Time
 - b. Duration
 - c. Calling Participant
 - d. Calling User
 - e. Called Participant
 - f. Called User

3. Click **Refresh** to update the list.
4. Click **Export** to save a comma separated file, csv, of the report.
5. To view a user's details, click on the Details button.
6. The Call Details page reports:
 - a. **CALL DETAILS**
 - i. Start Time
 - ii. Total Duration
 - iii. Encrypted
 - iv. Reported Time
 - v. Termination Reason
 - vi. Voice Codec
 - b. **FROM**
 - i. Name
 - ii. Address (SIP)
 - iii. User Name
 - iv. Product (Client)
 - v. TeamLink
 - vi. Operating System
 - vii. Hardware
 - viii. Network Interface
 - ix. Cellular Carrier
 - x. Calling Latitude
 - xi. Calling Longitude
 - xii. Calling Altitude
 - c. **TO**
 - i. Name
 - ii. Address
 - iii. User Name
 - iv. Product (Client)
 - v. TeamLink
 - vi. Operating System
 - vii. Hardware
 - viii. Network Interface
 - ix. Cellular Carrier
 - x. Called Latitude
 - xi. Called Longitude
 - xii. Called Altitude
3. **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. GOP
 - g. Video Bit Rate
 - h. Limit
 - i. Device Type
 - j. Video Codec
 - k. Audio Codec
4. Exit the page when done viewing.

EVENTS

The Events page tracks administrator and user activity on OPM as well as Server based event messages.

1. Set the **Filter Parameters** and click **Apply Filter** to display Set the Filter Parameters:
 - a. Severity options
 - b. Standard Users and/or External Guest Users.
 - c. Start/End date.
2. Click **Apply Filter** to display the Event Log.
3. The event log displays:
 - a. Time
 - b. User
 - c. Description
4. Click **Refresh** to update the list.
5. Click **Export** to save a comma separated, csv, file of the report.

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 can 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.

To run a report:

1. Select the Report Name:
 - 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) – lists the # of licenses used during the period.
 - h. Guest Invite Summary – lists the # of guest invites sent for the period including sender, guest, invite status, etc.
 - i. Overall Usage Summary – lists the # of calls and the total duration for the period.
2. Select the User Account Type: **Default** – All Users, **Standard**

or **External Guest Users**.

3. Select the Start Date and End Date of the report.
4. Select the Groups to include in the report (optional -the default is **All Users**).
5. Select the Country to filter on (optional- default is **All Countries**).
6. Select Custom Fields for filtering (optional – default includes all custom fields).
7. Set the Call Duration filter:
 - a. Any
 - b. Greater or equal
 - c. Less or equal
 - d. Between
 - e. Set the number of minutes based on the Call Duration selection.
8. Select the Number of Results to include in the report.
 - a. 10, 25, 50 or 100
9. Click **Run Report**.
10. Click **Export** to download and view the results in comma separated, csv, file format.

HEAT MAPS

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

1. Select the Heat Map type:
 - a. Call
 - b. Login
2. For Calls also select the Participant Type:
 - a. Caller
 - b. Callee
 - c. Both
3. Select the Start Date and End Date of the report.
4. Click **Apply Filter**.
5. Click **Print** to print a PDF copy of the map.
6. Click **Export** to save a CVS file containing location and counts of the results.

The Heat Map will be displayed indicating the location and quantity of calls/logins.

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.



ONSIGHT CONNECT FOR WINDOW - INSTALL

A new Onsight Connect User is sent a **Welcome email** that will notify the new user of their Onsight Connect account and how to download and install Onsight Connect for Windows (as well as iOS, and Android).

Onsight Connect for Windows can be installed on either a per-user (Standard) or per-machine (Enterprise) basis. The Standard installation option enables installations of Onsight Connect by users that do not have Administrator privileges on their Windows PC.

For Full details on Onsight Connect for Windows Installation, see the **App Note: Onsight Connect for Windows - Standard x64 Enterprise - available at <https://www.onsight.librestream.com>**. Click the **TRAINING** link then visit the Technical Materials section.

Users who have **Windows Administrator privileges** will default to the Enterprise version of Onsight Connect for Windows install. You may wish to install the Standard version of the software; however, if you previously installed the Enterprise version, you must first un-install the Enterprise version before proceeding with the Standard install.

LANGUAGE SUPPORT

Onsight Connect supports the following languages in 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. There is no configuration required in 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:

Invite Guest

- OC for Windows download
- Register for an Account
- Forgot Password
- Reset Password
- SSO login

Emails originating from OPM are also localized including:

- Account registered (HTML, text)
- Guest user confirmation (text)
- Guest user invitation (HTML, text, SMS)
- Password reset requested (text, SMS)
- User password changed (text, SMS)

CUSTOM MESSAGES

Custom Messages can be displayed within the Onsight Connect application at login or before starting a recording. They must be acknowledged by a user before login completes or a recording is started. If the message is not accepted by the user (they must press OK) then the action will not be allowed, i.e., the user will be returned to the login screen or recording will not start. Typically, a custom message is used to display the terms of use for using the Onsight Connect within your company.

CUSTOM MESSAGES - FORMS

Go to the Custom Messages page to manage custom messages forms.

1. Press the **New** button to create a new custom message.
2. Enter the following:
 - a. **Name** - this is only visible within OPM.
 - b. **Available for Use** - check this box if you want the form available for use in client policies.
 - c. **Title** - this is displayed in the app.
 - d. **Message** - this is the message the users will see. There is a 500-character limit.
 - e. **Trigger** - select which event will trigger the display of the message, Login or Recordings.
 - f. **Button Styles** - select the style of response buttons you wish 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 do NOT select this option.
 - h. Press **OK** to save your custom message. Press Cancel if you don't want to save your changes.

CUSTOM MESSAGES - CLIENT POLICY

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

1. Go to the USERS page and select a group.
2. Press the **Edit** button.
3. Select the **CLIENT POLICY** tab.
4. Press the **Choose Settings** button.
5. Select **Custom Messages**.
 - a. Select **Login** if you want to display a Login message.
 - b. Select **Recording** if you want to display a Recording message.
6. Press **OK** to return to the Client Policy.
7. Go to Custom Messages section.
 - a. Select the Login message you want to display.
 - b. Select the Recording message you want to display.
8. Press **Save** to keep your changes.

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/>

CONTACT SUPPORT

For support, please contact support@librestream.com or call **1.800.849.5507** or **+1.204.487.0612**.

