ONSIGHT

USER MANUAL

Onsight Account Manager

Software Version 7.1

LIBRESTREAM

Document Revision

Librestream
Onsight Account Manager User Manual
Doc #: 400199-06
July 2016

Table of Contents

1 Overview

Onsight Account Manager (OAM) is a secure online tool for system administrators to centrally manage their Onsight user licenses, manage corporate contacts lists and groups, and configure user license policies and settings. Using OAM, administrators can efficiently manage and maintain groups of Onsight users.

OAM provides tools for three main tasks:

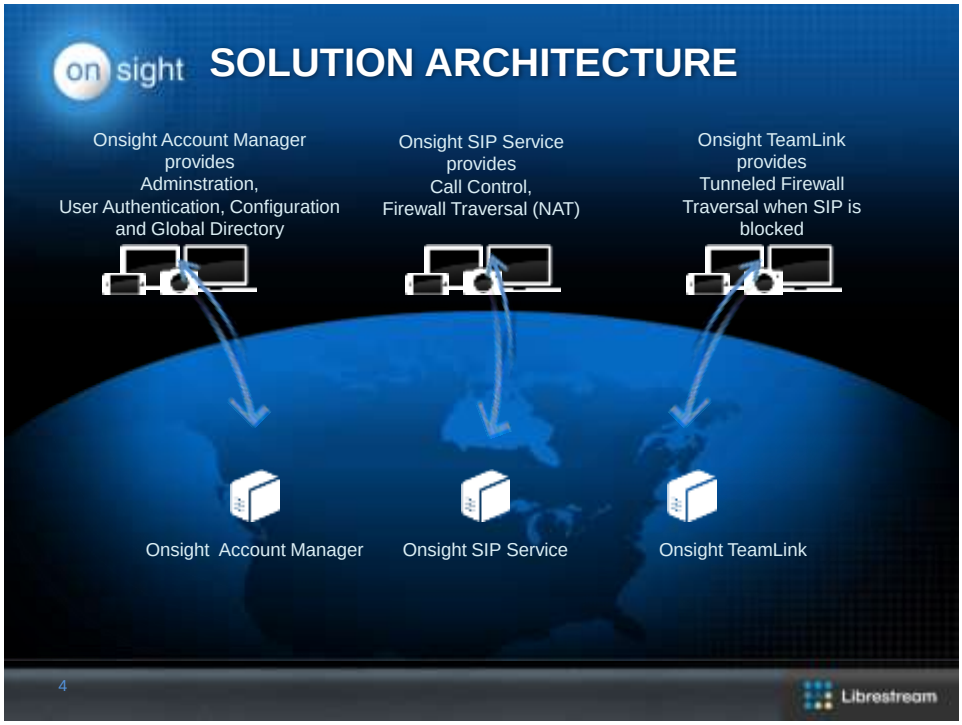
- Create and Manage User Accounts – Onsight Administrators can view and manage the status of their Onsight Connect user license pool such as adding new Onsight Connect users.
- Create and Manage Global Contacts List – The Onsight Global Contact List is a centrally managed contact list that all Onsight users can access.
- Configure Client Policies and Settings – The Onsight Client Policies and Settings are applied to an Onsight endpoint when the user logs in.

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 settings and affect the endpoint's ability to function.

1.1 Onsight Connect Service Solution Architecture

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, iPhone, iPad and Librestream Onsight Device 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, review the online documentation at http://www.librestream.com/support/knowbase.html.



2 Network Requirements

Onsight software requires HTTPS network protocol to communicate with the Onsight Account 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.

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 Account 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 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.

3 Logging into OAM for the First Time

3.1 Logging In

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

To login to OAM, 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 Passwor in paragraph 4.1.1, on page 8.

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

3.2 Home

The OAM Home page provides a Summary of the Users, Licenses and Sessions currently assigned and active on the OAM Server as shown in Figure 2. 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 tabs at the top of the page.

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.

4 Administrator's Settings

4.1 Changing the Administrator's My Profile

The Administrator account can be used to login to an Onsight Connect endpoint as a User as well as being used to configure OAM. My Profile allows the Administrator to configure their personal settings like any other User Account. Once these settings are configured the Administrator can also login to an Onsight endpoint and use it for collaboration.

4.1.1 Changing the Administrator's Password

- Choose My Profile > Profile. This will take you to the Profile configuration page.
- Locate the Change Password link, and enter the new password into both provided fields.
- Click the Change Password button to save your changes.

4.1.2 Changing the Administrator's Client Settings (SIP)

- Choose the **Client Settings** tab.
- Enter the **SIP Server** settings you would like to use for the Administrator Account.

4.1.3 Changing the Administrator's Personal Contacts

- Choose the Personal Contacts tab.
- Click the Global Contacts button to search for a Global contact to add to your Personal Contacts list.
- To Enter a New Contact manually, click the New button.
- Enter the Name, Address, and Type for the contact.
- Click OK to save.

5 Users and Groups

There are three ways the Administrator can add Users:

- Manually Create New User.
- Import User list (Contacts.xml or .csv).
- Have users Register for an account using the OAM Registration web page. You will need to decide if you want users to self-register their User Accounts.

5.1 Manually Adding Users and Groups

Onsight endpoints retrieve User and Group configuration updates from Onsight Account Manager. When a user is added to the Onsight Account domain they can be assigned to a Group.

The five default Groups provided by OAM include:

- All Users – by default includes everyone in the domain: Administrators, Standard users and Guest users.
- Standard Users – by default includes Standard Users and Administrators (Guest users are not included) and allows Client Policy configuration.
- Guest Users – by default includes all Guest Users and allows Client Policy configuration.

- Awaiting Approval – used as an indicator of the number of self-registered users awaiting Administrator approval. Client Policy is not applicable.
- Administrators – indicates the OAM Administrator accounts. Client Policy is not applicable.

The default OAM Groups cannot be deleted. The OAM Administrator can create custom Groups based on any logical partitions e.g. location, business unit, etc.

Groups allow Client Policies (Group Policy) to be applied to groups of users, see section 6.1.5 for details.

Groups Policies can be overridden by the User's Effective Client Policy (User Policy).

5.1.1 To Manually Create Users and Groups

- Select the Users and Groups tab.
- To add a custom Group click on the New Group button in the Manage Users and Groups Panel. Enter the Group name and Description, and then click OK.
- To add a new User click the New User button. You will be presented with the Create New User screen, enter the required information.
- Enter the Profile for the User. Select whether to 'Send Welcome Email' or 'Generate Temporary Password'.
- Check 'Automatically assign SIP account to user' to assign a SIP Account from the Auto-Assignment Pool. See Settings-SIP Settings for details on configuring the Auto-Assignment Pool.
- Select the Group Membership for the user.
- To apply your changes, click the Create New User button at the bottom of the screen.

Send Welcome email will notify the new user of their Onsight Connect account and how to download and install Onsight Connect.

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.

5.1.2 User Account Type

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

Standard User: No Administration Privileges, allowed to invite 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.

Administrator: Full Access to OAM and the Company Domain Settings.

5.1.2.1 To Assign a Group Administrator

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 Change Account Type to apply the change.
2. Assign the Group Administrator to the Group.
   a. Go to Users and Groups, click on the Group to which you wish to assign the Group Administrator.
   b. Press the Modify button.
   c. In the Common Actions area click on Group Administrators.
   d. Select the Group Administrator from the list; click OK to apply the change.
   e. Press Save

5.1.3 Editing Group Policy and Settings

1. On the Users and Groups tab select the Group you wish to edit and press the Pencil icon.
2. In the Common Actions area click on Group Administrators, to see a list of assigned Users assigned with Group Administrator privileges. You can press Delete the remove the group.
3. Select the Members tab to add (+) or remove (-) members from the Group.
4. Select the Client Policy tab to configure Group Policy.
   a. Select 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.
5. Select the Global Directory tab to control the group visibility and access in the Global Directory.
   a. Global Directory Availability controls whether other groups or users can search for the current Group in the Directory. Select Private to limit availability to the selected Groups.
   b. Global Directory Filter controls whether members of the current Group can search for non-members of the current Group in the Global Directory. 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. 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 the current Group.

5.1.4 Import/Export Users

The OAM Administrator can import users using a Comma Separated File (CSV) that was created manually. Administrators can also import users from an existing Users and Contacts list created in Onsight Management Suite.

5.1.4.1 To Import Users

1. Create the file to import. To create a CSV file, follow the format outlined in the OAM 'CSV Import Instructions'*. You can also export a Contacts.xml file from Onsight Management Suite.
2. Go to Users and Groups, click on Import Users.
3. Select Users from the Import mode drop down list.
4. Select the File to Import; click Browse to find the file you are importing.
5. Click Upload to import the file.

Setting Import Personal Contacts in the Import User dialog screen will import all the personal contacts associated with users in the contacts.xml file. (By default only Shared contacts would be imported.) This places all of the Personal contacts contained in the contacts.xml file in the Global directory. Users can add them to their personal contact list by searching the Global Directory. Once they have been added they are present in the contact list when a user logs in to an Onsight Connect endpoint.

*The CSV Import Instructions provide the CSV file format details and is accessible on the *Import from File* page.

5.1.4.2 To Export Users

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

5.1.5 Self-Register Users

See Section 6.7.1 for details.

5.1.6 Configuring External Contacts

By default, any user added to OAM is Automatically added to the Global Directory. To add an External contact that is not an Onsight Connect User such as a third party video conference room, click the 'New Contact' or 'Import' buttons on the External Contacts page.

5.1.6.1 To add an External Contacts List manually

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 will have access to the list.

5.1.6.2 To add External Contacts manually:

1. Click the New Contact button above global contact list. You will be presented with the New Contact screen, shown below.
2. Enter a Name, Address and Type for the endpoint you are adding.
3. If desired, select the Contact List to which you are adding the Contact.
4. Click the OK button to save your changes.•

5.1.6.3 To Import External Contacts:

1. Click Import External Contacts button above the global contact list. You will be presented with the Import From File screen.
2. Verify the Import Mode is set to External Contacts.
3. Browse to the File to Import.
4. Click Upload to import the File.

When Importing External Contacts, the proper file format must be followed as outlined in the CSV Import Instructions.

6 Settings

The OAM 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.

- Guest Users can be enabled so that any active Onsight Connect User can invite a Guest for a period of time as defined by the Administrator. Guest Users have restricted access to OAM but have full access to the Onsight collaboration experience with the exception of the ability to invite another Guest.
- 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 OAM during the login process.

6.1 Account Information

• To view the current Account Information:

- Choose the Settings tab. You will be presented with the Account Information screen.
- Account Information is listed including your Company Name, Customer Domain, etc.
- In the section labelled Licenses, you will see the number of User Licenses, Available Licenses and enabled features such as Guest Users, TeamLink, etc.
- In the Common Actions section, you can Grant Super Administrator Access to Librestream. This allows you to specify the number of hours you would like to grant Librestream access to your domain. Librestream access is granted for assistance with setup or troubleshooting purposes.

Once Super Administrator Access has been Granted it can be disabled by pressing Deny Super Administrator Access, otherwise it will expire after the set time limit.

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

6.2 User Accounts

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

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.

• Guest Users:

- To enable Guest Users check Allow users to invite guests. Default: Enabled.
- If Advanced Management Service 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.
- Set the Password control for 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 Default Expiry to the desired number of days. Default: 1.
- To allow users to choose the expiry date check Users can choose expiry time when inviting guests. Default: Disabled.
- If desired, set Disable recording of images and video to disallow a Guest from making recordings. Default: Disabled. I.E. Guest Users can record images and video.
- if desired, set Disable global directory access to disallow a Guest from searching the Global Contacts Directory. Default: Disabled. I.E. Guest users can access the Global Directory.

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 Deactivate guest user account when removed from contact list. Default: Disabled.
- Set whether to Include option for guest to call host immediately. Default: Enabled.

Global Directory options:

- Set whether Users are public by default. Users that do not belong to any Group will be available to everyone in the Global Directory.
- 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 User Mode

When logging into Onsight Connect on Smart Phones (iOS or Android), users can be configured to operate in two different ways, Expert or Field Mode. The Mode is managed by Client Policy for Groups or can be applied directly to the user account by using the Effective Client Policy.

Expert mode allows users to access all features of the application when using Onsight Connect on Smart Phones (iOS or Android).

Field mode restricts users so that they have limited access to features. While in Field mode the user is guided by the remotely connected expert. Field mode provides a simple interface for a new user to join an Onsight call without requiring any knowledge of the Onsight Connect platform. All control during the call is performed by the remotely connected Expert. The Expert directs the Field user where to point the camera during the call and controls all other aspects such as video streaming, media configuration, zoom, image capture, etc.

Field Mode features:

- Make and Receive calls
- Global Directory – contacts must be added by the Administrator for the Field Mode User.
- Video streaming, Image Capture and Recording is controlled by the remotely connected Expert.
- Telestration – onscreen drawing

6.4 SIP Accounts

SIP Accounts can be automatically assigned when a User is created; they can also be automatically assigned to a User who self-registers to OAM using the Registration URL supplied by the Customer Administrator (see page 20).

When a Customer is hosting their own SIP Server, SIP Accounts can be entered into the Auto-Assignment Pool using Multiple Accounts or a Shared Account. Note that when using a Shared Account, the SIP URI (a.k.a. the SIP address) is automatically generated from the SIP URI domain and the User ID associated with the OAM User account.

The Transport selected (TCP or TLS) must match the configuration of the SIP Server to which you are registering. 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.

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

6.4.1 SIP Settings: Onsight Connect Hosted SIP Service

Onsight Connect SIP Service is used when you have subscribed to use the Onsight SIP Service. The Settings are read-only since SIP account information is automatically assigned by Librestream to your OAM domain; SIP Accounts are assigned to each user when created by the OAM Administrator.

6.4.2 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 first created on the SIP Server with a unique authentication name, password and URI. It is then added manually to the OAM SIP Pool for use as Onsight Connect Users are added.

1. Acquire your SIP Account information from the SIP Server Administrator. The SIP Account information must include the SIP Server Address, 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 Auto-Assignment Pool to Multiple Accounts.
4. On the Public Server tab, set the Server Address to the address provided by your SIP Server Administrator.
5. Add the SIP Accounts information for each user by clicking the New button.
6. In the Add SIP Account window enter the SIP URI (SIP URI = username & sip domain e.g. user@sip.librestream.com), the User Name, Password and Transport.
7. Repeat steps 4 to 6 on the Private Server tab, if required.
8. Save the changes

6.4.3 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 OAM SIP Pool for use as Onsight Connect Users are added. Each SIP account shares the same authentication name and password but has a unique URI.

1. Acquire your SIP Account information from the SIP Server Administrator. The SIP Account information must include the SIP Server Address, 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 Auto-Assignment Pool to Shared Account.
4. On the Public Server tab, set the Server Address to the address provided by your SIP Server Administrator.
5. Set the SIP URI Domain to either Default or Custom.
6. If applicable, enter the Custom SIP Domain.
7. Enter the User Name, Password and Transport.
8. Repeat steps 4 to 7 on the Private Server tab, if required.
9. Save the changes.

6.4.4 •Manually Assigning SIP Account to Users

SIP Accounts can be assigned when a new User Account is created by checking the Automatically assign a SIP account to this user checkbox. 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. The next time the user logs in to Onsight Connect they will begin using their new SIP Account settings.

6.5 Onsight Connect Version Control

The OAM Administrator can select which version of Onsight Connect for Windows is available for download by Onsight Connect Users. You can select the Latest Published Version or a Specific Version from a drop down list. Based on your selection the Users will receive Welcome emails or Guest Invites containing links to download the Version of Onsight Connect for Windows you have chosen.

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.

6.6 Client Policy

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

The Effective Client Policy is the policy associated directly with a user account. If a User belongs to multiple Groups each with its own Client Policy applied, the User will be subject to the settings based on the Effective Client Policy settings for that user. The default Effective Client Policy for a user is to Inherit all settings. Each Client Policy category can be set to Inherit, Override or Clear.

To edit the Effective Client Policy for a User go to Edit User-Client Policy. Set the policy for each setting under Action.

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.

6.6.1.1 Policy Precedence

Users who belong to multiple Groups will have configuration settings applied so that the more restrictive setting is active. For example; Bob belongs to two groups: Sales and Support. The Group Sales 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 Effective 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 Effective Client policy settings.

1. On the Client Policy tab select the Group to which you wish to apply a policy.
2. Click the Choose Settings button. You will be presented with the Choose Settings screen.
3. Select the appropriate category for each setting and click OK.
4. When you are returned to the Client Policies page set the appropriate value for each Category.
5. Repeat the process for each Group to which you want to apply a Client Policy.

By Setting the Remote Management policy you are able to further configure endpoints by pushing configuration and update packages from Onsight Management Suite.

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. tunnel SIP through HTTP/S. Librestream recommends that 'Always use TeamLink' be disabled and only used on a per endpoint basis for troubleshooting purposes.

Client Policies can also be applied to Guest Users

Refer to the TeamLink and Firewall Detect Application Note for details on how to configure the Client Policy for TeamLink.

6.6.1.2 Local Privacy

Onsight Privacy settings allow control over which users can capture still images or recordings during a call.

Select Disable recordings and saving snapshots for ALL participants (Privacy Mode) to prevent the capture of any video or images by any participant in a call. This is the most restrictive privacy setting for streaming media during a call.

To control Local Privacy for individual users, enable Local Privacy Mode. Select the appropriate privacy setting for the user:

- Allow recordings and saving snapshots
- Disable saving snapshots
- Disable recordings
- 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.

6.6.1.3 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.

6.7 Security

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

1. Set the Password Policy. Minimum Length, Minimum Capital Letters and Minimum Non-Alpha Characters can be enforced.
2. Set the Login Policy for Maximum Login Attempts and Account Lockout Duration.
3. User Account Creation lets the Administrator Allow users to create their own accounts. When enabled new users can register for a User Account using the Registration URL. The Administrator can decide whether the Administrator must approve new accounts and whether to Notify Administrators by email when an account is registered.
4. Click Update to save the changes.

6.7.1 User Account Creation (To Self-Register Users)

OAM 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 Account Manager by the OAM Admin.

1. Enable 'Allow users to create their own accounts'.
2. Either enter an Account Creation Key or press Generate Random Key to create the Key if you want Onsight Connect Users to enter additional information for security.
3. Set the Allowed Email Domains if you wish to only allow certain email domains to register to Onsight Connect.
4. Enable Administrator must approve new accounts if you want to approve user accounts before they are activated.
5. Enable Notify Administrators by email when an account is registered if you want to be notified when users register for an account.
6. Send an email notice with the Registration URL and the Account Creation 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.)
7. Save the changes.

6.7.1.1 • Sample Self-Registration Email Notice:

Subject: Onsight Connect Account Registration

Onsight Connect Account Registration is now available; please go sign-up for your account at the following link:

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

Account Creation Key: fae7eee3750e41c49545f11453faf3d5

You will need to create your own User Name and Password. 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 Account Manager

6.7.1.2 • Register for an Onsight Connect Account:

The account Registration URL 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 Account Creation Key. The User Name domain will match your enterprise's Customer domain as configured by Librestream.

6.8 SMS Invitations

If you have subscribed to Enhanced Management Service, SMS Invitations is enabled within your Onsight domain, it allows users to send 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 Message Customization

If you have subscribed to Enhanced Management Service, Message Customization allows you to customize Email and SMS notices the Onsight Connect users will receive from your Company's Onsight Domain.

Messages are sent out for the following events:

- User Account Creation
- User Account Deletion
- Guest Invitation
- Guest Confirmation
- Password Reset Request
- Password Changed Confirmation

OAM defined tags are used to access Company and User specific information for placement in the messages. For more information please refer to the Onsight Customization application note.

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.

The following Messages can be customized:

1. Custom Message: add a custom message for your Onsight domain users.
2. Company Logo URL: add your company's logo to the Onsight email notifications.
3. Support Desk Contact Information: add information on how to contact your Company's Support desk.
4. Account Created Subject: add a Custom Subject to your Account Creation notification email.
5. Account Created Title: add a Custom Title to your Account Creation notification email.
6. Guest Invitation Subject: add a Custom Subject to your Guest Invitation email.
7. Guest Invitation Title: add a Custom Title to your 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. Guest Invitation.
2. Password Reset Request.
3. Password Changed Confirmation.

7 Statistics and Events

Client Activity and Events can be viewed on the Statistics and Events page by the OAM Administrator.

7.1 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.

Set the Filter Parameters and click Apply Filter to display the Client Activity.

Click Refresh to update the list.

Click Export to save a comma separated file of the report.

7.2 Events

The Events page tracks Administrator activity on OAM as well as Server based event messages.

1. Set the Filter Parameters and click Apply Filter to display the Event Log.
    a. The selected Severity options determine what events are logged.
2. Set the date range for the period you wish to review.
3. Click Refresh to update the list.
4. Click Export to save a comma separated file of the report.

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.

Onsight Connect for Windows version 6.0 and later can be installed on either a per-user (Standard) or per-machine (Enterprise) basis. Previous Onsight Connect for Windows versions only supported the Enterprise installation option. The Standard installation option was added to enable 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.librestream.com/support/knowbase.html.

Users who are upgrading to Onsight Connect for Windows v6.1 from version 6.0 or earlier will automatically install the Enterprise version of the software. This is due to the fact that all previous versions of Onsight Connect (or Onsight Expert) used the Enterprise method of installation. If you wish to install the Standard version of the software, you must first un-install the Enterprise version.

Users who have Administrator privileges will automatically install the Enterprise version of Onsight Connect for Windows.

9 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

10 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