ON SIGHT

ADMIN GUIDE

Onsight Platform Manager

Software Version 8.1

LIBRESTREAM

Document Revision

Librestream
Onsight Platform Manager Admin Guide
Doc #: 400199-07
May 2017

Information in this document is subject to change without notice.

Name of Librestream Software Onsight Connect

1 Table of Contents

1 Overview

Onsight Platform Manager (OPM) is a secure online tool for system administrators to centrally manage their Onsight user licenses, manage 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** – Onsight Administrators can view and manage the status of their Onsight Connect user license pool such as adding new Onsight Connect users.
- **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.

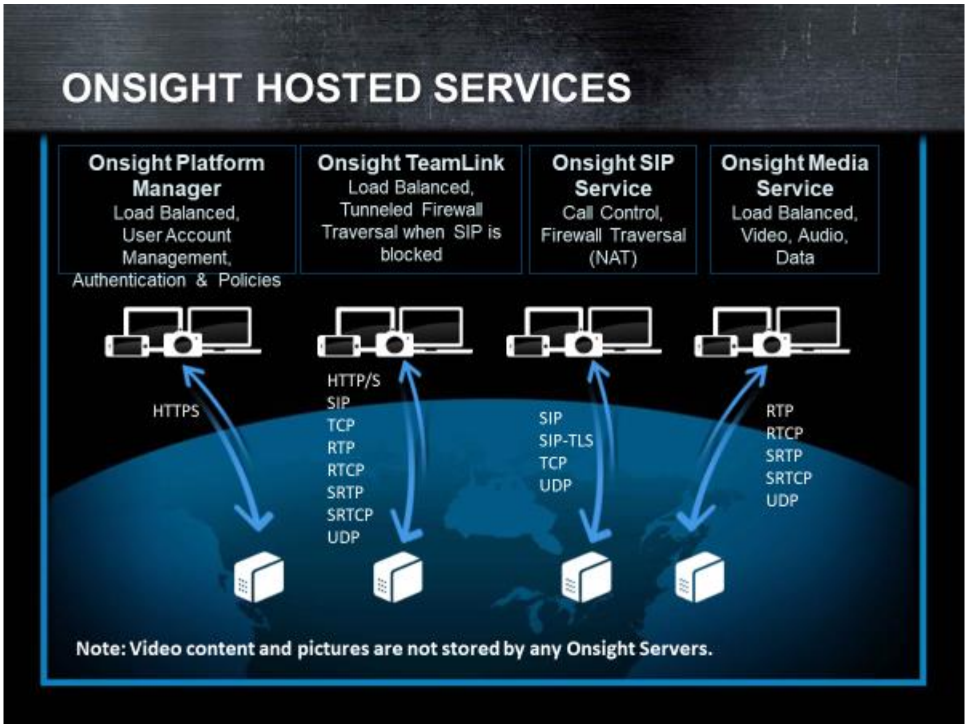
The tasks described are administration-level tasks and are not intended for end-users of Onsight Connect. Many of the tasks involve configuring Client Policy and Permissions, and affect the endpoint's ability to function.

ℹ **ON PREMISES:** Details specific to the Onsight Platform Manager – On Premises installation are highlighted by the information icon.

1.1 Onsight Hosted Services

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

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 3rd party video endpoint that supports Session Initiation Protocol (SIP). For more information on the full Onsight Connect capabilities, access the online training portal at http://www.onsight.librestream.com.



ONSIGHT HOSTED SERVICES

Onsight Platform Manager
Load Balanced, User Account Management, Authentication & Policies

Onsight TeamLink
Load Balanced, Tunneled Firewall Traversal when SIP is blocked

Onsight SIP Service
Call Control, Firewall Traversal (NAT)

Onsight Media Service
Load Balanced, Video, Audio, Data

Note: Video content and pictures are not stored by any Onsight Servers.

2 Network Requirements

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

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

2.1 Firewall Configuration

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

Table 1 – Windows Firewall Exceptions

Name	Protocol	Port	Description

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

3 Logging into OPM for the First Time

3.1 Logging In

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

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

User Name:	user@domain.com
Password:	Password

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

After successfully logging in, you will be taken to the Home page.

ON PREMISES: The URL of your OPM server will depend on the server's URL assigned during installation.

3.2 Home

The Onsight Platform Manager Homepage provides a **Summary** of the following:

- Total Users
- External Guest Users
- Active Users
- Users awaiting approval by the administrator
- Expired Users
- Total User Licenses
- Available User Licenses
- Active Onsight Sessions

ON PREMISES: External Guest Users are not supported by On Premises installations.

There are direct links to the configuration and status pages for each item in the Summary list as well as access to the pages through the menu links at the top of the page. The Personal Settings, Users, External Contacts and Administration sections provide task related links, e.g., Import Users.

Also on the Home page is a list of current Notifications for the Administrator. Notifications appear when a User has registered for an Account and it requires Administrator approval before use can begin.

ON PREMISES: The Setup Wizard is accessed on the Home page. For details, refer to the Onsight Platform Manager – On Premises installation guide.

4 Administrator's Settings

4.1 Changing the Administrator's My Profile

The **Account Owner** is the main Administration account. The Administrator account includes an Onsight Connect endpoint license; therefore, you can log in to Onsight Connect software as a User as well as configure OPM. When logged in to OPM, **My Profile** allows the Administrator to configure their personal settings like any other User Account. Once these settings are configured, the Administrator can also log in to an Onsight endpoint and use it for collaboration.

4.1.1 CHANGING THE ADMINISTRATOR'S PASSWORD

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

4.1.2 CHANGING THE ADMINISTRATOR'S PERSONAL CONTACTS

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

4.1.3 ADDING ADMINISTRATORS TO OPM

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

To add additional Administrators:

- Select the **USERS** tab.
- Press the **New User** button.
- Enter the **PROFILE** settings:
  - Username
  - First Name
  - Last Name
  - Email

  - 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 usernames and passwords.
  - If Single Sign On is enabled, enter the **Federated SSO ID** (if required). See the SSO section for details.
- Under **CLIENT SETTINGS**, select **Administrator** for the **Account Type**.
- The **Automatically assign a SIP account to this user** is selected by default. This is required if you want your administrators to be able to log in locally on an Onsight endpoint and make calls.
- By default, the **Administrator** will belong to the **Domain** license group. You do not need to assign the administrator to a different license group.
- By default, the **Administrator** belongs to the **Domain** policy group. You do not need to assign the administrator to a different client policy group.
- It is recommended you do not set the account expiry for **Administrators** unless required. For example, a temporary administrator has been assigned while someone is on vacation.

5 Users and Groups

Onsight administrators centrally manage Onsight user licenses, manage contacts lists and groups, and configure user group policies and permissions. Using OPM, administrators can efficiently manage and maintain groups of Onsight users.

There are three ways the Administrator can add Users:

- Manually Create New User.
- Import Users from a file (e.g., SampleUserImport.csv).
- Self-registration using the OPM Self-Registration webpage.

5.1 Manually Adding Users and Groups

When a new user is added to the Onsight Account domain, they are automatically assigned to the **All Users** Group. The seven default Groups provided by OPM include:

- **All Users** – by default includes everyone in the domain: Administrators, Standard users and External Guest users.
- **Standard Users** – by default includes Standard Users and Administrators (External Guest users are not included) and allows Client Policy configuration.
- **External Guest Users** – includes all External Guest Users and allows Client Policy configuration.
- **Awaiting Approval** – indicates of the number of self-registered users awaiting Administrator approval. Client Policy is not applicable.
- **Onsight Client Licensed** – indicates the number of licenses assigned to administrators and users. Client Policy is not applicable.
- **Administrators** – indicates the number of administrator accounts. Client Policy is not applicable.
- **License Groups** – includes the default Domain. Any custom License Groups created will be listed separately.

The default Groups cannot be deleted. The OPM Administrator can create 2 types of custom Groups: **Policy** and **License**.

Policy Groups are used to apply client policy to groups of users.

License Groups are used to apply client policy and assign a specific number of user licenses to the group. This allows an administrator the ability to partition the number licenses among groups. A Group Administrator can be assigned to the group. For example, an Administrator assigns 10 licenses to a License Policy Group. A Group Administrator is assigned and is able to add a maximum of 10 users to the group. If a user is deleted from the group, the license becomes available for use and can be assigned to a new user. The licenses will remain assigned to the group unless the OPM Administrator reassigns them back to the domain.

In both cases, an Administrator can override group policy for a specific user by editing the user's **Client Policy**.

The use of License Groups is optional. You can manage your domain only using Policy Groups. In this case, the pool of user licenses is unmanaged and free to be assigned by Administrators and Group Administrators. When you are not using License Groups, there are no restrictions on the number of users a Group Administrator can add to their group as long as there are available licenses in the domain.

5.1.1 TO MANUALLY CREATE USERS AND GROUPS

5.1.1.1 Add a Group

- Select the **USERS** page.
- 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 have a defined number of licenses assigned to them by the administrator. Users can only be added to the license group as long as there are available licenses. Both **Policy** and **License** groups have associated **Client Policy** and **Permissions** associated with them.

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

5.1.1.2 Add a User

- To add a new user, click the **New User** button. You will be presented with the **CREATE NEW USER** screen.
- Enter the **PROFILE** for the user. By default, the **Send Welcome Email** and **Generate Temporary Password** options are selected.
- Select the Account Type: **Standard User**, **Administrator**, or **Group Administrator**. 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.

- Select the **GROUP MEMBERSHIP** for the user. By default, all users belong to the **Domain** license group if you have created licenses groups select the group to which you are assigning the user. You may also 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.
- 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. OPM does not support Onsight 2500 device settings.

5.1.2 WELCOME EMAIL

The Welcome email will notify 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: The Welcome email will contain a Login to Onsight Connect link which will launch Onsight Connect and direct it to your Onsight Platform Manager's URL.

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.

5.1.3 USER EMAIL REQUIREMENT

Email addresses are now optional for user accounts within OPM. However, if a user does not have a configured email address, they will not 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 will not confirm to them whether anything was actually sent. On the user's profile page, the Resend Welcome Email will be hidden if the user has no email address.

Emails are required under the following conditions:

a. External Guest users require a valid email address or phone number to invite.
b. The Account Owner 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 the **SSO** page.

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 address. **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 will not 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", 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.

5.1.4 USER ACCOUNT TYPE

The **Account Type** indicates what level of access the User has to OPM:

Standard User: No Administration Privileges. Allowed to invite External Guests if invite guests is enabled in the domain (requires Enhanced Management Service).

Group Administrator: Access to the Group level settings to which they have been assigned, i.e., modify users that are in their group (change settings, passwords, etc.); create new users within their group and 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 Administrator.

Administrator: Full Access to OPM and the Company Domain Settings. Note: only an Administrator can assign licenses to License Policy Groups.

5.1.4.1 To Assign a Group Administrator

1. Assign a user Group Administrator privileges.
    a. Go to **USERS**, click on the user in the Active list.
    b. In the **Common Actions** area, click on **Change Account Type**.
    c. Select **Group Administrator** from the **Account Type** and click **Change Account Type** to apply the change.
2. 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 and click **OK** to apply the change.
    e. Press **Save**.

5.1.5 EDIT GROUPS

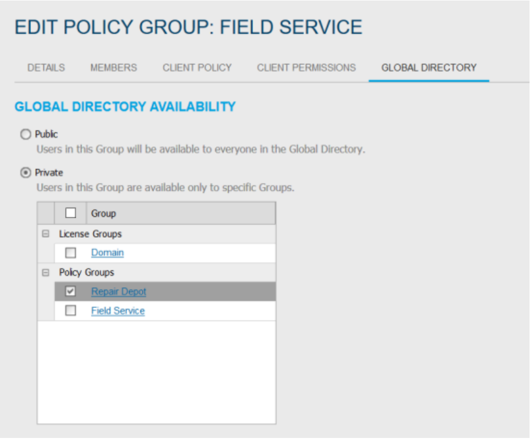
1. On the **USERS** tab, select the group you wish to edit and press the Pencil icon.
2. Assign a group administrator in the **Common Actions** area. Click on **Group Administrators** and a list of users with group administrator privileges is displayed.
3. Select the **Group Administrator**(s) you wish to assign to the group. Press **OK**.
4. Select the **Members** tab, press **add** (+) or **remove** (-) to move members to or from the group.
5. 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**.
6. Select the **CLIENT PERMISSIONS** tab.
    a. Set the action as **Inherit**, **Allow**, or **Deny** for each setting.

    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.

7. Select the **Global Directory** tab to control the group visibility and access in the Global Directory.
    a. **Global Directory Availability** controls whether the current groups is visible in the Global Directory. (Think of this as, who can search for me?)
        i. Select **Public** to make the members of the group visible in the Global Directory.

ii. Select **Private** to make this group visible to specific 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.



EDIT POLICY GROUP: FIELD SERVICE

GLOBAL DIRECTORY AVAILABILITY

○ Public
Users in this Group will be available to everyone in the Global Directory.

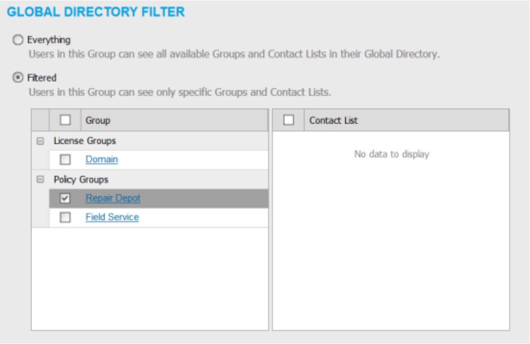
● Private
Users in this Group are available only to specific Groups.

	Group
⊟	License Groups
□	Domain
⊟	Policy Groups
☑	Repair Depot
□	Field Service

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

i. Select **Everything** if you want the group to be able to view all Groups and Contacts in the Global Directory.

ii. 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.



GLOBAL DIRECTORY FILTER

○ Everything
Users in this Group can see all available Groups and Contact Lists in their Global Directory.

● Filtered
Users in this Group can see only specific Groups and Contact Lists.

	Group
⊟	License Groups
□	Domain
⊟	Policy Groups
☑	Repair Depot
□	Field Service

□	Contact List
	No data to display

Note: 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.

5.1.6 IMPORT/EXPORT USERS

The OPM Administrator can import users using a Comma Separated File (CSV) created from the import template. If you are transitioning from Onsight Management Suite (OMS), administrators may also import users from an existing Users and Contacts list created in OMS. Since Onsight users are automatically added to the Global Directory, importing from OMS would only be required for 3rd Party external contacts.

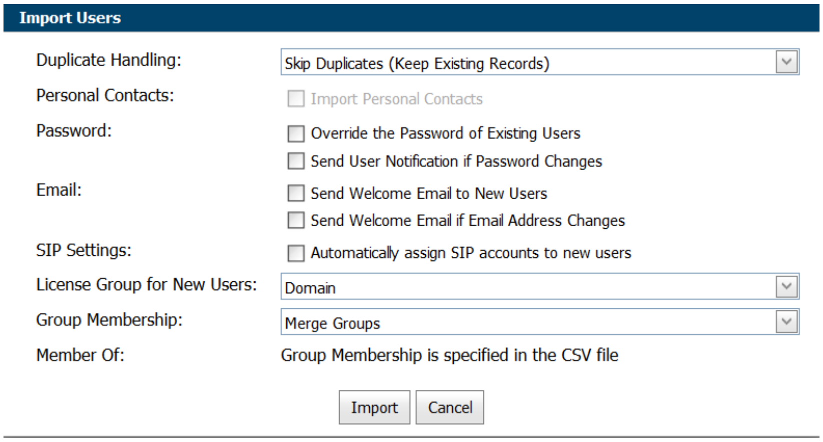
5.1.6.1 To Import Users

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.

1. Go to **USERS**, click on **Import**.
2. Select **Users** from the **Import Mode** drop down list.
   a. 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 may press **More-Export** to download a contacts 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:



Import Users

Duplicate Handling: Skip Duplicates (Keep Existing Records)

Personal Contacts: □ Import Personal Contacts

Password: □ Override the Password of Existing Users
□ Send User Notification if Password Changes

Email: □ Send Welcome Email to New Users
□ Send Welcome Email if Email Address Changes

SIP Settings: □ Automatically assign SIP accounts to new users

License Group for New Users: Domain

Group Membership: Merge Groups

Member Of: Group Membership is specified in the CSV file

   a. Select how you would like to handle duplicates: Skip Duplicates (Keep Existing Records) or Update existing records.
   b. In the **Password** section, select how you would like to import passwords:
      i. Override the Password of Existing Users.
      ii. Send User Notification if Password Changes.
   c. In the **Email** section, select the relevant options:
      i. Send Welcome Email to New Users.
      ii. Send Welcome Email if Email Address Changes.
   d. Select **SIP Settings – 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.
   e. Select the **License Group for New Users**. The default is the Domain which places all users in the standard domain license group. If you have defined other license groups, you may select to which group the users are imported. Alternatively, you may have already defined group membership for all users within the Onsight Users file (csv).
   f. In the **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 to either **Merge Groups** or **Overwrite Groups**. Merging groups results in users who are members of multiple groups.

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

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.

5.1.6.2 To Export Users

1. Go to Users and Groups and click on Export to download a csv file containing a list of all users in the domain.

5.1.7 SELF-REGISTER USERS

The Onsight Administrator can enable the ability for user to self-register for their Onsight accounts. The administrator will distribute 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) e.g. Enter the word show below

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.

5.1.8 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, i**f 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:

- On the **EXTERNAL CONTACTS** page, select **More-Import**.
- 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.
- Select the **File to Import**, press the **Browse** button.
- Press **Upload**.
- You will be presented with the Import External Contacts dialog screen.
    - Select the Duplicate Handling option appropriate for your situation:
        - Skip Duplicates (Keep Existing Records)
        - Update Existing Records
        - Create a Duplicate
- Press **Import.**
- When the import is complete you will be presented with the **Import Results** screen.
- Press **View Report** for details.
- Press **Close**.
- 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 contacts file template.

5.1.8.1 To 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.

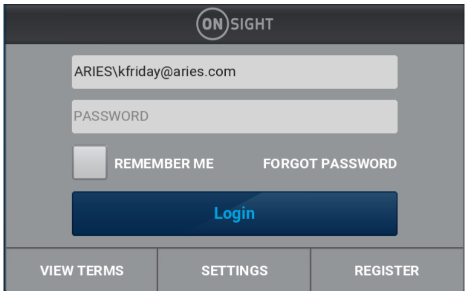
5.1.8.2 Add/remove External Contacts from Lists

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.

5.1.9 ON PREMISES - MANUALLY CONFIGURING THE OPM PATH

ON PREMISES: This section only applies to users who have installed **Onsight Platform Manger – On Premises**..

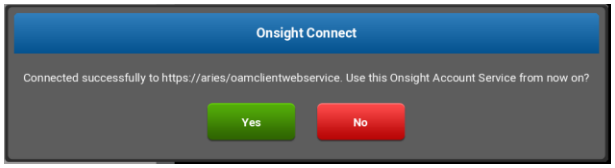
On Premises users who are logging in for the first time without using the Welcome message link will need to enter the OPM Server address as part of their user name on the initial login. The format must be [OPM URI]\user@domain.



ARIES\kfriday@aries.com

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 username and password to login or set the autologin feature.

Onsight Account Service Confirmation:



Onsight Connect

Connected successfully to https://aries/oamclientwebservice. Use this Onsight Account Service from now on?

ON PREMISES: Onsight 5000HD users must manually configure the OPM Server on first login since they do not have the option of using the Welcome Message link.

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: [http|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: [http|https]://[host]\user@domin. Path will be set to 'OamClientWebService'. Scheme and host are used as-is.

* Only https schemes are accepted.

6 Settings

The OPM Administrator can configure the Settings for each Onsight endpoint to comply with your desired 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 by OPM during the login process.

6.1 ACCOUNT

6.1.1 • ACCOUNT INFORMATION

- 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.
- 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.
- Also in the **Common Actions** section, you **Change Account Owner**. This allows you to specify the primary OPM Administrator for your Onsight Account Domain.

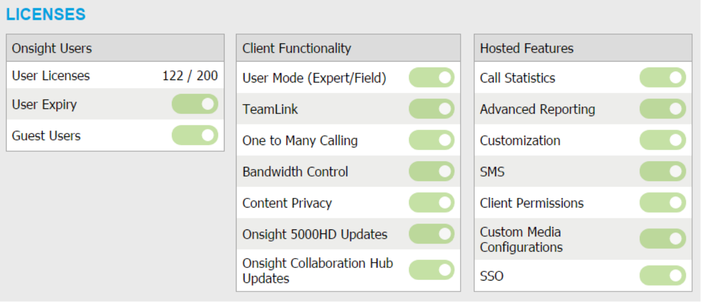
ON PREMISES: When managing your own server, Super Administrator access is not applicable. Call Librestream Support is assistance is required.

Change Account Owner allows the 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.

6.1.2 LICENSES

The licenses enabled in your Onsight Domain are listed in the **LICENSES** section. They are divided into 3 main categories: Onsight Users, Client Functionality, and Hosted Features.

Figure 1: Licenses



LICENSES

Onsight Users	
User Licenses	122 / 200
User Expiry	●
Guest Users	●

Client Functionality	
User Mode (Expert/Field)	●
TeamLink	●
One to Many Calling	●
Bandwidth Control	●
Content Privacy	●
Onsight 5000HD Updates	●
Onsight Collaboration Hub Updates	●

Hosted Features	
Call Statistics	●
Advanced Reporting	●
Customization	●
SMS	●
Client Permissions	●
Custom Media Configurations	●
SSO	●

6.1.2.1 Onsight Users

User Licenses: lists the number of used licenses vs the total number of licenses.

User Expiry: enables the ability to set expiry dates on user licenses.

External Guest Users: enables the ability to send external guest invites.

6.1.2.2 Client Functionality

User Mode (Expert/Field): enables the ability 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 tunnelling 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 not supported, public internet access is required to communicate with TeamLink servers.

One to Many Calling: enables the ability to set Windows PCs as conference hosts. When enabled, a Windows PC 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 Windows PC. 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 5000HD Updates: enables the ability to deploy software updates to Onsight 5000HD Rugged Smart Cameras.

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

6.1.2.3 Hosted Features

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

Advanced Reporting: enables the ability to generate an export Advanced Call Statistic reports.

Customization: enables the ability to customize Onsight Platform Manager messages sent to Onsight users. Messages are text and html based.

SMS: enables the ability to send External Guest Invites via SMS.

Client Permissions: enables the ability to control user access to endpoint settings.

Custom Media Configurations: enables the ability to deploy custom media configurations via Client Policy.

SSO: enables Single Sign On support for your domain. See the SSO section for setup details.

6.2 USERS

1.1.1 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 are based on UTC however, the Default Time Zone setting will adjust the time stamp data within OPM for display purposes only.

Librestream Onsight Devices must have the accurate date and time set to use the Onsight Connect Service. SSL relies on time/date accuracy to perform authentication.

6.2.1 EXTERNAL GUEST USERS

- To enable **External Guest Users** check **Allow users to invite guests**. Default: Enabled.

- If External Guest Licenses is enabled, **SMS Invitations** is enabled by default. This allows users to use text messages for guest invitations.
- Set the **SMS Max Message** to User Length to set 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.
- Set the **Password** control for External Guest Users – Guest users must change 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.
- Set the **Confirmation** control. The host will receive a confirmation email that the invite was sent.
- To allow users to choose the expiry date, Users can check expiry time when inviting guests. Default: Disabled.
- Set **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.

6.2.2 EXTERNAL GUEST INVITATION DEFAULTS

- Set **Expiry** number of days for the Guest Users.
- Set whether **Users can choose the expiry time when inviting guests**. Default: Disabled.
- Set whether to **Deactivate guest user account when removed from contact list**. Default: Disabled.
- Set whether to **Include option for guest to call host immediately**. Default: Enabled.

6.2.3 GLOBAL DIRECTORY OPTIONS

- Set whether **Contacts are public by default**. Contacts that do not belong to any Contact List will be available to everyone in the Global Directory.

6.3 SECURITY

The OPM Administrator configures Security so that each Onsight Connect endpoint complies with your desired Policies.

6.3.1 PASSWORD POLICY

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

6.3.2 PASSWORD EXPIRATION

1. Set the **Enable Password Expiration** option.
2. Set the **Password Expires** length in days.
3. Set to **Warn Users Before Expiration** length in days.

6.3.3 LOGIN POLICY

1. Set the **Maximum Login Attempts** and **Account Lockout Duration** in minutes.
2. Click **Save** to save the changes.

6.3.4 SELF REGISTRATION PAGE

OPM Administrators have the option of allowing users to self-register for an Onsight User Account. This feature is only available if enabled on the Security page of Onsight Platform Manager by the OPM Admin.

1. Select **Enable Self-Registration**.
2. **URL**: Note the URL will need to be sent to users who will be self-registering for an Onsight account.
3. **Key**: To prevent unsolicited registration attempts, either enter a Registration Key or press Generate Random Key. Users will need to enter the **Key** when registering for an Onsight account.
4. Send an email notice with the **URL** and the **Key** to the list of users who will be self-registering. (See a sample email notice that you can send through your standard email program below).
5. **Account Activation Method**: When enabled, **Administrators must approve accounts registered using the Self- Registration Page** before the account is activated.
6. **Notification:** When enabled, **Notify Administrators by email when an account is registered** - the administrator will receive a notification email when an account is registered.
7. **Email**: When enabled, **Require Email Address for Self-Registered Accounts** - the user must provide an email address to register.
8. Set the **Allowed Email Domains** if you wish control from which email domains users are authorized to register for an Onsight account. If left blank, no restrictions exist.
9. **Save** the changes.

6.3.4.1 • Sample Self-Registration Email Notice:

Below is a sample email that an OAM Administrator would send to employees that need to self-register for an Onsight Connect Account.

Subject: Onsight Connect Account Self-Registration

Onsight Connect Account Self-Registration is now available. Please sign up for your account at the following link:

Registration URL:
https://onsight.librestream.com/OPMAdministrator/AccountServices/Register.aspx?id=librestream.com

You will need to create your own User Name and Password. For example: john.doe.

Enter the **Self Registration Key**: fjrjl9Yf7&tst

Enter the **code word** displayed on screen in the confirmation box.

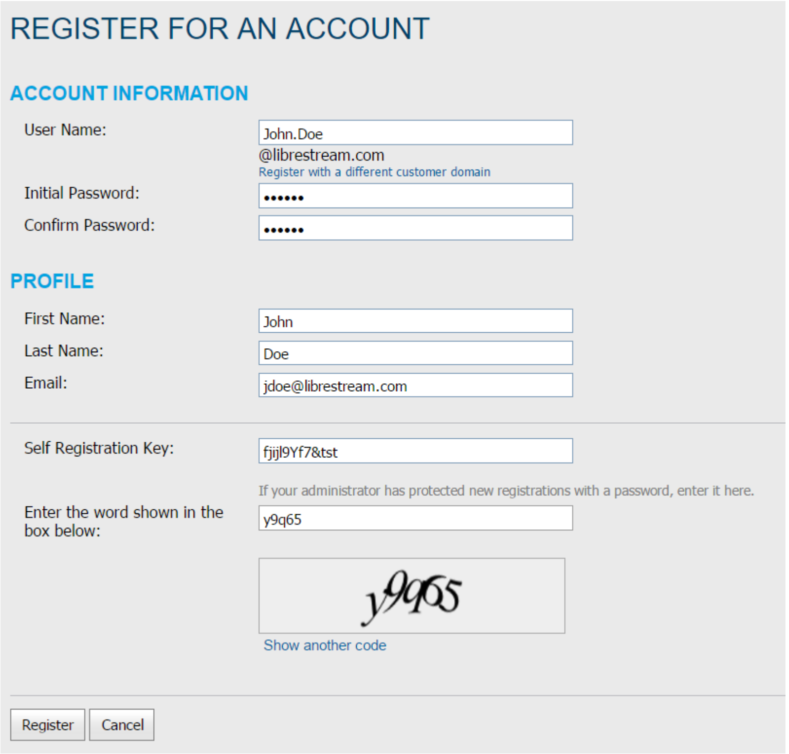
When your account has been approved, you will receive a confirmation email. To begin using Onsight, log in to Onsight Connect with the Username and Password you created.

Regards,

Onsight Platform Manager

6.3.4.2 • Self-Registration Page Example

The Self-Registration URL (and Key if enabled) is sent in an email to the user. The user can Register for an Onsight Account by providing the following information: User Name, Password, First Name, Last Name, Email and the Key. The User Name domain will match your enterprise's Customer domain. Enter the information and press **Register**. The Onsight Administrator will receive an email notification (if enabled) and must approve the self-registration request (if enabled).



REGISTER FOR AN ACCOUNT

ACCOUNT INFORMATION

User Name: John.Doe @librestream.com
Register with a different customer domain

Initial Password: ••••••

Confirm Password: ••••••

PROFILE

First Name: John

Last Name: Doe

Email: jdoe@librestream.com

Self Registration Key: fjijl9Yf7&tst

If your administrator has protected new registrations with a password, enter it here.

Enter the word shown in the box below: y9q65

6.4 SSO

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

6.4.1 SINGLE SIGN-ON

To begin configuring SSO, check the **Enable Single Sign-On** box 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.
- Select **Offline Login** if you would like users to be able to login to Onsight Connect endpoints when network access is not available. In this scenario if a user for some reason cannot reach the **IdP,** they would still be able to log in to Onsight Connect.

6.4.2 SAML CONFIGURATION

6.4.2.1 LOCAL SERVICE PROVIDER SETTINGS

These settings will tell the **SSO Identity Provider** how to communicate with **OPM**, the Service Provider. The SP Server Provider Metadata file is exported and then imported into your IdP to provide the configuration details.

- **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 name of the Entity ID for the IdP.
- **ACS URL**: provides the 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**.

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).

6.4.2.2 PARTNER IDENTITY PROVIDER SETTINGS

These settings will tell **OPM** how to communicate with the **SSO Identity Provider**. In most cases, you can use the **Import IdP Metadata** feature to configure **OPM** with your **Partner Identify Provider Settings**. Importing the metadata will provide the **Entity ID, SSO URL, SSO binding, Signature Algorithm,** and **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** and **Require Encrypted Assertions**.

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, enable **Sign Authentication Requests**.
5. If required, select the **Signature Algorithm**.
6. If required, select the **Digest Algorithm**.
7. If required, enable **Require Signed Responses**.
8. If required, enable **Require Signed Assertions**.
9. If required, enable **Require Encrypted Assertions**.
10. Press **Import IdP Metadata** to import the **IdP metadata file.** The metadata file will normally contain the IdP Public Certificate.
11. 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.

6.4.3 USER IDENTITY FEDERATION

User Identity Federation defines how enterprise users map to Onsight users.

6.4.3.1 USER IDENTITY MAPPING

Identity mapping provides the link between the user information sent via the SAML assertion and the corresponding Onsight Account Fields. This link 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**:
   - **User Name** – Onsight Account User name
   - **Email Address** – Onsight Account Email Address

   - **Federated SSO Id*** – Onsight user's associated **Federated SSO Id**. This is defined by the Onsight Administrator and can be included as part of the Imported User list. This may be mapped to either the **Subject Name Id** or an **Attribute** of the SAML Assertion.

2. Select the **Mapped IdP Attribute** to be compared to the **Onsight Account Field**:
   - **Subject Name ID**
   - **Attribute** – set the **Attribute Name** of the **Attribute** to be compared to the **Onsight Account Field**

* **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).

6.4.3.2 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.

6.4.3.3 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.

6.4.3.4 SSO CERTIFICATE SETUP

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**.

- To configure OPM to use the SSO certificate go to **Site Administration – Server Settings – General**.
- In the SSO section, paste the certificate's SHA1 thumbprint in the **Local Service Provider Certificate SHA1 Hash** text box.
- To verify the certificate, go to **Customer Portal – Settings – SSO**.
- Verify the certificate is available for use by OPM. Click the **Download SP Certificate** button.
- The certificate should be downloaded successfully.

6.4.3.5 NOTIFY EXISTING USERS

Once you have completed the SSO setup, you can send instructions to your existing users via email. Press the **SEND INSTRUCTIONS** link in the **Notify Existing Users** section. 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.

6.5 SIP

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

6.5.1 SIP SETTINGS

6.5.1.1 Auto-Assignment

It is recommended that SIP accounts can be automatically assigned to self-registered users to simplify configuration.

1. Enable **Automatically assign SIP Accounts to self-registered users**.

Note**: Automatically assign SIP accounts to External Guest users** is enabled by default and is displayed for reference.

6.5.2 SIP ACCOUNTS

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.

6.5.2.1 SIP Settings: Onsight Connect Hosted SIP Service

Onsight Connect Hosted SIP Service is used when you have subscribed to Librestream's Onsight SIP Service. The Settings are read-only since SIP account information is automatically assigned by Librestream to your OPM domain. SIP Accounts are automatically assigned to each user when 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.

6.5.2.2 SIP Settings: Multiple Accounts

Multiple Accounts are used when you 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.

6.5.2.3 SIP Settings: 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.

6.5.2.4 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).

6.6 SOFTWARE

6.6.1 SOFTWARE UPDATES (ONSIGHT CONNECT FOR WINDOWS AND ONSIGHT 5000HD)

The OPM Administrator can select which version of **Onsight Connect for Windows** and **Onsight 5000HD** are available for download by Onsight 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 Onsight Connect for Windows and Onsight 5000HD.

If Latest Published Version is selected, users will receive notifications at the Onsight Connect login screen when a new version has been published and is ready for download.

Note: If you have purchased Onsight Collaboration Hubs, software updates are managed by Librestream. Users can check for updates by selecting SETTINGS-ONSIGHT COLLABORATION HUB-CHECK FOR UPDATES.

ON PREMISES: Refer to the Onsight Platform Manager – Installation Guide for details on deploying update packages for Onsight Connect for Windows, Onsight 5000HD, and Onsight Collaboration Hub.

6.7 CLIENT POLICY

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

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

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.

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 Section 9: Client Policy and Client Permissions for details.

Local Privacy

Onsight 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 the Disable recordings and save snapshots to the Group's Client Policy.

WebEx CMR Compatibility

Enabling WebEx CMR Compatibility allows Onsight Endpoints to call into WebEx Meeting rooms and act as a video/audio streaming endpoint. WebEx Meeting rooms will not accept calls from Onsight unless this feature is enabled.

6.8 SMS

If you have subscribed to SMS, SMS Invitations are enabled within your Onsight domain. It allows users to send External Guest invites through an SMS Messaging Service. Librestream configures the SMS Settings page for the Customer - changes must not be made to these settings. Please contact Librestream for assistance if you are experiencing any issues with SMS.

6.9 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

OPM 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.

6.9.1.1 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

1. Email Sender Address: Enter the address to which you would like the user to reply.
2. Company Logo URL: add your company's logo to the Onsight email notifications.
3. Support Contact Information: add information on how to contact your Company's Support desk.
4. Company Message: add a custom message for your Onsight domain users.
5. Account Created Message:
    a. Subject: add a Custom Subject to your Account Creation notification email.
    b. Title: add a custom title to your Account Creation notification email.
6. External Guest Invitation Subject: add a Custom Subject to your External Guest Invitation email.
7. External Guest Invitation Title: add a Custom Title to your External Guest Invitation email.

6.9.1.2 SMS Customization

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 **Custom Messages Help** link on the CUSTOMIZATION page.

7 Statistics and Events

Client Activity and **Events** can be viewed on the **STATISTICS AND EVENTS** page by the OPM Administrator.

7.1 CLIENT ACTVITY

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.
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.

7.2 STATISTICS

The Statistics page provides Onsight Call statistics.

1. Set the **Filter Parameters** and click **Apply Filter** to display the Calls activity.
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
    b. FROM
    c. TO
    d. CONNECTIONS
7. Exit the page when done viewing.

7.3 EVENTS

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

1. Set the **Filter Parameters**:
    a. Severity options
    b. Start Date
    c. End Date
2. Click **Apply Filter** to display the Event Log.
3. You are shown a view of:
    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.

7.4 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 usage review include:

- Identifies top users as potential leaders
- Identifies candidates for mentorship/coaching
- Underscores management's support and interest in the new technology

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. Overall Usage Summary
2. Select the Start Date and End Date of the report.
3. Select the Groups to include in the report, the default is **All Users**.
4. 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.
5. Select the Number of Results to include in the report.
    a. 10, 25, 50 or 100
6. Click **Run Report**.
7. Click **Export** to download and view the results in comma separated, csv, file format.

8 Onsight Connect for Windows – Installation

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 vs Enterprise** - available at http://www.onsight.librestream.com.

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.

9 Client Policy and Client Permissions

Client Policy allows you to control endpoint behaviour. The policy is assigned to a Group and applied to the group members each time they log in to an Onsight Connect endpoint. Whether users are logging in to a Windows PC, iOS or Android smartphone, or an Onsight Smart Camera their assigned client policy will be applied.

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

Client permissions determine authorization for user access to settings on an Onsight endpoint. For each setting, you can select either **Allow**, **Deny** or **Inherit** to set the permission access to the setting. When a user is logged into Onsight Connect Software, **Allow** will let them edit the setting, **Deny** will prevent access, 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.

10 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:

http://www.librestream.com/products/termsofuse.html

11 Librestream Contact Information

Website

www.librestream.com

Head Office

Librestream Technologies Inc.

895 Waverley St., Suite 110

Winnipeg, Manitoba

Canada, R3T 5P4

General Inquiries

Email	information@librestream.com
Phone	+1.204.487.0612
Fax	+1.204.487.0914

Support

Email	support@librestream.com
Phone	+1.204.487.0612
Fax	+1.204.487.0914