



Onsight Platform Manager

Guía del administrador

Derechos de autor

Guía de Onsight Platform Manager

Doc. #: 400199-24 Rev: F

Febrero 2022 (v11.4.7)

La información contenida en este documento está sujeta a cambios sin previo aviso. Queda estrictamente prohibida la reproducción de cualquier forma sin la autorización por escrito de Librestream.

Aviso de derechos de autor:

Derechos de autor 2004-2022 Librestream Technologies Incorporated. Todos los derechos reservados.

Aviso de patentes:

Patente de Estados Unidos # 7.221.386, junto con otras patentes pendientes en Canadá, Estados Unidos y otros países, todas ellas a nombre de Librestream Technologies Inc.

Aviso de marca registrada

Librestream, el logotipo de Librestream, Onsight, el logotipo de Onsight, Onsight Connect, Onsight Flow, Onsight Workspace, Onsight Cube, Onsight Collaboration Hub, Onsight Smartcam, Onsight Platform Manager y Onsight Teamlink son marcas registradas o marcas comerciales de Librestream Technologies Incorporated en Canadá, Estados Unidos, Unión Europea y otros países. Todas las demás marcas registradas son propiedad de sus respectivos propietarios.

Contenidos

Derechos de autor.....	ii
1. INFORMACIÓN GENERAL.....	7
1.1. Arquitectura de plataforma de realidad aumentada Onsite.....	7
2. REQUERIMIENTOS DE RED.....	9
2.1. Configuración de firewall.....	9
2.2. Local.....	9
2.3. Iniciar sesión en OPM por primera vez.....	9
3. PANTALLA DE CONTROL.....	11
4. CONFIGURACIÓN DEL ADMINISTRADOR.....	13
4.1. Cambiar la contraseña del administrador.....	13
4.2. Cambiar los contactos personales del administrador.....	14
4.3. Agregar administradores a OPM.....	16
5. LICENCIAS DE USUARIO.....	19
5.1. Opciones de licencia.....	19
5.2. Modo de captura.....	20
6. ADMINISTRAR USUARIOS Y GRUPOS.....	21
6.1. Administración de política y licencia de dominio.....	21
6.2. Administración de grupo de licencias.....	22
6.3. Administración de usuario y grupos de licencia/política.....	22
6.4. Agregar un grupo.....	23
7. USUARIOS Y GRUPOS.....	25
7.1. Crear usuario nuevo.....	25
7.1.1. Crear un usuario nuevo.....	25
7.2. Correo electrónico de bienvenida.....	27
7.2.1. Correo electrónico local de bienvenida.....	28
7.2.2. Formatos URL locales.....	28
7.3. Requerimiento de correo electrónico de usuario.....	29
7.4. Tipos de cuenta y permisos de usuario.....	31
7.5. Promoción de usuarios y asignación de un administrador de grupo.....	32
7.6. Editar grupos.....	34
7.6.1. Agregar/eliminar miembros del grupo.....	34
7.6.2. Asignación de administradores de grupo.....	35
7.6.3. Editar política y permisos del cliente.....	36
7.6.4. Directorio global.....	38
7.7. Importar/exportar usuarios.....	39
7.7.1. Crear una plantilla de importación de usuarios.....	40
7.7.2. Importar usuarios.....	40
7.8. Exportar usuarios.....	43
7.9. Autorregistro de usuarios.....	43
8. CONTACTOS EXTERNOS.....	45
8.1. Agregar manualmente un contacto externo al directorio global.....	45
8.2. Importar una lista de contactos externos.....	46
8.3. Agregar una lista de contactos externos.....	47
8.4. Agregar/eliminar contactos externos de las listas.....	48

9. CONFIGURACIÓN.....	51
9.1. Tiempo de espera de autenticación.....	51
9.2. Cuenta.....	52
9.2.1. Acceso de superadministrador.....	52
9.2.2. Cambiar propietario de cuenta.....	53
9.2.3. Licencias.....	53
9.2.4. Anonimización de datos.....	56
9.2.5. Anonimización programada.....	56
9.3. Usuarios.....	57
9.3.1. Cuentas de usuario.....	57
9.3.2. Usuarios invitados externos.....	58
9.3.3. Directorio global.....	58
9.3.4. Campos personalizados.....	59
9.4. Seguridad.....	59
9.4.1. Política de contraseña.....	60
9.4.2. Expiración de la contraseña.....	61
9.4.3. Política de inicio de sesión.....	61
9.4.4. Autorregistro.....	61
9.5. Inicio de sesión único.....	62
9.5.1. Inicio de sesión único.....	62
9.5.2. Configuración del lenguaje de marcado de aserción de seguridad.....	63
9.5.3. Federación de identidad del usuario.....	64
9.5.4. Autorregistro de SSO.....	67
9.5.5. Enlaces de aprovisionamiento de usuario.....	68
9.5.6. Notificar a los usuarios existentes.....	69
9.5.7. Local: configuración del certificado SSO.....	70
9.6. Protocolo de inicio de sesión.....	70
9.6.1. Configuración SIP.....	71
9.6.2. Cuenta SIP.....	71
9.7. Onsite Workspace.....	73
9.7.1. Habilitar el acceso a Workspace para usuarios.....	74
9.8. Workspace Webhooks.....	75
9.8.1. Crear y modificar la configuración de un Webhook.....	75
9.9. Actualizaciones de software.....	77
9.9.1. Onsite Connect para Windows.....	77
9.9.2. Notificaciones de liberación nueva.....	77
9.9.3. Actualizaciones para Onsite Cube, Hub de Collaboration y 5000HD.....	77
9.9.4. Actualizaciones de software local.....	77
9.10. Política y permisos del cliente.....	78
9.10.1. Usuarios invitados externos.....	79
9.10.2. Valores predeterminados de invitación de invitado externo.....	80
9.10.3. Precedencia de políticas.....	80
9.10.4. Política y permisos del cliente de grupo.....	83
9.10.5. Privacidad de video remoto.....	84
9.10.6. Compatibilidad con CMR de WebEx.....	85
9.11. Servicio de mensaje de texto.....	85
9.12. Personalización.....	86

9.13. Claves de interfaz de programación de aplicaciones.....	86
9.13.1. Clave generada por API.....	87
9.14. Configuración de inteligencia artificial.....	88
10. ESTADÍSTICAS Y EVENTOS.....	91
10.1. Actividad del cliente.....	91
10.1.1. Generar un informe de actividad del cliente.....	91
10.2. Estadísticas.....	93
10.2.1. Generar un informe estadístico.....	93
10.3. Eventos.....	96
10.3.1. Generar un informe de eventos.....	96
10.4. Informes.....	98
10.4.1. Generar un informe.....	99
10.5. Mapas térmicos.....	100
10.5.1. Generar un informe del mapa térmico.....	101
11. SOPORTE DE IDIOMA.....	103
12. MENSAJES PERSONALIZADOS.....	105
12.1. Crear un mensaje personalizado (formulario).....	105
12.2. Mensajes personalizados y política del cliente.....	106
12.2.1. Modificación de la política del cliente para admitir mensajes personalizados.....	106
13. ACUERDO DE LICENCIA DE USUARIO FINAL.....	109
14. CONTACTO DE SOPORTE.....	111
APPENDICES.....	113
Política del cliente y precedencia de prioridad.....	113
Best Practices.....	118
15.2.1. Cuenta, mejores prácticas.....	118
15.2.2. Usuarios, mejores prácticas.....	120
15.2.3. Seguridad, mejores prácticas.....	121
15.2.4. Software, mejores prácticas.....	123
15.2.5. Política del cliente, mejores prácticas.....	124
15.2.6. Permisos de cliente, mejores prácticas.....	136
Índice.....	a

1. INFORMACIÓN GENERAL

Onsight Platform Manager (OPM) es una herramienta en línea segura para la administración de usuario centralizada. Los administradores del sistema pueden administrar las licencias de usuario de Onsight, los grupos y listas de contactos y configurar las políticas y los permisos de grupos de usuario. Con OPM, los administradores pueden administrar y mantener eficazmente los grupos de usuarios de Onsight.

OPM proporciona herramientas para:

1. **Crear y administrar cuentas de usuario:** los administradores OPM pueden crear usuarios, grupos de política, grupos de licencia, y políticas y permisos del cliente.
2. **Administración de licencia:** los administradores OPM pueden ver y administrar el estado de sus grupos de licencia que incluyen:
 - **Connect Enterprise:** proporciona servicios de llamadas Onsight Connect. En versiones anteriores de OPM (v9 y anteriores) este se denominaba licencia de usuario Onsight. **Connect Enterprise** equivale a la licencia de usuario Onsight.
 - **Workspace Enterprise:** proporciona al usuario acceso a Workspace según los permisos asignados por el administrador. Cargar, ver, compartir y analizar datos, imágenes y grabaciones entre los equipos internos. En versiones anteriores de OPM (v9 y anteriores) esta era una configuración de dominio que se activaba para proporcionar a todos los usuarios acceso a Workspace. Ahora se administra mediante las asignaciones de licencia del usuario.
 - **Workspace Contributor:** proporciona al usuario acceso a su carpeta de carga de **Workspace**, no se puede conceder acceso a otros activos. Centraliza de forma segura el contenido de los clientes, proveedores y terceros colaboradores para su análisis.
3. **Configurar las políticas y los permisos del cliente:** las **Client Policies** y **Permissions** Onsight se aplican a un endpoint de Onsight cuando el usuario inicia sesión.
4. **Generar informes avanzados:** la revisión periódica de las estadísticas de uso, incluido quién se conectó al software, cuántas llamadas hizo y recibió una persona, y la duración total y promedio de las llamadas indicará el nivel de adaptación de la tecnología.

Las tareas descritas son de nivel de administración y no están destinadas a los usuarios finales de Onsight Connect. Varias tareas implican la configuración de **Client Policy** y **Permissions**, afectan el funcionamiento de endpoint.

1.1. Arquitectura de plataforma de realidad aumentada Onsight

La plataforma de realidad aumentada Onsight es un servicio por suscripción administrado centralmente. Un usuario autorizado puede iniciar sesión como cliente Onsight Connect en una PC con Windows, un iPhone o un iPad y conectarse a dispositivos Onsight como el Cube o el Hub.

Una vez inicia la sesión, un usuario de Onsight Connect puede ver y compartir de forma segura video, imágenes, audio y telestración con otro usuario de Onsight. También pueden compartir audio y video con un endpoint de video de terceros que admite el Protocolo de inicio de sesión (SIP). Para obtener más información sobre todas las funciones de Onsight Connect, consulte los documentos en línea en www.librestream.com/support/

2. REQUERIMIENTOS DE RED

El software de Onsight requiere el protocolo de red HTTPS para comunicarse con Onsight Platform Manager.

Tabla 2-1 Requerimientos de red

HTTPS:	443
Proxy web:	Según lo establecido por la política de seguridad de su Enterprise
Wireless Network:	802.11 a/b/g/n
Wired Network:	Se recomienda un puerto Ethernet 10/100 con cable.

2.1. Configuración de firewall

Si el firewall de Windows u otro software de firewall de terceros está ejecutándose en la red en la que está intentando acceder a Onsight Platform Manager, es posible que tenga que agregar excepciones de firewall para los puertos enumerados en la Tabla 1.

Tabla 2-2 Configuración de firewall

Nombre	Protocolo	Puerto	Descripción
HTTPS	TCP	443	Es obligatorio si los endpoints remotos van a acceder al servidor de paquetes o a la interfaz de servicios web a través de HTTPS. Si su configuración de IIS utiliza un puerto distinto al 443, asegúrese de haber permitido ese puerto en su lugar.

2.2. Local

A lo largo de este documento, la información que se aplica solo a las instalaciones locales estará en las secciones On Premises.

2.3. Iniciar sesión en OPM por primera vez

Recibirá su información de inicio de sesión a la administración de OPM desde Librestream a través de un correo electrónico de bienvenida.


Para iniciar sesión en OPM, abra un navegador y navegue a: <https://onsight.librestream.com>. Introduzca el nombre de usuario y la contraseña que recibió en el correo electrónico de bienvenida:

Tabla 2-3 Nombre de usuario y contraseña

User Name:	user@domain.com
Password:	Contraseña

Para evitar el acceso no autorizado al software, debe cambiar esta contraseña inmediatamente después de iniciar sesión por primera vez, como se describe en [Cambiar la contraseña del administrador \(en la página 13\)](#).

Después de iniciar sesión con éxito, se le llevará a la pantalla de control.

 **Nota:** Local: la URL de su servidor OPM dependerá de la URL del servidor asignada durante la instalación. Consulte la guía de instalación Local.

3. PANTALLA DE CONTROL

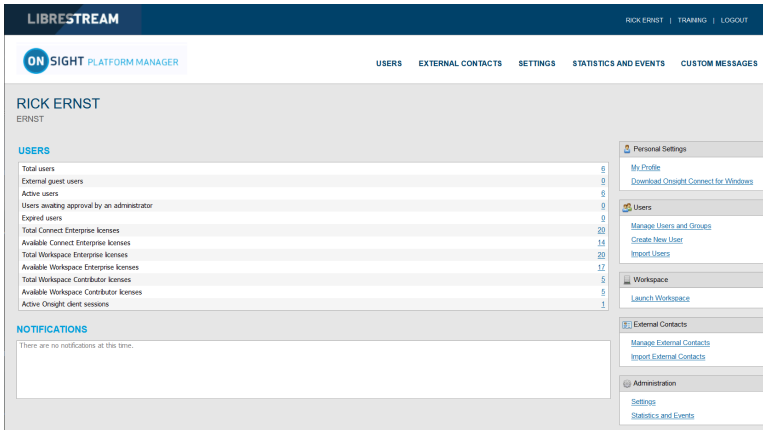


Figura 3-1 Pantalla de control

La página de la pantalla de control incluye una sección de **USERS** y **NOTIFICATION** , además de una lista de enlaces.

USERS

La sección USUARIOS contiene una tabla que muestra los tipos de usuarios, las licencias y la información relacionada:

Total Users

El número total de todos los usuarios (activos y expirados) en el dominio.

External Guest Users

El número total de cuentas activas de invitados externos.

On Premises

Los usuarios invitados externos no son compatibles con las instalaciones locales.

Active Users

El número total de usuarios activos en el dominio.

Users Awaiting Approval by an administrator

El número total de usuarios autorregistrados en espera de la aprobación del administrador. (Para más detalles, consulte la sección de autorregistro).

Expired Users

El número total de cuentas de usuarios expirados.

Total and Available Licenses

En la lista aparecen las licencias totales y las disponibles para cada tipo:

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

4. CONFIGURACIÓN DEL ADMINISTRADOR

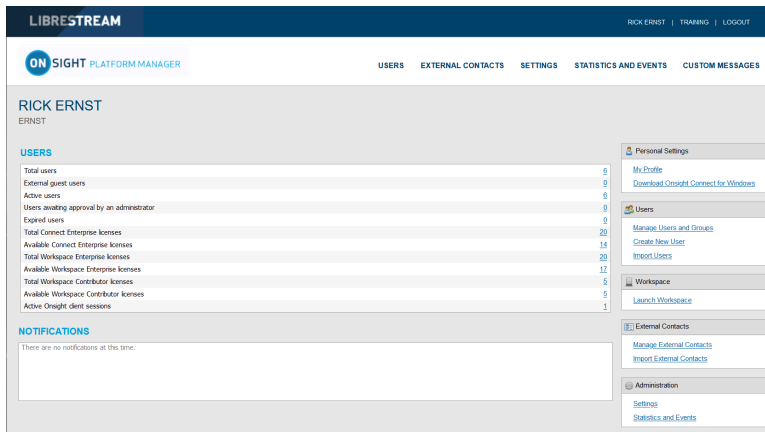



Figura 4-1 Pantalla de control

El propietario de cuenta es el administrador principal. El administrador no utiliza ninguna de las licencias de OnSight Connect Endpoint; por lo tanto, para iniciar sesión en un cliente OnSight Connect como usuario debe asignar una licencia de cliente al propietario de cuenta.

Una vez iniciada la sesión en OPM, busque  **Personal Settings** acceder a **My Profile**. My Profile le permite al administrador configurar sus ajustes personales como cualquier otra cuenta de usuario, incluyendo la asignación de licencias. Una vez asignadas las licencias a la cuenta, el administrador también puede iniciar sesión en cliente OnSight Connect y utilizar las funciones proporcionadas por el tipo de licencia.

Los administradores no necesitan tener licencias asignadas para administrar su dominio de cliente OPM. Puede crear varias cuentas de administrador.

4.1. Cambiar la contraseña del administrador

1. Inicie sesión en OPM y acceda a su pantalla de control.

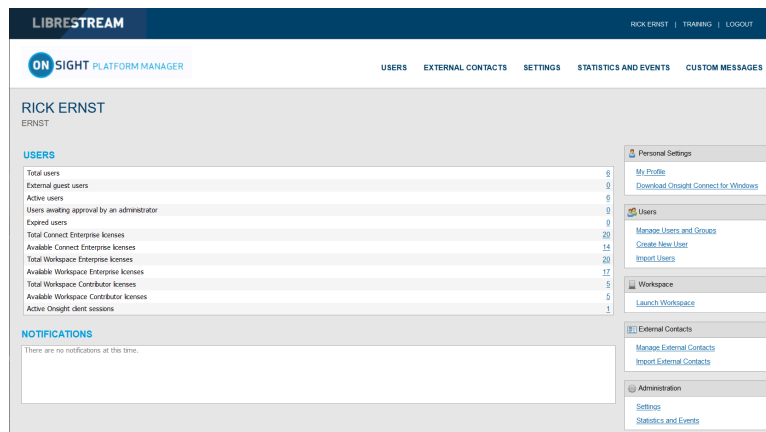


Figura 4-2 Pantalla de control

2. Busque  **Personal Settings** a la derecha y seleccione **My Profile**. Esto lo llevará a la página de configuración **My Profile**.

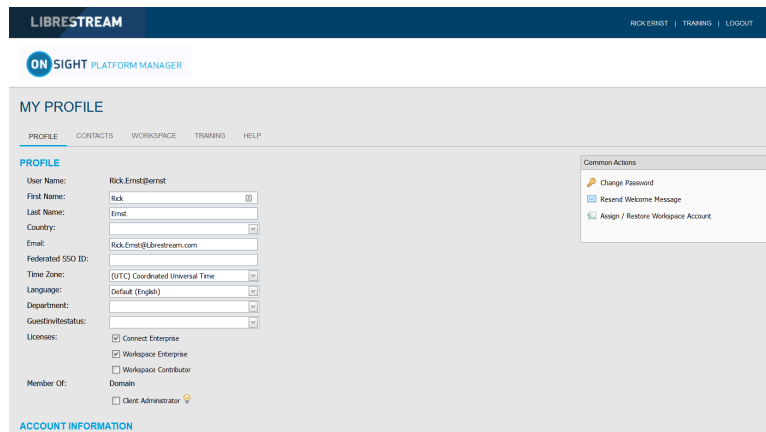



Figura 4-3 Mi perfil

3. Busque **Common Actions** en la derecha y seleccione  **Change Password**. Introduzca la contraseña nueva en ambos campos provistos.

 **Nota:** Su contraseña debe ser diferente a la contraseña actual.

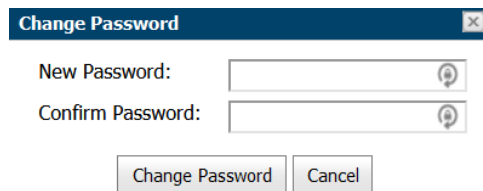


Figura 4-4 Cambiar contraseña

4. Haga clic en el botón **Change Password** para guardar los cambios. Esto completa el procedimiento.

4.2. Cambiar los contactos personales del administrador

Iniciar sesión en OPM.

1. Busque  **Personal Settings** y seleccione **My Profile**.

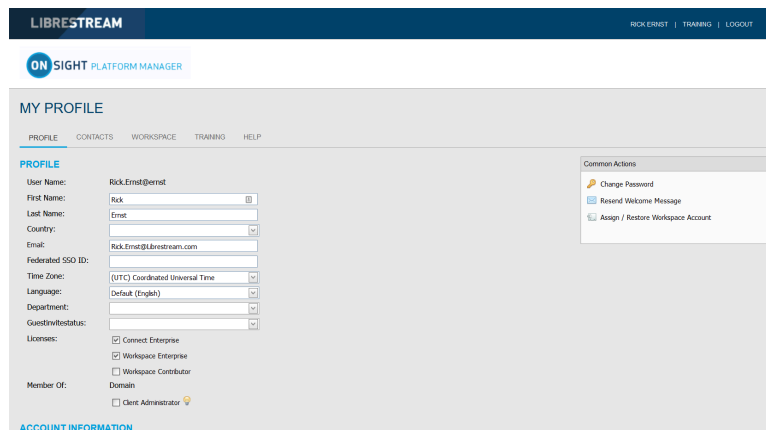


Figura 4-5 Mi perfil

2. Seleccione la pestaña **CONTACTS**.

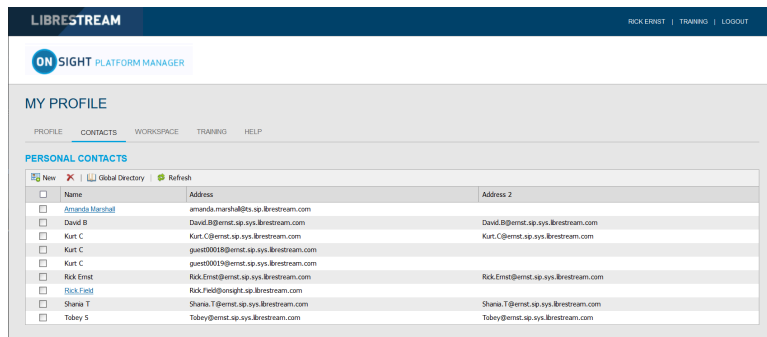


Figura 4-6 Mis contactos

- Haga clic en el icono **Global Directory** para buscar un contacto para agregar a su lista **Contacts**.

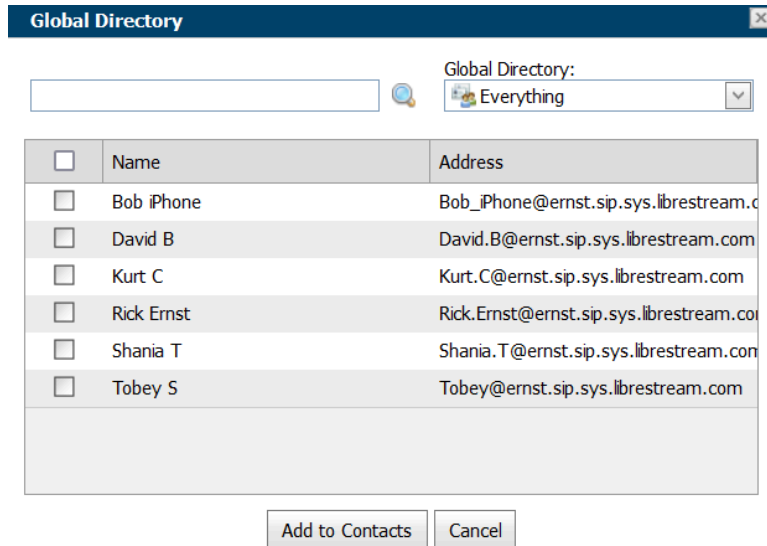


Figura 4-7 Directorio global

- Introduzca un nombre para buscar y presione el icono **Search** para ver una lista de todos los usuarios.
- Habilite la casilla de verificación junto al nombre de la persona y haga clic en **Add to Contacts**.
- Para crear manualmente un contacto, haga clic en el icono **New Contact**. Esto solo es necesario si necesita agregar un contacto de terceros.

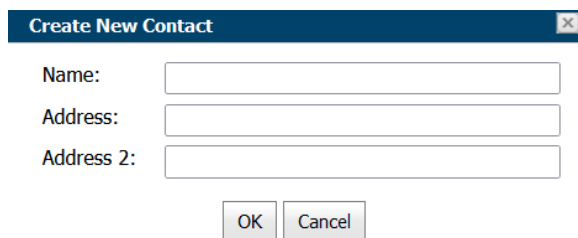


Figura 4-8 Crear contacto nuevo

- Introduzca **Name** y el protocolo de inicio de sesión (SIP) en el campo **Address** para el contacto. También puede introducir **Address 2** opcional.

Nota: La dirección debe estar en el formato SIP URI, por ejemplo, **user@sipdomain.com**.

- Haga clic en **OK** para guardar. Esto completa el procedimiento.

4.3. Agregar administradores a OPM

Debe iniciar sesión en OPM.

Para agregar usuarios, deberá:

1. Seleccionar **USERS** del menú principal. Se muestra la página USERS.

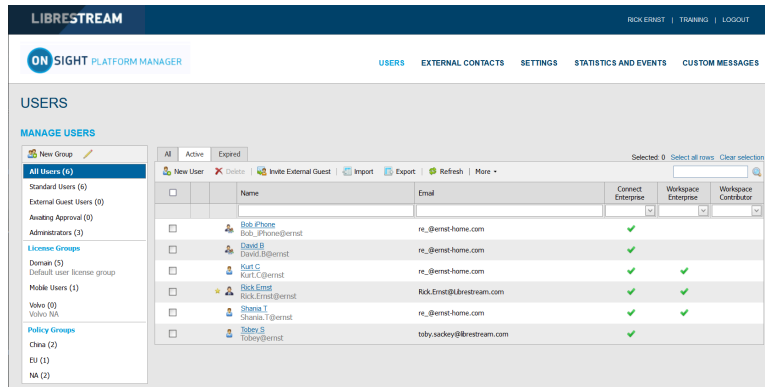


Figura 4-9 USUARIOS

2. Hacer clic en el icono  **New User**. Aparece la página CREATE NEW USER.

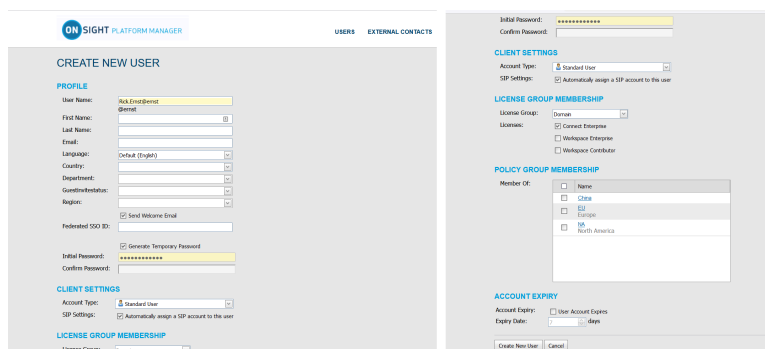


Figura 4-10 Crear usuario nuevo

3. Introduzca la información de **PROFILE** que incluye:

- a. **User Name**
- b. **First Name**
- c. **Last Name**
- d. **Email**



Nota: Send Welcome Email y Generate Temporary Password están seleccionadas de manera predeterminada. Si elige no enviar el correo electrónico de bienvenida, se recomienda deshabilitar también **Generate Temporary Password**. Deberá notificar a los administradores nuevos sus nombres de usuario y contraseñas.

- e. Defina **Language, Country, Department** y **Region** con los menús desplegables, según sea necesario.
- f. Si **Single Sign On** está habilitado, ingrese a **Federated SSO ID** (si es necesario). Consulte la sección **SSO** para obtener detalles.

4. En **CLIENT SETTINGS**, seleccione **Administrator** para el **Account Type**.

5. Verifique que la opción **Automatically assign a SIP account to this user** esté habilitada de manera predeterminada.



Nota: Esto es obligatorio si asigna una licencia de Connect Enterprise y desea que sus administradores puedan iniciar sesión localmente en un cliente de Onsite y hacer llamadas.

6. De manera predeterminada, el **Administrator** pertenecerá al grupo de **licencias del dominio**. No debe asignar al administrador a un grupo de licencias diferente.
7. De manera predeterminada, el **Administrator** pertenece al **grupo de política de dominio**. No debe asignar el administrador a un grupo de políticas del cliente diferente.
8. Se recomienda que no configure la expiración de la cuenta para **Administradores** a menos que sea necesario. Por ejemplo, se asignó un administrador temporal mientras alguien está de vacaciones. Esto completa el procedimiento.

5. LICENCIAS DE USUARIO

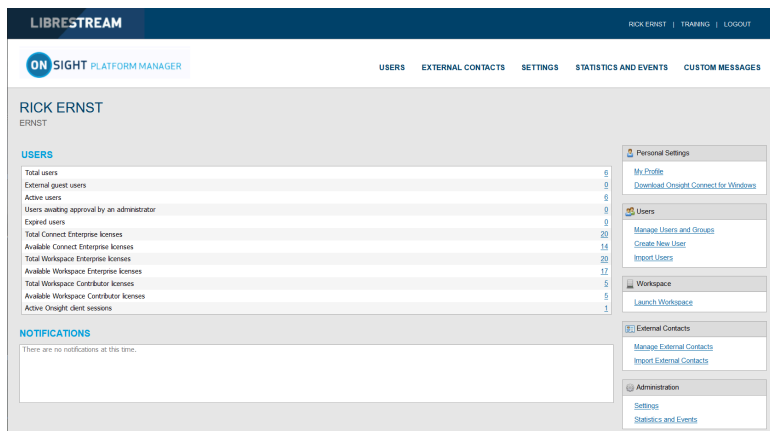



Figura 5-1 Pantalla de control

Onsight Platform Manager admite tres opciones de licencia de usuario:

- **Connect Enterprise:** proporciona servicios de llamada en OnSight (la configuración SIP debe hacerse en el dominio).
- **Workspace Enterprise:** proporciona el acceso a Workspace al usuario Enterprise según los permisos asignados del administrador.
- **Workspace Contributor:** proporciona el acceso a Workspace al usuario colaborador a su carpeta de carga y para editar su contenido, no se puede dar acceso a otros activos al colaborador.

 **Nota:** Los tipos de licencia de Workspace son mutuamente excluyentes. No se puede asignar a un usuario ambos tipos de licencia de Workspace. Cada licencia habilita funciones para el usuario en la aplicación OnSight Connect. Los usuarios pueden tener licencias individuales o múltiples asignadas a su cuenta. Todas las licencias permiten la captura de contenido a nivel local (imágenes y grabaciones).

5.1. Opciones de licencia

La siguiente tabla muestra las combinaciones válidas de asignación de tipos de licencia:

Tabla 5-1 Opciones de licencia

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

Usuario A (Connect Enterprise):

Los usuarios de **Connect Enterprise** pueden iniciar sesión en **Onsight Connect**, hacer llamadas, capturar contenido, y compartir contenido con otros usuarios de Connect Enterprise.

Usuario B (Workspace Enterprise):

Los usuarios de **Workspace Enterprise** pueden iniciar sesión en **Onsight Connect**, capturar contenido, cargar contenido a **Workspace**, y pueden iniciar sesión en Workspace para editar, administrar y colaborar en el contenido. Esto incluye cualquier activo al que se le haya concedido permiso de acceso.

Usuario C (Workspace Contributor):

Los usuarios de **Workspace Contributor** pueden iniciar sesión en **Onsight Connect**, capturar contenido, cargar contenido a **Workspace** y pueden iniciar sesión en Workspace para acceder al contenido de su carpeta de carga. A este usuario no se le puede otorgar acceso al contenido fuera de su carpeta de carga.

Usuario D (Connect Enterprise con Workspace Enterprise):

Los usuarios de **Connect Enterprise** pueden iniciar sesión en **Onsight Connect**, hacer llamadas, capturar contenido, y compartir contenido con otros usuarios de **Connect Enterprise**. Además, los usuarios de **Workspace Enterprise** pueden cargar contenido a **Workspace**. Este usuario también puede iniciar sesión en Workspace para editar, administrar y colaborar en el contenido. Se les puede conceder permisos para acceder a otros contenidos dentro del Workspace fuera de su carpeta de carga.

Usuario E (Connect Enterprise con Workspace Contributor):

Los usuarios de **Connect Enterprise** pueden iniciar sesión en **Onsight Connect**, hacer llamadas, capturar contenido, y compartir contenido con otros usuarios de Connect Enterprise. Además, los usuarios de **Workspace Contributor** pueden cargar contenido a **Workspace**. Este usuario también puede iniciar sesión en **Workspace** para acceder al contenido de su carpeta de carga. A este usuario no se le puede otorgar acceso al contenido fuera de su carpeta de carga.

5.2. Modo de captura

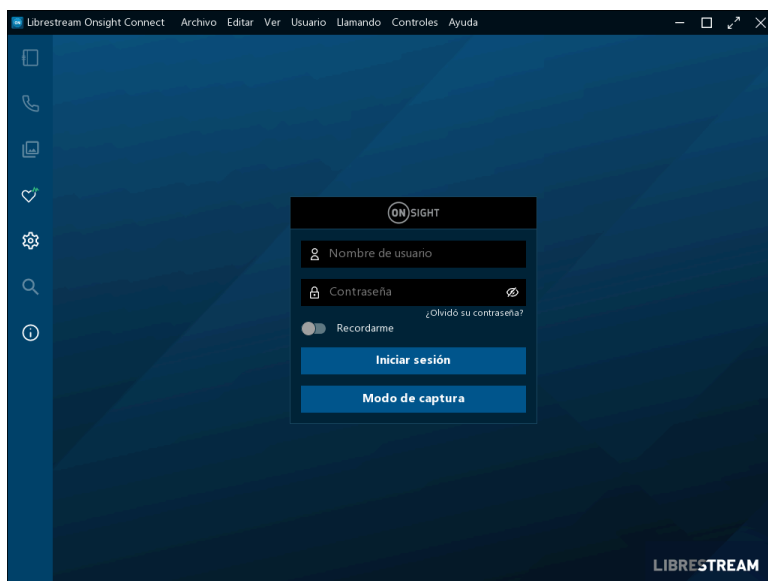


Figura 5-2 Modo de captura

Capture Mode proporciona el uso fuera de línea de Onsight Connect sin necesidad de iniciar sesión. Desde la ventana de inicio de sesión para Onsight Connect, los usuarios pueden presionar el botón **Capture Mode** para ingresar a **Onsight Connect Viewer**. Este habilita el acceso a las fuentes de video para cámaras de dispositivos móviles, así como de dispositivos Onsight como **Cube** y **Hub** sin necesidad de iniciar una sesión de usuario en Onsight.

Los usuarios que no tienen asignada una cuenta de Onsight pueden descargar **Onsight Connect** y capturar contenido inmediatamente. Todo el contenido se guarda localmente en su dispositivo móvil o PC con Windows. Una vez que se les asigne una cuenta, pueden iniciar sesión y acceder a sus imágenes y grabaciones capturadas previamente, las que pueden compartir en una llamada en Onsight o cargarlas en Workspace.

Una vez que un usuario inicie sesión en la aplicación Onsight Connect con un nombre de usuario, **Capture Mode** ya no está disponible en la ventana de inicio de sesión. Un inicio de sesión en Onsight debe utilizarse para obtener acceso a la aplicación desde ese momento.

6. ADMINISTRAR USUARIOS Y GRUPOS

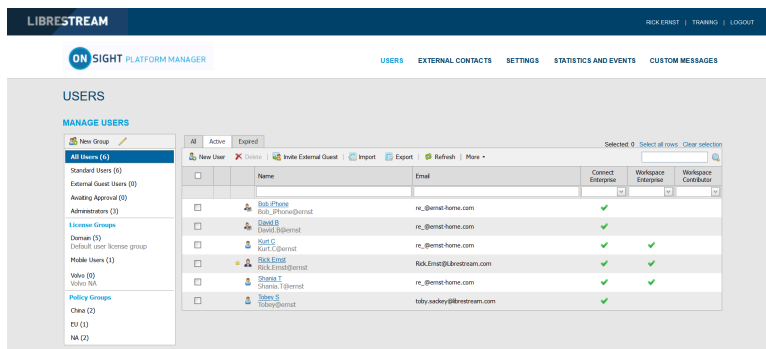


Figura 6-1 Administrar usuarios y grupos

Los administradores de OnSight usan OPM para administrar de forma centralizada las licencias de usuario, las listas de contactos, las políticas y los permisos. Hay dos enfoques principales para la administración de licencias dentro de OnSight Platform Manager. **Select Users** en el menú principal para poder administrar:

- Administración de licencia de dominio
- Administración de grupo de licencia y política

6.1. Administración de política y licencia de dominio

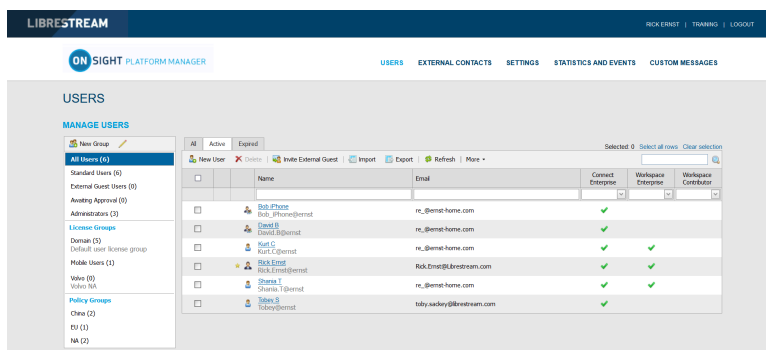


Figura 6-2 Todos los usuarios/grupo de licencias de dominio

El dominio es el grupo de licencias predeterminada. Todas las licencias están bajo el control del dominio, es un grupo de licencia única del que se asignan todas las licencias a los usuarios. Los tipos de licencia que se agregan al dominio pueden ser asignados por un administrador a cualquier usuario del dominio.

Client Policy puede establecerse para todos los usuarios editando el grupo de **All Users**.

Referencia relacionada

[Política del cliente, mejores prácticas \(en la página 124\)](#)

6.2. Administración de grupo de licencias

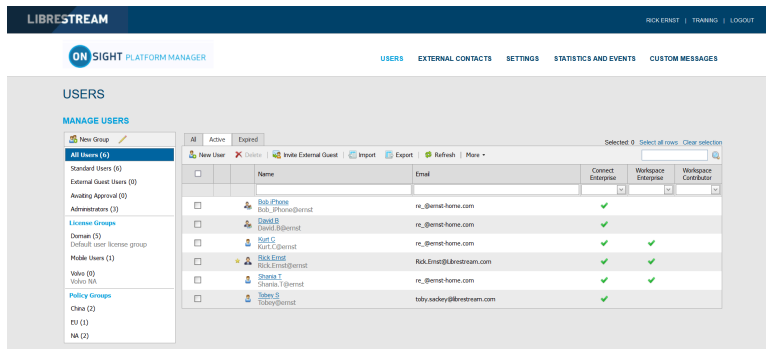


Figura 6-3 Grupos de licencia

La administración del grupo de licencia es un método opcional para administrar las licencias. Se habilita solo bajo petición. Permite a un administrador OnSight crear grupos de licencia y asignar licencias del dominio a los grupos de licencia. Los miembros del grupo se agregan a cada grupo de licencias y se les asignan licencias bajo el control del grupo de licencia.

Cuando se activan los grupos de licencia, el dominio predeterminado sigue activo y actúa como un grupo de licencias independiente. Las licencias se transfieren del dominio predeterminado a los grupos de licencia personalizados. Una vez que se transfiere una licencia, queda bajo el control del grupo de licencias.

Los administradores y los administradores de grupo pueden crear usuarios dentro de un grupo de licencias siempre que tengan licencias disponibles en el grupo. Los usuarios se pueden crear sin licencias, pero se les debe asignar una licencia antes de que estén activos.

Client Policy puede establecerse de forma independiente para cada grupo de licencias.

Referencia relacionada

[Política del cliente, mejores prácticas \(en la página 124\)](#)

6.3. Administración de usuario y grupos de licencia/política

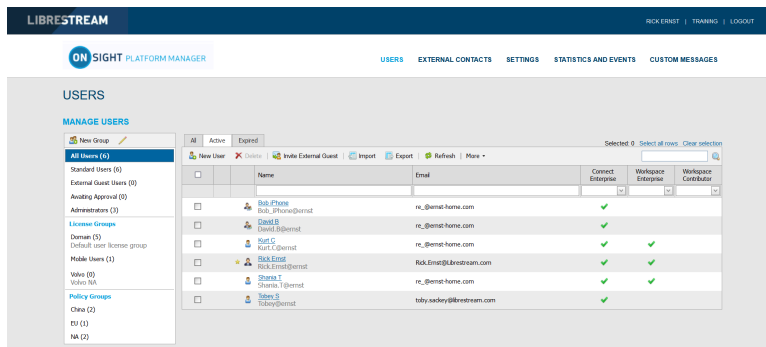


Figura 6-4 Grupos de licencia y política

El administrador de OPM puede crear dos tipos de grupos: **License** y **Policy**.

Grupos de licencia

License Groups son opcionales y pueden activarse a petición. Se usan para aplicar la **Client Policy** y asignar licencias a los miembros del grupo. El administrador puede asignar licencias a diferentes grupos de licencia. Los administradores pueden asignarse a un grupo (administrador de grupo). Por ejemplo, un administrador de OPM asigna 10 licencias de Connect Enterprises a un **License Group**. Se puede asignar un administrador de grupo para administrar y conceder un máximo de 10 licencias de **Connect Enterprise** a un máximo de 10 miembros del grupo. Si un usuario de **Connect Enterprise** se elimina del grupo, la licencia queda disponible para su uso y puede asignarse a un usuario nuevo. El administrador de OPM puede reasignar las licencias al dominio o a otro grupo de licencias.

Los grupos predeterminados no se pueden eliminar.

Grupos de política

Policy Groups se usan para aplicar la política del cliente a los miembros del grupo. Los grupos de políticas no tienen función de administración de licencias. Cuando se usan grupos de política, las licencias se asignan a los usuarios desde el grupo de licencia del dominio.

Anulación por el administrador

Un administrador puede anular el grupo de política para un usuario específico editando la página **Client Policy** del usuario. La configuración de la política del cliente del usuario tendrá precedencia sobre cualquier configuración de la política del cliente de grupo.

Grupos de licencia y uso

El uso de los **License Groups** es opcional y debe estar habilitado para su dominio.

- Puede dejar todas las licencias asignadas a su dominio predeterminado. Si no necesita administrar las licencias para los grupos personalizados, se recomienda administrar las licencias desde el grupo de dominio.
- Puede gestionar la **Client Policy** al usar grupos de política personalizados. Si no necesita administrar la política del cliente para los grupos personalizados, puede establecer la **Client Policy** para todos los usuarios al editar la política del cliente de **Standard Users**.
- Si los **External Guests** están habilitados, puede administrar la política del cliente para ellos al editar la política del cliente de **External Guest Users**.
- Las licencias de dominio se pueden asignar por los administradores y administradores de grupo que se asignaron a los grupos.
- Si los grupos de licencias no están habilitados para su dominio, no hay restricciones en el número de usuarios que un administrador de grupo puede agregar a su grupo, siempre que haya licencias disponibles en el dominio.

Administración de usuario

Las opciones predeterminadas del panel **MANAGE USERS** incluyen:

- **All Users** incluye a todos los integrantes del dominio: Administradores, usuarios no administrativos y usuarios invitados externos. Incluye la configuración de la política del cliente. Cuando se agrega un usuario nuevo, este se convierte automáticamente en miembro del grupo de todos los usuarios.
- Los **Standard Users**, de forma predeterminada, incluyen a los usuarios no administrativos y a los administradores (no se incluyen los usuarios invitados externos). Incluye la configuración de la política del cliente.
- **External Guest Users** (opcional) incluye todos los usuarios invitados externos y permite la configuración de la política del cliente.
- **Awaiting Approval** indica el número de usuarios autorregistrados en espera de la aprobación del administrador. La política del cliente no es aplicable.
- **Administrators** indica el número de cuentas de administrador. La política del cliente no está incluida.
- **License Groups** (opcional) incluye grupos de licencia personalizados y el dominio predeterminado. La política del cliente está incluida.
- **Policy Groups** incluye grupos de política personalizados. La administración de licencias no está incluida.



Nota: Los grupos predeterminados no se pueden eliminar.

Referencia relacionada

[Política del cliente, mejores prácticas \(en la página 124\)](#)

6.4. Agregar un grupo

Iniciar sesión en OPM.

Para agregar manualmente un grupo, deberá:

1. Seleccionar **USERS** en el menú principal. Se muestra la página Users.

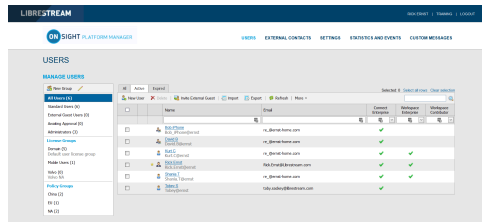



Figura 6-5 USUARIOS

2. Para agregar un grupo personalizado, haga clic en el icono  **New Group** en el panel **MANAGE USERS**. Aparece la ventana Create New Group.

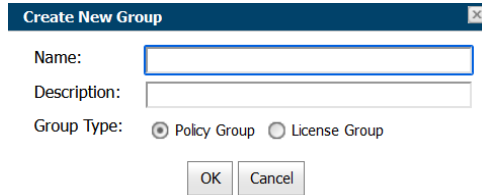


Figura 6-6 Crear un grupo nuevo

3. Introduzca información en los campos **Name** y **Description**.

4. Defina el **Group Type** como:

- **Policy Group**
- **License Group**

5. Haga clic en **OK**.



Nota: Los grupos de licencias deben tener un número definido de licencias asignadas por el administrador. Los usuarios solo se pueden agregar al grupo de licencias siempre que haya licencias disponibles. Tanto los grupos de políticas como los de licencias incluyen políticas de cliente y permisos.

Esto completa el procedimiento.

Para obtener más información, consulte la sección [Política y permisos del cliente \(en la página 78\)](#).

Referencia relacionada

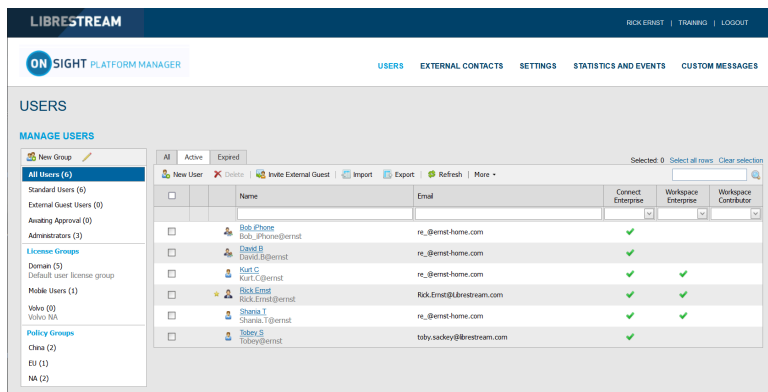
[Política del cliente, mejores prácticas \(en la página 124\)](#)

[Permisos de cliente, mejores prácticas \(en la página 136\)](#)

Información relacionada

[Política y permisos del cliente \(en la página 78\)](#)

7. USUARIOS Y GRUPOS



Hay tres métodos para que un administrador agregue usuarios:

1. Crear manualmente un usuario nuevo.
2. Importar usuarios desde un archivo (por ejemplo, SampleUserImport.csv).
3. Autorregistro mediante la página web de autorregistro de OPM.

7.1. Crear usuario nuevo

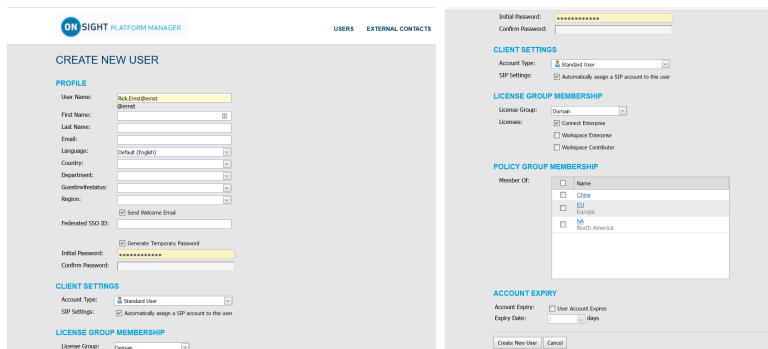



Figura 7-2 Crear un usuario nuevo

Seleccione **USERS** en el menú principal y haga clic en el icono  **New User** para acceder a la ventana **CREATE NEW USER**. Para crear un usuario nuevo, deberá proporcionar los detalles de:

- **PROFILE:** proporcionar detalles de información del usuario que incluyan **User Name, First Name, Last Name, Email** y utilizar los menús desplegables para indicar: **Language, Country, Department** y **Region** etc.
- **CLIENT SETTINGS:** defina el **Account Type** usando el menú desplegable como **Administrator, Group Administrator, o Standard User**.
- **LICENSE GROUP MEMBERSHIP:** asigne el usuario nuevo a un grupo de licencias según sea necesario y habilite la casilla de verificación para indicar el tipo de licencia (**Connect Enterprise, Workspace Enterprise, o Workspace Contributor**).
- **POLICY GROUP MEMBERSHIP:** asigne el nuevo usuario a un **Policy Group** según sea necesario.
- **ACCOUNT EXPIRY:** habilite la opción de **User Account Expires** y proporcione una **Expiry Date** según sea necesario.

y haga clic en el botón **Create New User**.

7.1.1. Crear un usuario nuevo

Iniciar sesión en OPM.

Para crear manualmente una cuenta de usuario nuevo, deberá:

1. Seleccionar **USERS** en el menú principal. Se muestra la página **USERS**.

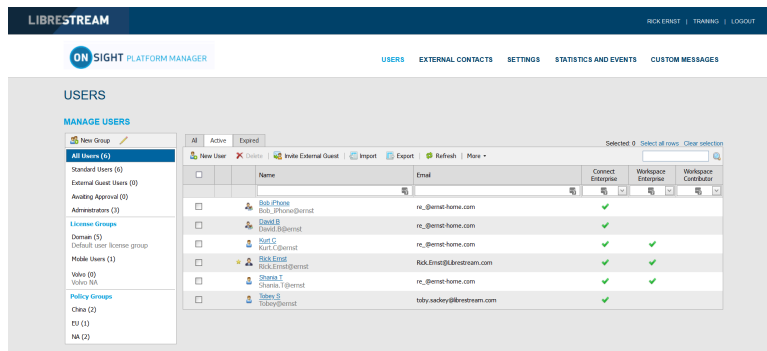



Figura 7-3 Página de usuarios

2. Hacer clic en el icono  **New User**. Se presentará la ventana **CREATE NEW USER**.

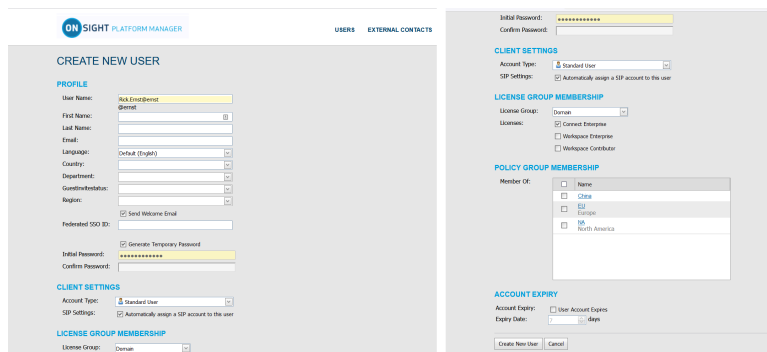






Figura 7-4 Crear un usuario nuevo



Nota: Si falta el icono  **New User**, entonces no puede agregar usuarios nuevos. Revise la configuración de **Client Policy** en **Allow New Contacts**, según sea necesario.

3. Introduzca la información de **PROFILE** para el usuario nuevo. Las opciones **Send Welcome Email** y **Generate Temporary Password** se seleccionan de manera predeterminada.
4. En **CLIENT SETTINGS**, seleccione Account Type:  **Standard User**,  **Administrator** o  **Group Administrator**.
5. La opción **Automatically assign a SIP account to this user** se selecciona de manera predeterminada. Consulte **SETTINGS > SIP** para obtener detalles sobre la configuración de **Auto-Assignment SIP Pool**.




Nota: Se puede asignar o actualizar la configuración SIP de los usuarios existentes desde el grupo de asignación automática al acceder a la página **Users Client Settings** y presionar **Assign Restore SIP Account** en la sección **Common Actions**.

6. Seleccione la **LICENSE GROUP MEMBERSHIP** para el usuario. De forma predeterminada, todos los usuarios pertenecen al **Domain license group**. Si creó grupos de licencias, seleccione el grupo y el tipo de licencia a los que está asignando el usuario. También podría asignar al usuario a un **Client policy group** al seleccionar la casilla de verificación **Member Of** para indicar a qué grupo pertenece.




Nota: Ambos **License groups** y **Policy groups** tiene la configuración de **Client Policy** y **Permission** asociada. Si definió una **Client Policy** dentro del **License group**, no tiene que asignarle un **Policy group** al usuario.

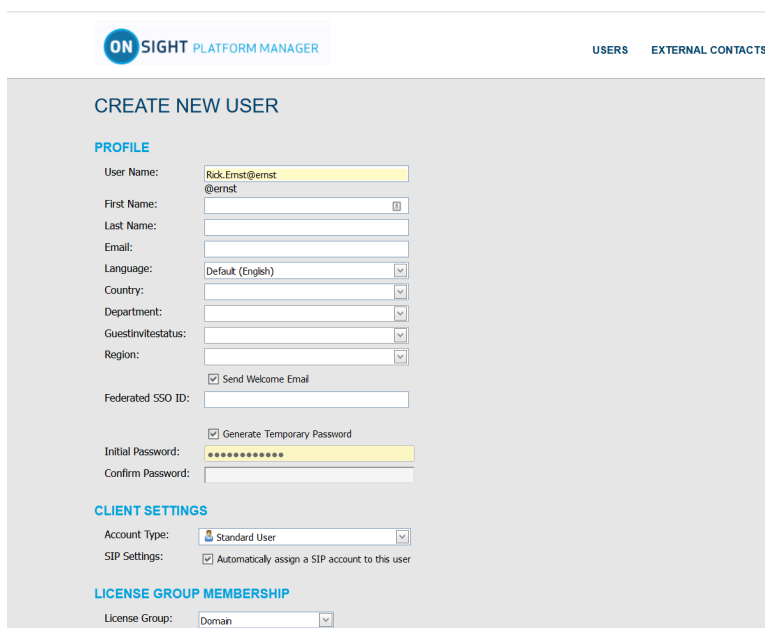


- **Opcional:** Podría establecer la casilla de verificación **User Account Expires** y **Expiry date** del usuario.
- Para aplicar sus cambios, haga clic en el botón  **New User** en la parte inferior de la ventana.
- Para establecer un usuario como **Client Administrator**, haga clic en el nombre del usuario en la lista de la página **USERS**. Seleccione la casilla de verificación **Client Administrator**. Entonces, el usuario puede editar todas las configuraciones en un endpoint.

7. Haga clic en el botón **Create New User**.
Esto completa el procedimiento.

 **Nota:** * La configuración del administrador del cliente para las cuentas de usuario está en desuso. Se recomienda que los usuarios se agreguen a los grupos de políticas para controlar los permisos de los clientes. Sin embargo, los usuarios que actualmente tienen un administrador del cliente habilitado en su cuenta de usuario se pueden administrar a través del grupo de política del administrador del cliente. Además, si está realizando la transición de OMS a OPM, la configuración del administrador del cliente es el único método para otorgar derechos de administrador a un usuario.

7.2. Correo electrónico de bienvenida



The screenshot shows the 'CREATE NEW USER' form in the OnSight Platform Manager. The form is organized into three main sections:

- PROFILE:** Contains fields for User Name (Rok.Ernst@ernst), First Name (@ernst), Last Name, Email, Language (Default (English)), Country, Department, Guestinviestatus, and Region. It also includes checkboxes for 'Send Welcome Email' and 'Generate Temporary Password'.
- CLIENT SETTINGS:** Includes 'Account Type' (Standard User) and 'SIP Settings' (Automatically assign a SIP account to this user).
- LICENSE GROUP MEMBERSHIP:** Includes 'License Group' (Domain).

Figura 7-5 Opción de correo electrónico de bienvenida

El correo electrónico de bienvenida notifica a los usuarios nuevos sobre su cuenta de OnSight Connect y les proporciona los enlaces para **Download and install OnSight Connect** y **Login**. El correo electrónico de bienvenida se puede activar en una casilla de verificación dentro de la sección **PROFILE** cuando se crea un usuario nuevo. A partir de eso, se puede volver a enviar el mensaje de bienvenida, si fuera necesario. Haga clic en **USERS** en el menú principal y seleccione un usuario de la lista de usuarios. Busque **Common Actions** y seleccione **Resend Welcome Message**.

7.2.1. Correo electrónico local de bienvenida

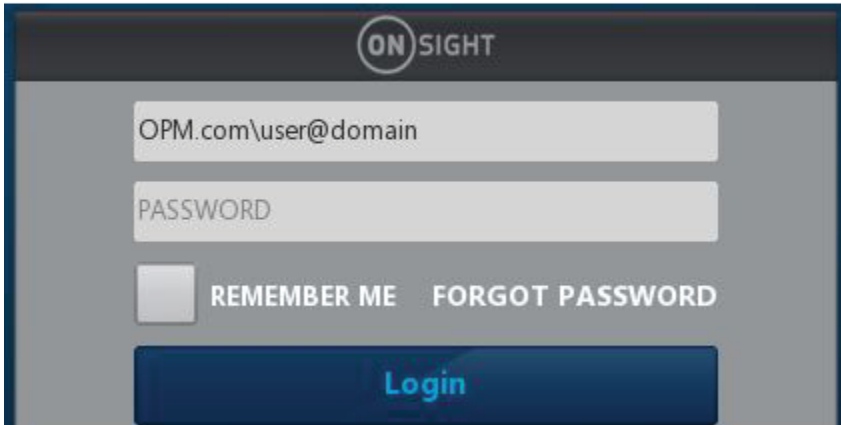


Figura 7-6 URL local

Los correos electrónicos de bienvenida **On-premises** tendrán un enlace para **Login to Onsight Connect** que iniciará Onsight Connect y lo dirigirá a la URL de su Onsight Platform Manager. La URL del enlace debe coincidir con la URL que se configuró durante la instalación de su servidor local.

El formato debe ser `OPM.com\user@domain`, en donde `OPM.com` es el nombre de dominio de su servidor.

Si está usando otro puerto distinto al 443 para instalar OPM-OP, el formato debe ser `OPM.com:port\user@domain`, en donde `OPM.com:port` es el nombre de dominio de su servidor y el número de puerto utilizado. Por ejemplo, `OPM.com:8083\user@domain`.

Una vez conectado, se les pedirá que confirmen que a partir de ahora quieren usar este servicio de cuenta de OnSight. El usuario debe hacer clic en **Yes** para aceptar los cambios. A partir de ahora, solo tendrán que introducir su **User Name** y **PASSWORD** para iniciar sesión o para habilitar la opción **REMEMBER ME** para automatizar el proceso de inicio de sesión.

7.2.2. Formatos URL locales

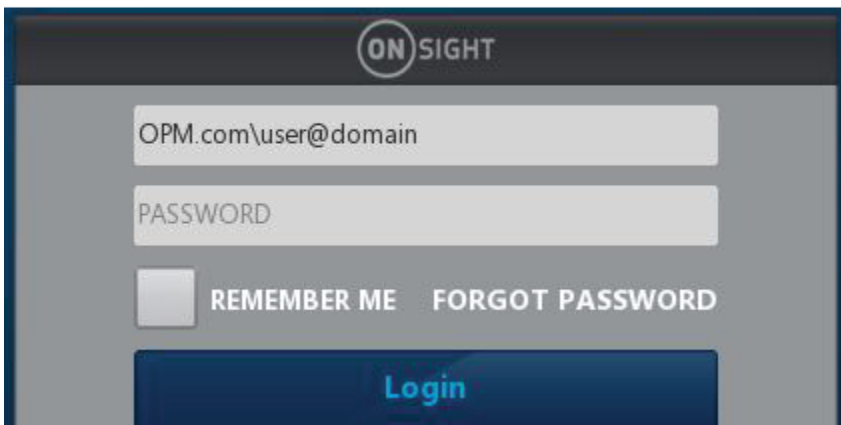


Figura 7-7 URL local

Cuando se especifica la ruta de OPM en el campo del nombre de usuario al iniciar sesión, se aceptan formatos abreviados. Use los típicos valores predeterminados codificados por hardware en caso de que falten elementos en la ruta.

Se asume que el campo de nombre de usuario contiene una ruta de OPM si el texto que se introduce tiene una diagonal invertida '\': `[OPM URI]\user@domain`

La parte "OPM URI" se analizará como un URI, por lo que solo se aceptarán los URI relativos o absolutos válidos (por ejemplo, sin espacios en el nombre del host). Los formatos que se aceptan son:

- Un URI absoluto `https://[autoridad]/[ruta]\user@domain`.
- Solo el host de OPM: `[host]\user@domain`. El esquema se establecerá como `https`, la ruta se establecerá como "OamClientWebService".

- Host y ruta de acceso de OPM: [host]/[ruta]\user@domain. El esquema se establecerá como https. El host y la ruta se usan tal cual.
- Esquema y host de OPM: https://[host]\user@domain. La ruta se establecerá como **OamClientWebService**. El esquema y el host se usan tal cual.
- Solo se aceptarán esquemas https.

Además, el mensaje de bienvenida contiene enlaces para descargar Onsight Connect desde su Onsight Platform Manager y enlaces de descarga tanto para **iOS App Store** como para **Android Google Play** store. El usuario puede hacer clic en **Download for Windows** o **Download for iOS** o **Android**.

Una vez que el usuario haya instalado Onsight Connect, DEBE hacer clic en el botón **Login to Onsight Connect** para configurar correctamente el software para iniciar sesión en su instalación de OPM.

Los usuarios de dispositivos móviles deben instalar Onsight Connect desde **Apple Store** o **Google Play Store**.

7.3. Requerimiento de correo electrónico de usuario

The screenshot shows the 'EDIT USER: DAVID B' page in the Onsight Platform Manager. The page has a navigation bar with 'LIBRESTREAM' and 'ON SIGHT PLATFORM MANAGER'. Below the navigation bar, there are tabs for 'IDENTIFICATION', 'SIP', 'GROUP MEMBERSHIP', 'PERSONAL CONTACTS', 'CLIENT POLICY', 'CLIENT PERMISSIONS', 'STATISTICS', and 'EVENTS'. The 'PROFILE' section is active, showing fields for User Name, First Name, Last Name, Country, Email, Federated SSO ID, Time Zone, Language, Department, Guest/In/Status, Licenses, and Member Of. The 'Common Actions' panel on the right includes options like Change Password, Change Account Type, Change Account Expiry, Resend Welcome Message, and Delete Account.

Figura 7-8 Requerimiento de correo electrónico de usuario

Las direcciones de correo electrónico son opcionales en OPM. **Sin embargo, si un usuario no configuró una dirección de correo electrónico, no recibirá los correos electrónicos de notificación (correos electrónicos de bienvenida, de restablecimiento de contraseña, etc.).** Si solicitan que se restablezca la contraseña, la página mostrará "Si se configura un correo electrónico válido...", pero no confirmará si se configuró un correo electrónico para su cuenta. En la página **PROFILE** del usuario, dentro de la sección **Common Actions**, la opción **Resend Welcome Email** estará oculta si el usuario no tiene una dirección de correo electrónico. Los correos electrónicos de bienvenida les notifican a los usuarios cómo **download, install** y **login** en Onsight Connect.

Los correos electrónicos son obligatorios en las siguientes situaciones:

- Los usuarios invitados necesitan una dirección de correo electrónico o un número de teléfono válido para recibir una invitación.
- El usuario **Account Owner** debe tener una dirección de correo electrónico válida.

Requerimientos de correo electrónico para la configuración de seguridad y SSO

Figura 7-9 Configuración de seguridad y SSO

El requerimiento de correo electrónico para los usuarios autorregistrados (ya sea a través de la página de autorregistro o provisto por SSO), se configura en las páginas **SETTINGS > SECURITY** y **SETTINGS > SSO**.

Si se establece como **Required**: los usuarios que se registren a través de la página de autorregistro deben introducir un correo electrónico.

SSO Users: si el correo electrónico que se proporciona como Atributo está en blanco, el aprovisionamiento fallará. Si el correo electrónico está configurado para **Prompt on First Login**, el usuario debe introducir un correo electrónico.


 **Nota:** No se puede desmarcar la opción **Require Email Address for Self-Registered Accounts**.

Si se establece como **Optional**: los usuarios que se registren a través de la página de autorregistro, opcionalmente, pueden introducir un correo electrónico. Si no proporcionan ninguno, el correo electrónico estará en blanco y no recibirán el correo electrónico de bienvenida.

SSO Users: si el correo electrónico que se proporciona como Atributo está en blanco, el aprovisionamiento procederá con un correo electrónico en blanco. Si el correo electrónico está configurado como **Prompt**, el usuario, opcionalmente, puede introducir un correo electrónico.

 **Nota:** Se puede desmarcar la opción **Require Email Address for Self-registered Accounts**.

Cualquier correo electrónico proporcionado por un atributo de SSO no requiere verificación.

 **Nota:** Cualquier correo electrónico proporcionado por un usuario durante el autorregistro requiere verificación antes de que se pueda utilizar la cuenta. Cualquier correo electrónico proporcionado por un atributo de SSO no requiere verificación.

7.4. Tipos de cuenta y permisos de usuario

The screenshot shows a user account creation form with the following sections:


- Initial Password:** A field with a masked password (dots).
- Confirm Password:** An empty text field.
- CLIENT SETTINGS**
 - Account Type:** A dropdown menu currently set to "Standard User".
 - SIP Settings:** A checkbox labeled "Automatically assign a SIP account to this user" which is checked.
- LICENSE GROUP MEMBERSHIP**
 - License Group:** A dropdown menu currently set to "Domain".
 - Licenses:** Three checkboxes: "Connect Enterprise" (checked), "Workspace Enterprise" (unchecked), and "Workspace Contributor" (unchecked).
- POLICY GROUP MEMBERSHIP**
 - Member Of:** A list of policy groups with checkboxes: "Name" (unchecked), "China" (unchecked), "EU Europe" (unchecked), and "NA North America" (unchecked).
- ACCOUNT EXPIRY**
 - Account Expiry:** A checkbox labeled "User Account Expires" which is unchecked.
 - Expiry Date:** A field with the number "7" and a "days" label.

At the bottom, there are two buttons: "Create New User" and "Cancel".

Figura 7-10 Tipo de cuenta de usuario

Dentro de **CLIENT SETTINGS**, el menú desplegable **Account Type** indica el nivel de acceso que tiene el usuario de Onsite Platform Manager. Las licencias asignadas al usuario determinan las características a las que el usuario tiene acceso en Onsite Connect y Workspace. La política y los permisos del cliente dictan el acceso de los usuarios a la configuración en las aplicaciones del cliente. Las opciones **Account Type** incluyen **Administrator**, **Group Administrator** y **Standard User**.

Administrator: Acceso total al OPM y a la configuración del dominio, incluyendo la administración de usuario.

 **Nota:** Solo un administrador puede asignar las licencias a grupos de licencia. Cuando por primera vez se crea un dominio para un cliente, el propietario de la cuenta es el único administrador. El propietario de la cuenta debe crear administradores adicionales.

Standard User Permissions: Un **Standard User** no tiene privilegios de administración. Están sujetos al grupo de política y a los permisos asignados a través de la membresía de grupo por el administrador de OPM. Ellos pueden invitar a participantes externos si la opción **Allow users to invite guests** está habilitada en el dominio (requiere la licencia maestra de invitados externos para el dominio).

Group Administrator Permissions: Un administrador de grupo tiene acceso a la configuración a nivel de grupo al que ha sido asignado, incluyendo:

- Modificar usuarios que están en su grupo (cambiar la configuración, contraseñas, etc.).
- Crear y borrar usuarios dentro de su grupo.
- Definir **Client Policy** para el grupo.

Para los **License Groups**, los administradores de grupo podrán agregar usuarios al grupo de acuerdo al número de licencias asignadas al grupo por el administrador de OPM.

7.5. Promoción de usuarios y asignación de un administrador de grupo

Iniciar sesión en OPM.

La administración de los administradores de grupo es un proceso de dos pasos. Debe cambiar un usuario estándar a un administrador de grupo y luego, asignarlos a un grupo.

Promoción de un usuario estándar a un administrador

1. Para promover a un usuario a **Group Administrator**, tendrá que iniciar sesión en OPM y seleccionar **USERS** en el menú principal. Se muestra la página USERS.

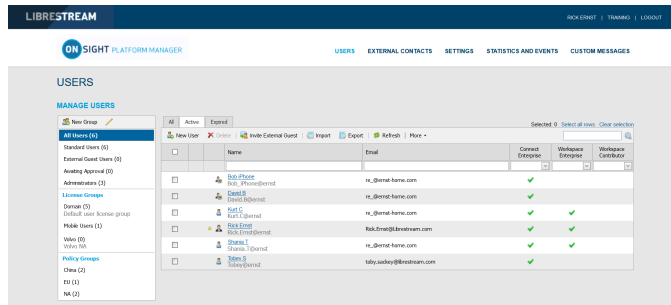


Figura 7-11 Página de usuarios

2. Haga clic para seleccionar un Nombre de usuario en la tabla de usuarios.

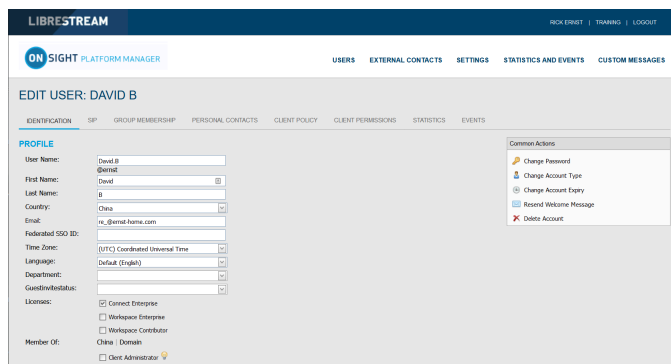


Figura 7-12 Editar página de usuario

- a. Busque el área **Common Actions** y seleccione **Change Account Type**.
- b. Seleccione **Administrador de grupo** desde **Account Type** y seleccione **Change Account Type** para implementar el cambio. Se muestra un mensaje que indica **El tipo de cuenta se cambió correctamente**.

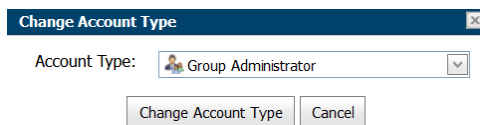


Figura 7-13 Cambiar tipo de cuenta

- c. Haga clic en **OK**.

Asignación de un administrador a un grupo

3. Para asignar un administrador de grupo a un grupo, tendrá que:

a. Seleccionar **Users** en el menú principal y seleccione el grupo para asignar un administrador de grupo.

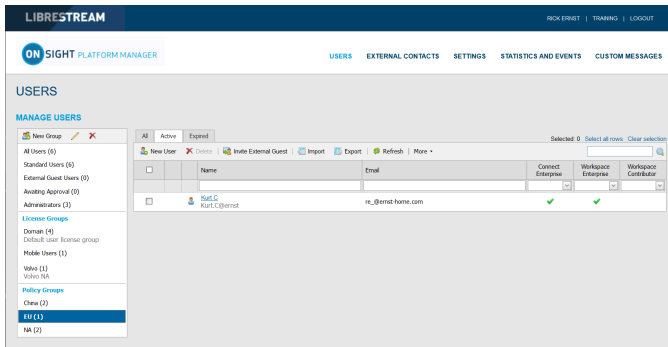



Figura 7-14 Seleccionar un grupo

b. Haga clic en el icono  **Modify Group** para editar. Se muestra la página EDITAR GRUPO.

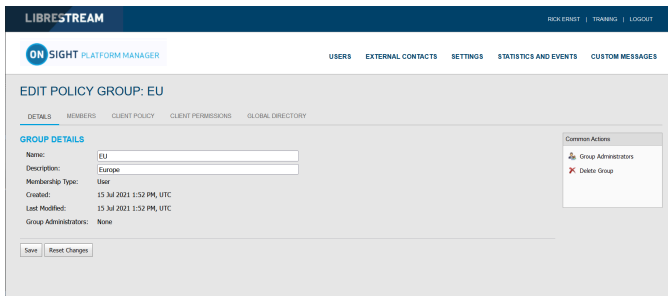


Figura 7-15 Editar grupo de políticas

c. En la sección **Common Actions**, haga clic en  **New Group**.

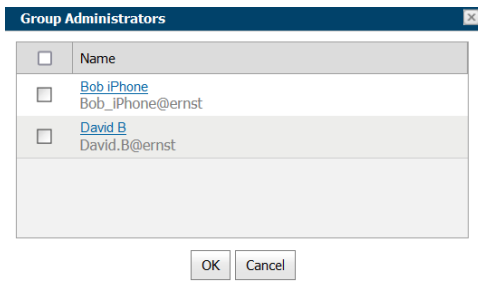


Figura 7-16 Administradores de grupo

d. Habilite la casilla de verificación junto a uno o más **Administradores de grupo** en la lista y haga clic en **OK**. La sección **Administradores de grupo** se actualiza en consecuencia.

e. Haga clic en **Save**.

7.6. Editar grupos

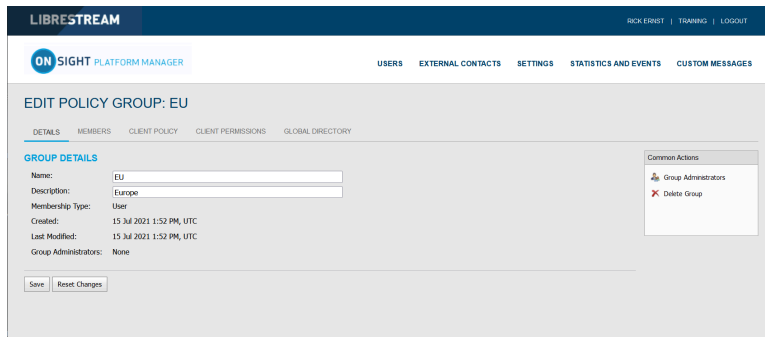





Figura 7-17 Editar un grupo

Para editar un grupo, seleccione **USERS** en el menú principal y seleccione un grupo en el panel **MANAGE USERS**. Haga clic en el icono  **Modify Group** (lápiz) para abrir la página **GROUP DETAILS**. La página **GROUP DETAILS** incluye:

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

Hay pestañas adicionales disponibles para editar el grupo, que incluyen **MEMBERS**, **CLIENT POLICY**, **CLIENT PERMISSIONS** y **GLOBAL DIRECTORY**.


La sección **Common Actions** lo habilita para modificar  **Group Administrator** y  **Delete Groups**.

Referencia relacionada

[Política del cliente, mejores prácticas \(en la página 124\)](#)

[Permisos de cliente, mejores prácticas \(en la página 136\)](#)

7.6.1. Agregar/eliminar miembros del grupo

Inicie sesión en OPM y seleccione **USERS** en el menú principal y seleccione un grupo en el panel **MANAGE USERS** y haga clic en el icono  **Modify Group** (lápiz) para abrir la página **EDIT GROUP**.

Para asignar miembros a un grupo puede:

1. Seleccione la pestaña **Members** y haga clic en el icono  **Add Members** para agregar usuarios al grupo.

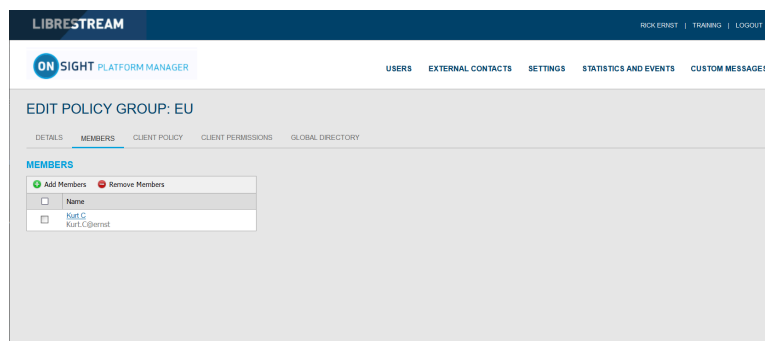


Figura 7-18 Editar grupo de políticas

2. Habilite las casillas de verificación de los usuarios que desea agregar y presione el botón **Add Selected Members**.

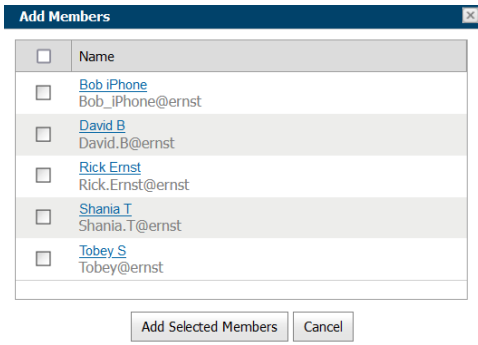





Figura 7-19 Agregar miembros

3. Para eliminar miembros, habilite la casilla de verificación junto a la lista de nombres de usuario y presione el icono  **Remove Members**. Esto completa el procedimiento.

7.6.2. Asignación de administradores de grupo

Seleccione **USERS** en el menú principal y seleccione un grupo en el panel **MANAGE USERS** y haga clic en el icono  **Modify Group** (lápiz) para abrir la página **EDIT GROUP**.

Para asignar un administrador de grupo, deberá:

1. Seleccionar **USERS** en el menú principal y seleccionar un grupo.
2. Haga clic en el icono  **Modify Group** (lápiz) para editar el grupo en la página DETAILS.

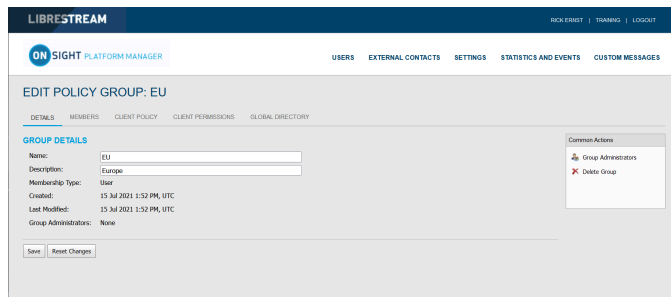


Figura 7-20 Detalles del grupo

3. Busque la sección **Common Actions** y haga clic en  **New Group**. Se muestra una lista de usuarios con privilegios de administrador de grupo.

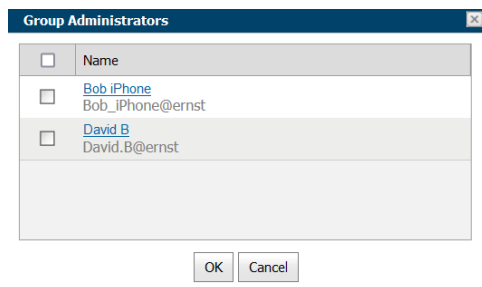



Figura 7-21 Administradores de grupo

4. Habilite la casilla de verificación junto a uno o más `Administradores de grupo` en la lista y haga clic en **OK**.
5. Haga clic en **Save** para finalizar sus cambios. Esto completa el procedimiento.

7.6.3. Editar política y permisos del cliente

Inicie sesión en OPM y seleccione **USERS** en el menú principal y seleccione un grupo en el panel **MANAGE USERS** y haga clic en el icono  **Modify Group** (lápiz) para abrir la página **EDIT GROUP**.

Para modificar la política del cliente y los permisos para un grupo, deberá:

1. Seleccionar la pestaña **CLIENT POLICY** para configurar los ajustes del endpoint.

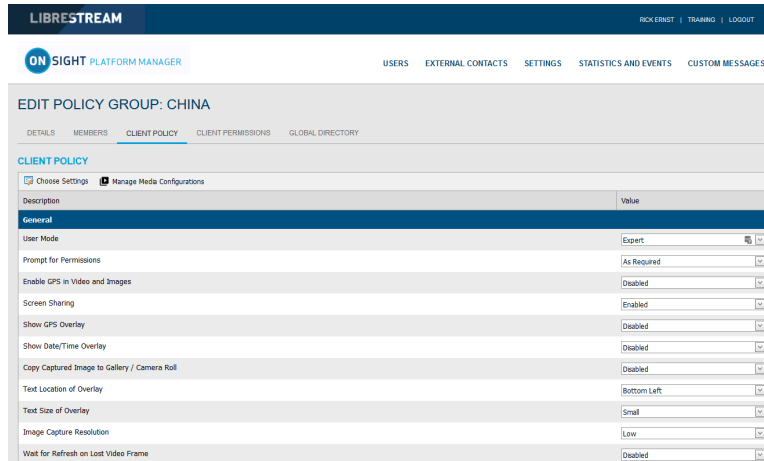



Figura 7-22 Editar grupo de políticas

2. Haga clic en  **Choose Settings** para agregar la configuración que desea controlar. Habilite las categorías y haga clic en **OK**.

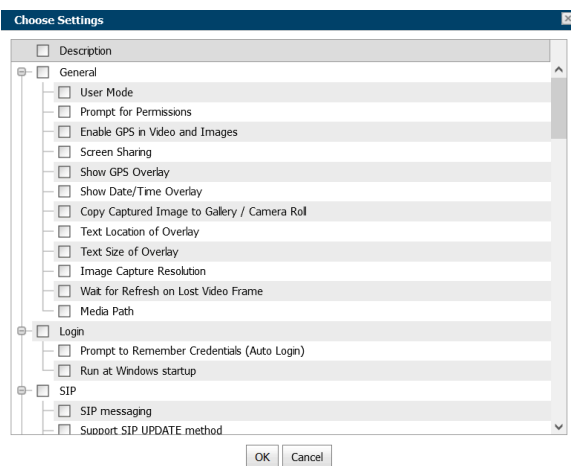


Figura 7-23 Elegir configuración

3. Establezca **Value** para cada categoría y presione **Save**.

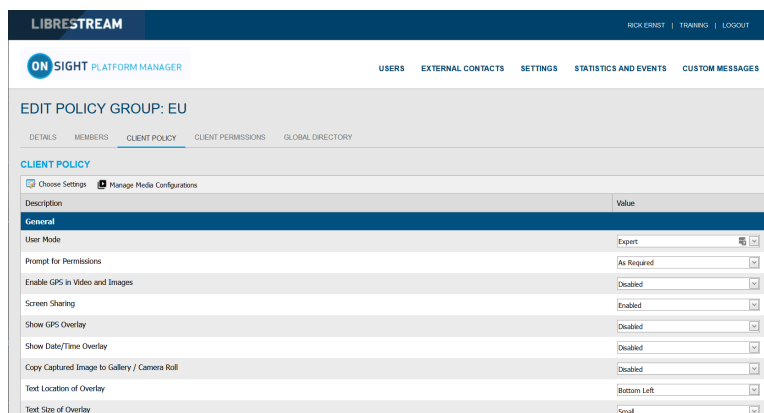
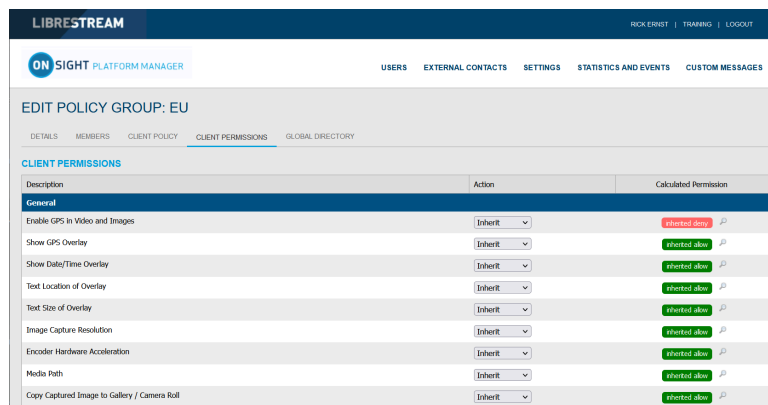


Figura 7-24 Política del cliente

4. Seleccione la pestaña **CLIENT PERMISSIONS**.



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

Figura 7-25 Permisos del cliente

5. Establezca la acción como **Inherit**, **Allow**, o **Deny** para cada configuración.



Nota: Inherit es el permiso predeterminado, el cliente heredará la configuración de cualquier grupo del que el usuario sea miembro si la configuración no se incluye en la política actual. Deny no permitirá que el usuario edite la configuración en la aplicación OnSight Connect. Allow permitirá que el usuario edite la configuración en la aplicación OnSight Connect.

Esto completa el procedimiento.

Consulte [Política y permisos del cliente \(en la página 78\)](#) para obtener una descripción más detallada de las acciones.

La **Onsight Platform Management Settings Template** describe y proporciona las mejores prácticas para cada configuración de política y permiso disponibles.

Referencia relacionada

[Política del cliente, mejores prácticas \(en la página 124\)](#)

[Permisos de cliente, mejores prácticas \(en la página 136\)](#)

Información relacionada

[Política y permisos del cliente \(en la página 78\)](#)

7.6.4. Directorio global

7.6.4.1. Disponibilidad de directorio global

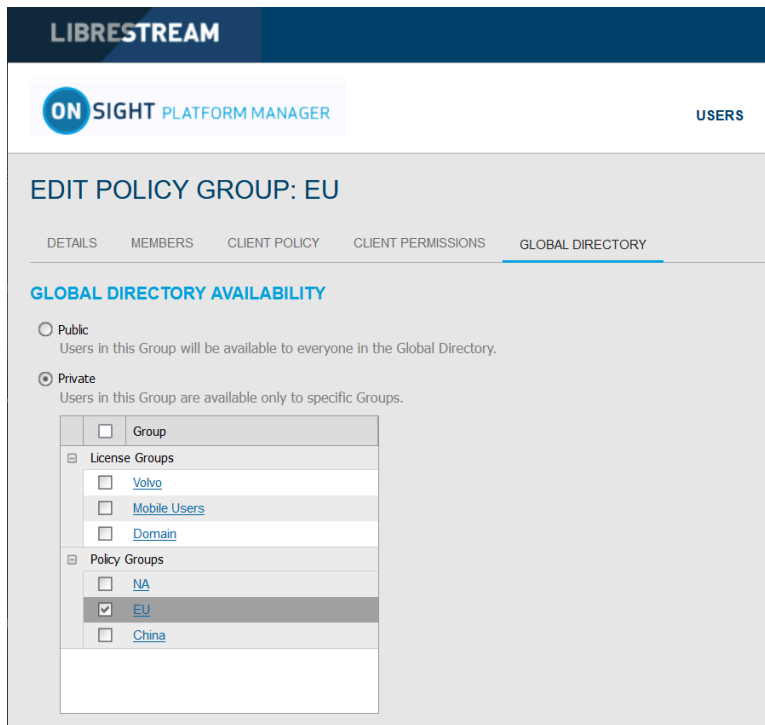




Figura 7-26 Editar grupo de políticas

Para editar el Directorio global, seleccione **USERS** en el menú principal y seleccione un grupo en el panel **MANAGE USERS**. Haga clic en el icono  **Modify Group** (lápiz) y seleccione la pestaña **GLOBAL DIRECTORY**. Los filtros de **GLOBAL DIRECTORY AVAILABILITY** controlan si el grupo actual es visible en el Directorio global.

- Seleccione **Public** para que los miembros del grupo sean visibles para todos los grupos en el Directorio global.
- Seleccione **Private** para que los miembros del grupo sean visibles para grupos selectos en el Directorio global. Seleccione los grupos para los cuales desea ser visible. Por ejemplo, es posible que desee que solo el grupo Servicio de campo sea visible para los miembros del grupo Taller de reparaciones.

 **Consejo:** Piense en esto como ¿quién puede buscarme?

7.6.4.2. Filtro de directorio global

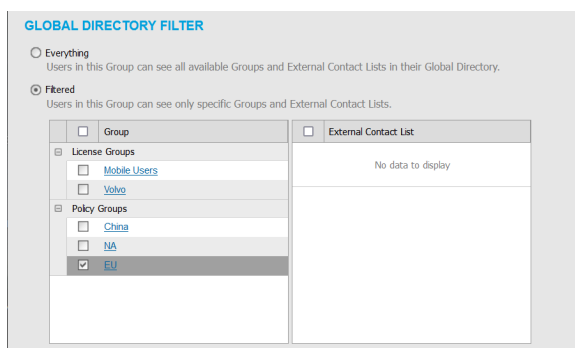


Figura 7-27 FILTRO DE DIRECTORIO GLOBAL

El Filtro de directorio global controla **quién es visible para el grupo actual** en el **Global Directory**.

1. Habilite la casilla de verificación **Everything** si desea que el grupo pueda visualizar a todos los grupos y contactos en el Directorio global.
2. Habilite la opción **Filtered** para limitar la visibilidad de búsqueda para el grupo actual. Habilite las casillas de verificación para los grupos y listas de contactos que desee que estén disponibles para el grupo actual. Por ejemplo, es posible que desee que el grupo **Servicio de campo** pueda buscar a los miembros del grupo **Taller de reparaciones**.

7.6.4.3. Contactos predeterminados

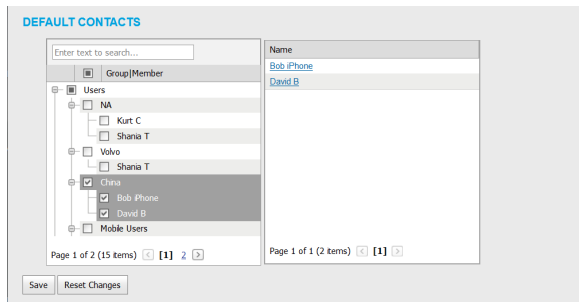



Figura 7-28 Contactos predeterminados

DEFAULT CONTACTS controla qué contactos se incluyen automáticamente en una lista de contactos de un miembro del grupo cuando inicia sesión en la aplicación OnSight Connect.

1. Habilite la casilla de verificación para los miembros de grupo o individuales del grupo que desea agregar a la lista de contactos predeterminados para el grupo actual. Cancele la selección y guarde para eliminar contactos.
2. Presione **Save** para conservar sus cambios.

 **Nota:** Las listas de contactos externos deben crearse en la pestaña **EXTERNAL CONTACTS** y asignarse a grupos antes de que estén disponibles en **Global Directory Filter** para su selección.

7.7. Importar/exportar usuarios

Un administrador de OPM puede importar usuarios mediante un Archivo de valores separados por comas (CSV) creado a partir de la plantilla de importación. Este es el método recomendado para crear usuarios nuevos y asignar licencias.

Mejores prácticas para importar contactos

En la mayoría de los casos, incluso la primera vez que importe usuarios, tendrá que incluir los siguientes encabezados de columnas en su archivo de importación:

- **UserName**
- **FirstName**
- **LastName**
- **EmailAddress** (opcional, pero es obligatorio cuando desee utilizar notificaciones del sistema y características como cambio de contraseña).
- **GroupMembership** (opcional)

Importar usuarios con esta información mínima es suficiente para tener todos los usuarios configurados correctamente con la configuración predeterminada en su dominio.

La configuración SIP se pueden configurar automáticamente al seleccionar **Automatically assign SIP accounts to new users** durante el paso de importación. Esta es la mejor manera de garantizar que sus cuentas SIP están configuradas correctamente para cada usuario.

Los casos especiales en los que necesita incluir más que la información básica del usuario incluyen:

- **Single Sign On (SSO)**
- **Private SIP Server settings**
- **Passwords** (se usa cuando no dependa del sistema para generar contraseñas temporales para los usuarios).

7.7.1. Crear una plantilla de importación de usuarios

Inicie sesión en OPM y seleccione **USERS** en el menú principal.

Para crear de forma manual una plantilla de importación de usuarios, tendrá que:

1. Hacer clic en el icono  **Import**.

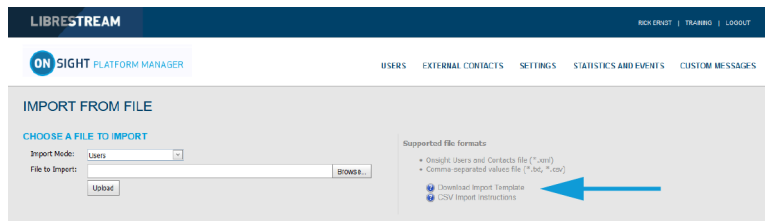


Figura 7-29 Importar desde archivo

2. Haga clic en el enlace **Download Import Template**.
3. Una vez descargado, abra el archivo `SampleUserImport.csv` en su aplicación de hoja de cálculo. Por ejemplo, Microsoft Excel, OpenOffice Calc, etc.
4. Siga las convenciones de formato descritas en **CSV Import Instructions** e introduzca la información según se requiera.

Importar una plantilla de importación de usuarios

5. Busque el campo **File to Import** y haga clic en el botón **Browse...** Se muestra la ventana **File Upload**.

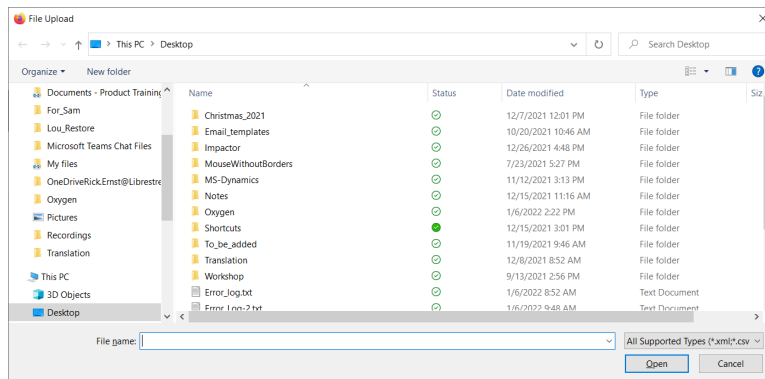



Figura 7-30 Carga de archivo

6. Navegue y seleccione **Plantilla de importación de usuarios** y haga clic en **Open**.
7. Haga clic en **Upload**.
Esto completa el procedimiento.

7.7.2. Importar usuarios

Inicie sesión en OPM y seleccione **USERS** en el menú principal. Debe haber descargado y modificado previamente una Plantilla de Importación como un archivo CSV. Consulte Creación de una plantilla de importación de usuarios.

Para importar usuarios utilizando una plantilla, deberá:

1. Hacer clic en el icono  **Import**.
2. Seleccionar **Users** en el menú desplegable **Import Mode**.

Consejo: Al configurar los contactos externos con el modo importar, se importarán los contactos externos que se enumeran en un archivo `contacts.csv` o `contacts.xml`. Consulte **CSV Import Instructions** para obtener detalles sobre el formato para CONTACTOS EXTERNOS. El archivo de contactos externos debe ser un archivo separado del archivo de importación de usuarios.

Nota: En la página **EXTERNAL CONTACTS**, puede seleccionar la opción **More > Export** para descargar una plantilla del archivo de contactos.

3. Busque el campo **File to Import** y haga clic en el botón **Browse...** Se muestra la ventana **File Upload**.

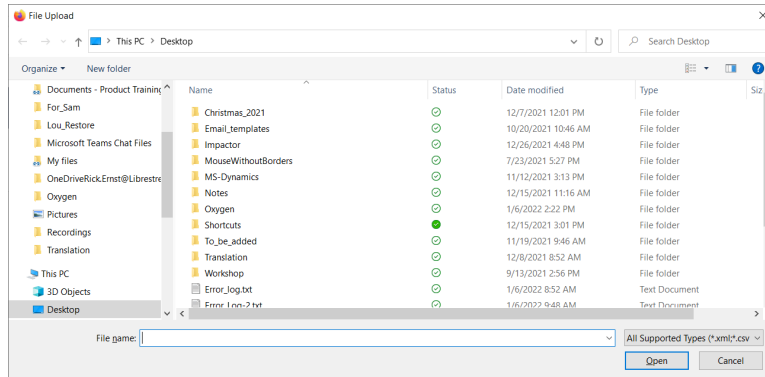


Figura 7-31 Carga de archivo

4. Navegue y seleccione Plantilla de importación de usuarios y haga clic en **Open**.

5. Haga clic en **Upload**. Aparece la ventana Importar usuarios.

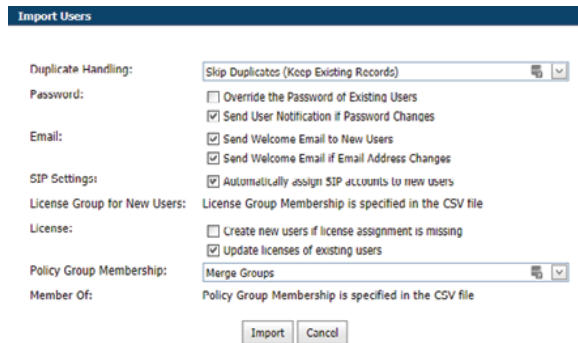


Figura 7-32 Importar usuarios

6. Determine cómo le gustaría manejar los duplicados:

- **Skip Duplicates**(Mantener registros existentes) o
- **Update existing records**.

7. En la sección **Password**, determine cómo le gustaría importar las contraseñas:

- **Override the Password of Existing Users**.
- **Send User Notification if Password Changes**.

8. En la sección **Email**, seleccione las opciones relevantes:

- **Send Welcome Email to New Users**.
- **Send Welcome Email if Email Address Changes**.

9. **SIP Settings:** activa la casilla de verificación **Automatically assign SIP accounts to new users**. Este es un paso importante en la configuración de las cuentas de los usuarios para garantizar que estén listos para hacer llamada de Onsite.

10. El grupo de licencias para nuevos usuarios se especifica en el archivo CSV.

11. Licenses: habilita las opciones apropiadas:

- a. **Create new users if license assignment is missing.**
- b. Actualice las licencias de los usuarios existentes como:
 - i. **Connect Enterprise**
 - ii. **Workspace Enterprise**
 - iii. **Workspace Contributor**



Nota: Los tipos de licencia que se asignan a cada usuario deben estar disponibles en el grupo de licencias elegido.

12. En la sección **Policy Group Membership**, determine cómo le gustaría asignar la membresía del grupo a los usuarios existentes. En este caso, está importando un archivo de usuario de Onsight para reconfigurar las cuentas de usuarios existentes. Seleccione entre:

- a. **Merge Groups:** permite a los usuarios ser miembros de varios grupos
- b. **Overwrite Groups:** modifica los grupos asignados.

13. En la sección **Member Of**, indica que la membresía del grupo de políticas se especifica en el archivo CSV.

14. Seleccione **Import** para continuar. Aparece la ventana **Import Results**.

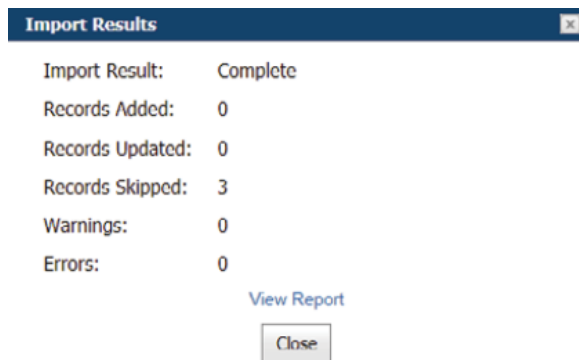


Figura 7-33 Importar resultados

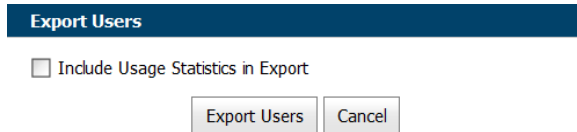
Esto completa el procedimiento.

Nota: Debe usar el campo **License Group for New Users** para asignar la membresía del grupo de licencias al importar usuarios y asignar licencias. Esto significa que el archivo de usuario especificado solo puede importar miembros del mismo grupo de licencias. El campo GroupMembership del archivo SampleUserImport.csv no se puede usar para especificar la membresía del grupo de licencias.

Al importar usuarios a un grupo de licencias, debe haber suficientes licencias disponibles para cada tipo que se asigna a cada usuario.

SSO: si usa la SSO y la **Federated SSO ID** para proporcionar un asignación de identidad entre los usuarios de Enterprise y las cuentas de usuario de Onsight, debe completar el campo Federated SSO ID para cada usuario que se enumera en el archivo UserImport.csv. El ID de SSO federado debe coincidir con el atributo de IdP asignado que configuró en la página SSO Settings.

7.8. Exportar usuarios



Export Users

Include Usage Statistics in Export

Export Users Cancel

Figura 7-34 Exportar usuarios

Haga clic en **USERS** en el menú principal y haga clic en **Export** para descargar un archivo CSV que contiene una lista de todos los usuarios en el dominio. Puede elegir la inclusión de **Usage Statistics** en el informe según sea necesario.

7.9. Autorregistro de usuarios

El administrador de Onsight puede habilitar el autorregistro de las cuentas de Onsight. El administrador distribuye el enlace a la página de autorregistro con instrucciones para los candidatos a la cuenta de Onsight.

A los usuarios que se les indique que se autorregistren se les pedirá que proporcionen la siguiente información en la página **REGISTER FOR AN ACCOUNT**.

- **User Name**
- **Initial Password**
- **First Name**
- **Last Name**
- **Email**
- **Self-Registration Key** (Si es obligatorio)
- **Challenge code** (CAPTCHA)

Dependiendo de cómo el administrador haya configurado el autorregistro, el usuario recibirá un correo electrónico para que **verifique su dirección de correo electrónico**. Lo dirigirá a la página de confirmación de la verificación del correo electrónico. Una vez que se verifique el correo electrónico y se apruebe la cuenta, el usuario recibirá un correo electrónico de confirmación de la aprobación y podrá empezar a usar Onsight Connect.

Si las cuentas no necesitan la aprobación del administrador, el usuario nuevo recibirá un **Correo electrónico de bienvenida a Onsight** inmediatamente después de registrarse.

Referencia relacionada

[Seguridad, mejores prácticas \(en la página 121\)](#)

8. CONTACTOS EXTERNOS

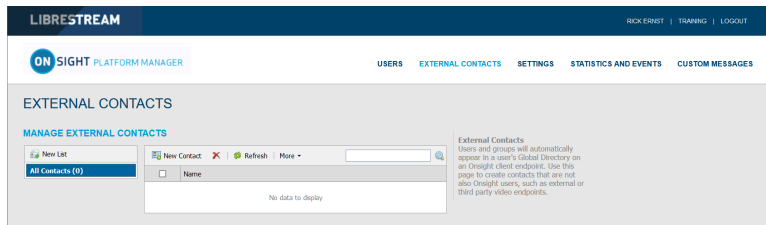



Figura 8-1 Contactos externos

Haga clic en **EXTERNAL CONTACTS** en el menú principal para visualizar todos los contactos externos. Los contactos externos son endpoints de SIP de video de terceros, como las salas de videoconferencias o cualquier otro dispositivo habilitado con SIP que no es un usuario de OnSight Connect en su dominio OnSight.

Cualquier usuario que se agregue a OPM se agrega automáticamente de forma predeterminada a **Global Directory**.

Lista de contactos externos

También puede utilizar el icono  **New List** para crear una lista nueva de contactos externos que se puede compartir a través de su dominio, licencia y grupos de política.

Exportar contactos externos

Puede exportar sus contactos externos como un archivo de plantilla CSV que se puede modificar para incluir los contactos de su organización y luego puede volver a importarlos a OnSight Platform Manager. Para exportar una lista de contactos externos, haga clic en **More > Export** para descargar una plantilla `ExportContacts.csv`.



Nota: Las direcciones que introduzca deben estar en formato SIP URI, por ejemplo, `videoroom@sipdomain.com`.

El archivo CSV puede entonces modificarse siempre que siga las convenciones para los nombres de las columnas y complete todos los campos obligatorios.



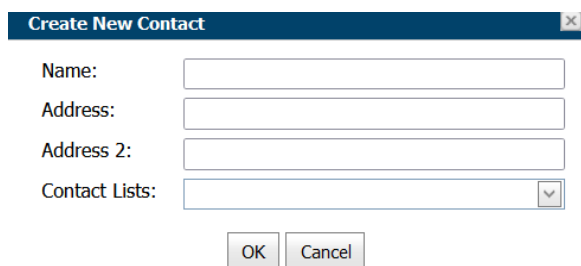
Consejo: Haga clic en **More > Import** para acceder al enlace **CSV Import instructions** en la sección **Supported file formats**, según sea necesario.

8.1. Agregar manualmente un contacto externo al directorio global

Inicie sesión en OPM y seleccione **EXTERNAL CONTACTS** en el menú principal.

Para agregar manualmente un contacto externo al directorio global, deberá:

1. Hacer clic en el icono  **New Contact**.



The dialog box titled "Create New Contact" contains the following fields and controls:

- Name:
- Address:
- Address 2:
- Contact Lists:
- Buttons: OK, Cancel

Figura 8-3 Crear contacto nuevo

2. Introduzca **Name** y **Direction** (Address 2, si es necesario).



Nota: Las direcciones que introduzca deben estar en formato SIP URI, por ejemplo, videoroom@sipdomain.com.

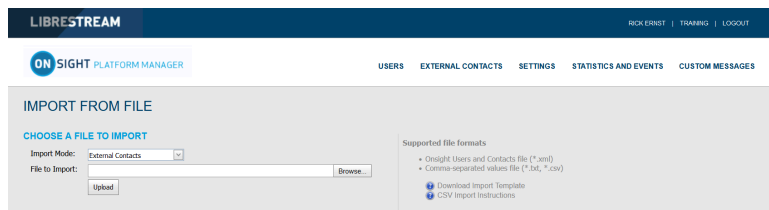
3. Seleccione el menú desplegable **Contacts Lists** para agregar el contacto externo.
4. Haga clic en **OK**. Entonces, podrá ver el contacto externo cuando busque en el directorio global desde un endpoint de Onsite. Esto completa el procedimiento.

8.2. Importar una lista de contactos externos

Inicie sesión en OPM y seleccione **EXTERNAL CONTACTS** en el menú principal. Debe haber creado y modificado previamente un archivo `ExternalContacts.csv` utilizando la operación **More > Import > Download Import Template**.

Para importar una lista de contactos externos revisada como un archivo, debe:

1. Hacer clic en **More > Import**. Aparece la ventana **IMPORT FROM FILE**.



The "IMPORT FROM FILE" dialog box includes the following elements:

- Import Mode: External Contacts (dropdown)
- File to Import: Browse...
- Upload button
- Supported file formats:
 - Onsight Users and Contacts file (*.xml)
 - Comma-separated values file (*.csv, *.csv)
- Links: Download Import Template, CSV Import instructions

Figura 8-4 Importar desde archivo

2. Navegue y seleccione el `ExternalContacts.csv` a importar al hacer clic en el botón **Browse**.

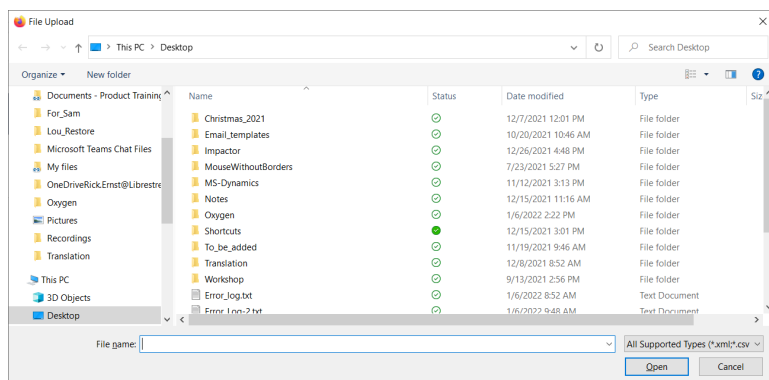


Figura 8-5 Carga de archivo

3. Haga clic en **Open**.
4. Presione **Upload**. Se presentará la ventana **Import Users**.

Figura 8-6 Ventana importar usuarios

5. Seleccione la opción **Duplicate Handling** que es ideal para su situación:
 - **Skip Duplicates** (mantener los registros existentes)
 - **Update Existing Records**
 - **Create a Duplicate**
6. Haga clic en **Import**.
Cuando se complete la importación, se presentará la ventana **Import Results**.
7. Haga clic en **View Report** para revisar los detalles.
8. Presione **Close**.
9. Vuelva a la página **EXTERNAL CONTACTS** para ver los contactos importados.
Esto completa el procedimiento.

8.3. Agregar una lista de contactos externos

Inicie sesión en OPM y seleccione **EXTERNAL CONTACTS** en el menú principal.

Para crear manualmente una lista de contactos externos, deberá:

1. Buscar y seleccionar el icono  **New List** bajo el título MANAGE EXTERNAL CONTACTS.

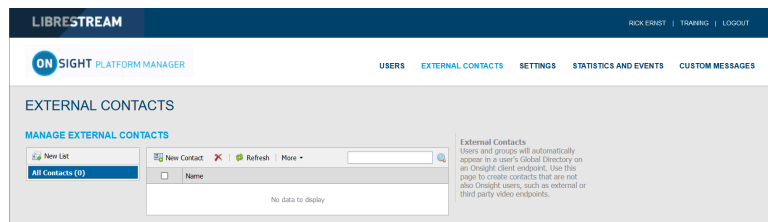


Figura 8-7 Administrar contactos externos

2. Aparece la ventana **Create New Contact List**.

Figura 8-8 Crear lista nueva de contactos

3. Introduzca **Name** para la lista y una descripción.
4. Seleccione **Public** o **Private** para establecer el nivel de accesibilidad de la lista.



Nota: Si selecciona Private, seleccione los grupos que tendrán acceso a la lista.

5. La lista nueva aparece en **All Contacts** bajo **MANAGE EXTERNAL CONTACTS**.

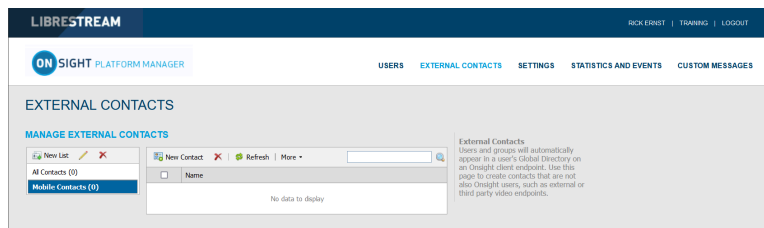


Figura 8-9 Aparece la lista nueva

Esto completa el procedimiento.

8.4. Agregar/eliminar contactos externos de las listas

Iniciar sesión en OPM.

Para modificar contactos dentro de su lista de contactos externos, deberá:

1. Seleccionar **EXTERNAL CONTACTS** en el menú principal.

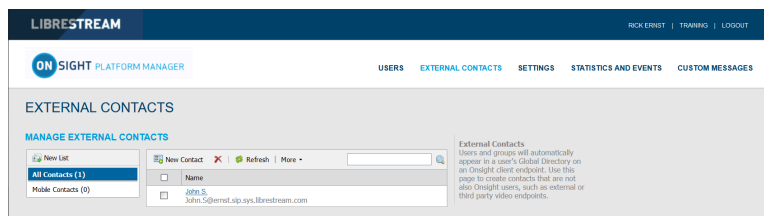


Figura 8-10 Administrar contactos externos

2. Seleccione la lista a la que desea agregar los contactos.
3. Habilite la casilla de verificación a lado de los **Contactos** externos que desea agregar a la lista.
4. Haga clic en **More > Add to List**.
5. Seleccione la lista a la que se agregarán los contactos.

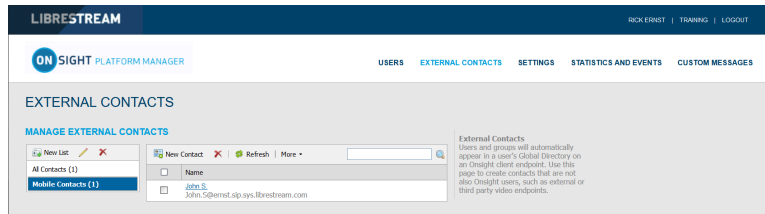


Figura 8-11 El nombre del contacto aparece en la lista

6. Verifique que el nombre del contacto aparezca en la lista.

i Consejo: Puede eliminar el nombre de un contacto de una lista al seleccionar la lista, activar la casilla de verificación junto a los nombres de los contactos y hacer clic en **More > Remove from List**.

Esto completa el procedimiento.

9. CONFIGURACIÓN

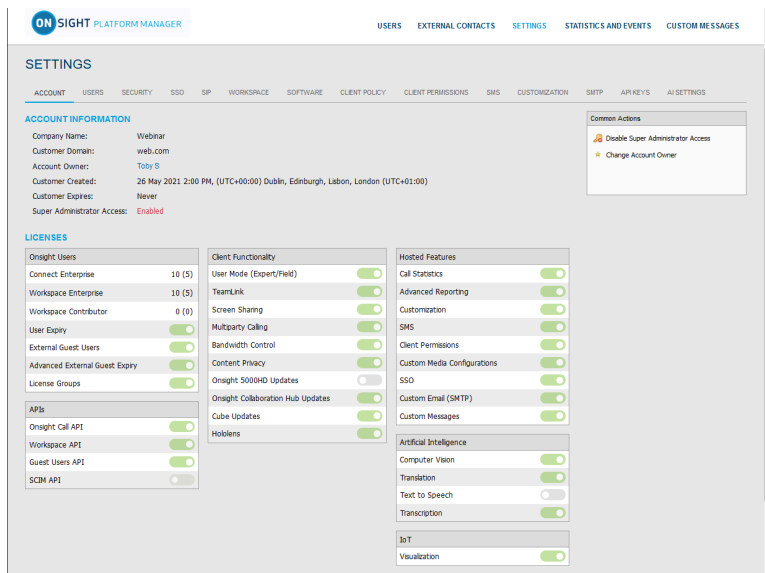


Figura 9-1 Configuración

Haga clic en **SETTINGS** en el menú principal para configurar los ajustes de cada endpoint de OnSight para cumplir con sus políticas. La configuración se aplica al endpoint cuando un usuario inicia sesión en OnSight Connect. Los **External Guest Users** se pueden habilitar dentro de **LICENSES** para que cualquier usuario activo de OnSight Connect pueda invitar a un participante externo durante un período determinado por el administrador. Los permisos de los usuarios invitados externos pueden restringirse, pero tienen acceso completo a la experiencia de colaboración de OnSight.

Dentro de **SETTINGS** se puede acceder a otras pestañas como:

- Configuración **SIP** que se asigna desde el grupo de asignación automática.
- Los ajustes del **Software** controlan los ajustes de la versión de OnSight Connect que se pueden seleccionar e instalar para los sistemas operativos de Windows.
- La configuración **Client Policy** se selecciona para cada endpoint, por ejemplo, en el modo Encryption.
- Se asigna la configuración **Security** que incluye la política de contraseña, la política de inicio de sesión y el método de creación de cuentas del usuario.

Todas las configuraciones se aplican a los endpoints de OnSight después de haber autenticado y autorizado a un usuario de OnSight durante el proceso de inicio de sesión.

Cuando se apliquen cambios a una página de configuración, debe hacer clic en **Save** para confirmar los cambios. Haga clic en **Reset Changes** para volver a la configuración anterior de la página.

9.1. Tiempo de espera de autenticación

Para permitir el acceso al contenido y a los servicios de llamada en caso de pérdida de conectividad a la red, los usuarios permanecen autenticados localmente durante 30 días en el cliente después de su autenticación inicial en línea. Los clientes deben volver a autenticarse por lo menos una vez cada 30 días para acceder al servicio en línea.

9.2. Cuenta

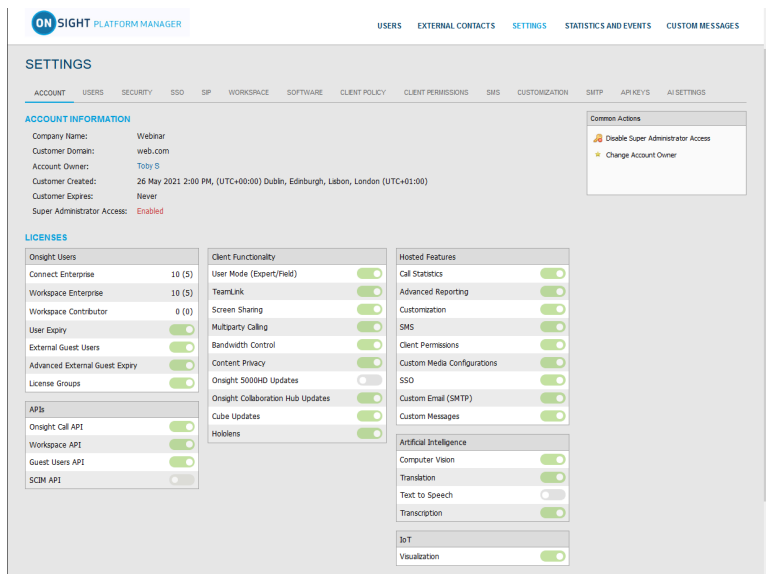




Figura 9-2 Configuración

Haga clic en **SETTINGS** en el menú principal para acceder a la información de la cuenta OPM de su empresa, dentro de la pestaña **ACCOUNT**. La pestaña ACCOUNT incluye las siguientes secciones: Account Information, Common Actions y Licenses.

Account Information

Incluye **Company Name**, **Customer Domain**, **Account Owner**, **Customer Created** date, **Customer Expiry** date y **Super Administrator Access** status.

Common Actions

Dentro del panel de la derecha **Common Actions**, puede acceder a las funciones adicionales que incluyen Enable/Disable  **Disable Super Administrator Access** y  **Change Account Owner**.

Licenses

Las licencias habilitadas en su dominio de OnSight aparecen en la sección **LICENSES**.

Referencia relacionada

[Cuenta, mejores prácticas \(en la página 118\)](#)

9.2.1. Acceso de superadministrador

En el panel **Common Actions** puede habilitar o deshabilitar **Super Administrator Access** al soporte de Librestream. Esto le permite indicar por cuántas horas desearía darle acceso a su dominio a **Soporte de Librestream**. Al darle acceso, el soporte de Librestream puede asistirlo con la configuración o resolución de problemas. El acceso de superadministrador se puede deshabilitar en cualquier momento al presionar **Deny Super Administrator Access**; de lo contrario, expirará al finalizar el plazo establecido.

LOCAL

El acceso de superadministrador no procede cuando se utiliza un servidor local. [CONTACTO DE SOPORTE \(en la página 111\)](#) en caso de necesitar asistencia.

Referencia relacionada

[Cuenta, mejores prácticas \(en la página 118\)](#)

Información relacionada

[CONTACTO DE SOPORTE \(en la página 111\)](#)

9.2.2. Cambiar propietario de cuenta

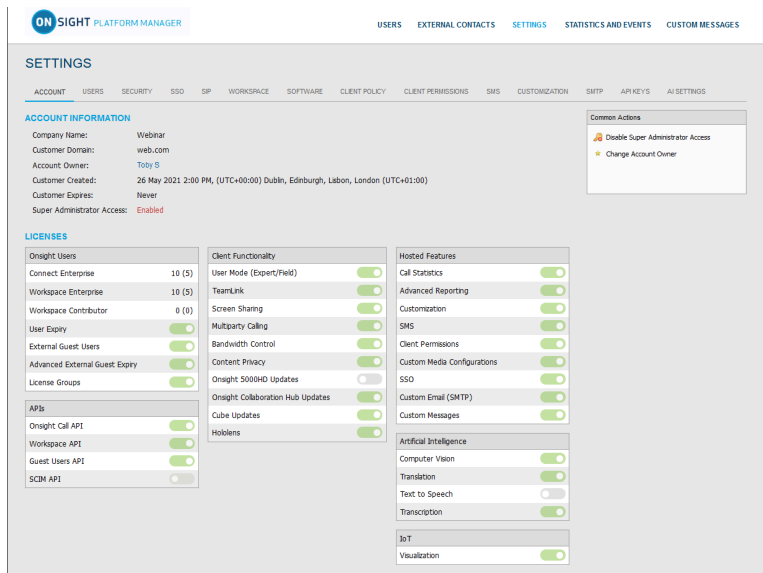
En la sección **Common Actions** puede utilizar **Change Account Owner** para indicar el **OPM Administrator** principal para su dominio de cuenta Onsignt. La opción **Change Account Owner** habilita a un administrador de Onsignt Platform Manager asignar a otro usuario como el **Account Owner**.

i Consejo: El usuario debe tener privilegios de administrador de Onsignt Platform Manager antes de ser asignado como Propietario de la cuenta.

Referencia relacionada

[Cuenta, mejores prácticas \(en la página 118\)](#)

9.2.3. Licencias



The screenshot displays the 'SETTINGS' page in the Onsignt Platform Manager interface. The 'ACCOUNT INFORMATION' section shows details for 'Webinar' (Company Name), 'web.com' (Customer Domain), and 'Toby S' (Account Owner). The 'LICENSES' section lists various license types and their counts: Onsignt Users (10), Connect Enterprise (10), Workspace Enterprise (10), Workspace Contributor (0), User Expiry (Enabled), External Guest Users (Enabled), Advanced External Guest Expiry (Enabled), License Groups (Enabled), Onsignt Call API (Enabled), Workspace API (Enabled), Guest Users API (Enabled), and SCIM API (Enabled). The 'LICENSSES' section is divided into several categories with feature toggles: Client Functionality (User Mode, TeamLink, Screen Sharing, Multiparty Calling, Bandwidth Control, Content Privacy, Onsignt 5000HD Updates, Onsignt Collaboration Hub Updates, Cube Updates, Holdlens), Hosted Features (Call Statistics, Advanced Reporting, Customization, SMS, Client Permissions, Custom Media Configurations, SSO, Custom Email (SMTP), Custom Messages), API (Onsignt Call API, Workspace API, Guest Users API, SCIM API), Artificial Intelligence (Computer Vision, Translation, Text to Speech, Transcription), and IoT (Visualization).

Figura 9-3 Configuración

Las licencias habilitadas para su dominio Onsignt se enumeran en la sección **LICENSSES**. Se dividen en cuatro categorías principales:

1. **Usuarios de Onsignt**
2. **Funcionalidad del cliente**
3. **API**
4. **Hosted Features**

Referencia relacionada

[Cuenta, mejores prácticas \(en la página 118\)](#)

9.2.3.1. Usuarios de Onsignt

La sección de usuarios de Onsignt registra el número de licencias por tipo y las características de la licencia. Cada tipo de licencia habilita la funcionalidad en las aplicaciones del cliente. Los tipos de licencia de usuario incluyen:

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

Cada característica de la licencia habilita la funcionalidad relacionada con el administrador de la licencia de usuario. Las características de la licencia incluyen:

- **User Expiry:** habilita la expiración de las cuentas de usuario
- **External Guest Users:** habilita invitaciones de participantes
- **Advanced External Guest Expiry:** habilita la expiración de invitaciones de participantes.
- **License Groups:** habilita la administración de grupo de licencia en un esquema por grupo

9.2.3.2. Interfaces de programación de aplicaciones

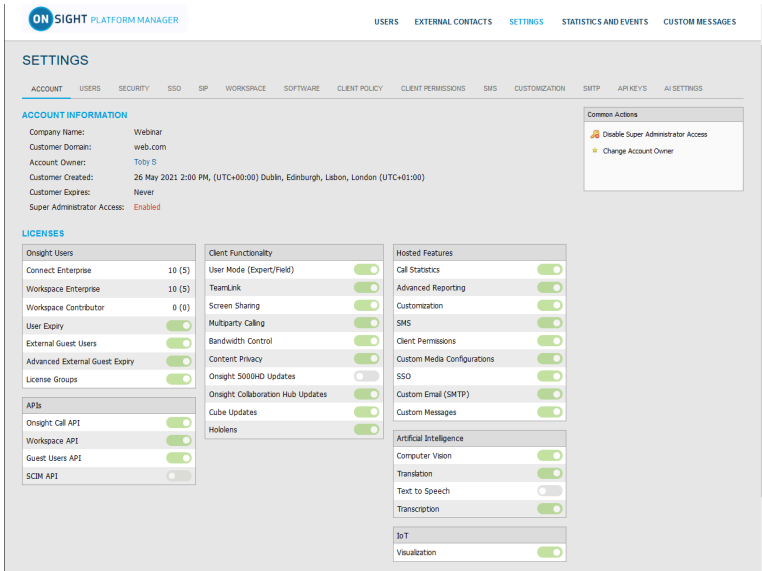


Figura 9-4 Configuración

Se puede habilitar Onsite Platform Manager para trabajar con varias Interfaces de programación de aplicaciones (API). Haga clic en **SETTINGS** en el menú principal y busque las API en la sección **LICENSES**. Las API incluyen:

- **Onsite Call API:** habilita el acceso a **Onsite Call REST API** y a **API Key Management**.
- **Workspace API:** habilita el acceso a **Workspace REST API** y a **API Key Management**.
- **Guest User API:** habilita la función de invitar a participantes externos.
- **SCIM API:** automatiza la administración de usuario y de grupo.

9.2.3.3. Funcionalidad del cliente

Puede acceder a **Client Functionality** al hacer clic en **SETTINGS** en el menú principal y ubicarlo en la sección **LICENSES**. La opción Funcionalidad del cliente se puede habilitar o deshabilitar para:

- **User Mode (Expert/Field):** habilita la función de definir las cuentas de usuario como modo **Expert** o **Field**. **Expert Mode** proporciona todas las características a los usuarios. **Field Mode** es una interfaz de usuario simplificada con un subconjunto de características disponibles para el usuario. Cuando se utiliza **Field Mode** es de esperar que llamen a expertos que controlarán la llamada de manera remota.
- **TeamLink:** habilita las funciones para atravesar el firewall de TeamLink para el dominio. TeamLink habilita la transmisión de datos HTTPS a través de un firewall que no permite tráfico SIP ni de medios.




Nota: Al habilitar **TeamLink Registration** enciende automáticamente **TeamLink** para cada endpoint. Al habilitar la opción **Always use TeamLink**, le está diciendo al endpoint que use TeamLink incluso si los puertos SIP en el firewall están abiertos; es decir, transmitir siempre SIP a través de HTTP/S.



Consejo: Librestream recomienda que **Always use TeamLink** esté **Disabled** y se use solo sobre una base de endpoint para fines de resolución de problemas.

- **Screen Sharing:** habilita la función de compartir cualquier ventana con los participantes de la llamada.
- **Multiparty Calling:** habilita la función de establecer las PC con Windows y los dispositivos Android como anfitriones de conferencias. Cuando se habilita, el dispositivo puede organizar una conferencia telefónica con varios participantes. El límite en la cantidad de participantes depende de los recursos de hardware y de red disponibles para el dispositivo.

 **Consejo:** La cantidad máxima de participantes de la llamada se puede controlar mediante **Client Policy**.

- **Bandwidth Control:** habilita la función de establecer **Maximum Video Bit Rate** que se permite para **Media configurations**.
- **Content Privacy:** habilita la función de grabación de control y captura de imágenes fijas en los endpoints al utilizar **Client Policy**.
- **Onsight 5000HD Updates:** habilita las actualizaciones para la cámara inteligente robusta 5000 HD.
- **Onsight Collaboration Hub Updates:** habilita la función de implementar actualizaciones de software en los Hub de Onsight Collaboration ya sea mediante clientes de iOS o de Android.
- **Cube Updates:** habilita las actualizaciones para el Onsight Cube.
- **Hololens:** habilita la accesibilidad a Hololens para la funcionalidad Onsight Connect.

Local: TeamLink

TeamLink no tiene soporte actualmente cuando se usan instalaciones locales, se requiere acceso público a Internet para comunicarse con los servidores de TeamLink.

9.2.3.4. Funciones alojadas

Las funciones alojadas se pueden habilitar o deshabilitar para:

- **Call Statistics:** permite capturar las estadísticas de llamadas de los endpoints de Onsight.
- **Advanced Reporting:** permite generar y exportar informes estadísticos avanzados de llamadas.
- **Customization:** permite personalizar los mensajes de Onsight Platform Manager enviados a los usuarios de Onsight. Los mensajes se basan en texto y HTML.
- **Permisos del cliente**
- **SMS:** permite enviar invitaciones para invitados externos a través de SMS. Permisos del cliente: permite controlar el acceso de los usuarios a la configuración del endpoint.
- **Custom Media Configurations:** permite desplegar configuraciones de medios personalizadas a través de la política del cliente.
- **SSO:** permite el soporte de inicio de sesión único para su dominio. Consulte la sección SSO para conocer los detalles de la configuración.
- **Custom Email** (SMTP)
- **Custom Messages**

9.2.3.5. Inteligencia artificial

Las funciones de Inteligencia artificial (IA) se pueden habilitar o deshabilitar para:

- **Computer Vision (CV):** permite acceder a las funciones de CV, como el OCR, la clasificación y la localización de objetos, y el etiquetado automático.
- **Natural Language Processing (NLP):** permite acceder a la función NLP para acceder al **Onsight Translator**.
- **Transcription:** permite acceder a las funciones de transcripción para todas las llamadas.


9.2.3.6. Internet de las cosas

Las funciones del Internet de las cosas (IoT) se pueden habilitar o deshabilitar para **Visualization**. Esto permite el acceso a los servicios de IoT, la visualización de los instrumentos y el autoetiquetado.

9.2.4. Anonimización de datos


Data Anonymization: puede habilitarse bajo petición, para que su dominio sea compatible con el Reglamento General de Protección de Datos (RGPD) para Europa y la legislación relacionada que incluye el cumplimiento de la privacidad de los datos y el derecho a ser olvidados (RTBF).

Cuando se habilita, los usuarios eliminados automáticamente tendrán su **Información Personal Identificable (PII)** anonimizada. El nombre de usuario, la dirección de correo electrónico y los eventos ya no se podrán mostrar en los informes de Onsight Platform Manager (OPM) y en las estadísticas de llamadas. En su lugar, se insertará un seudónimo anónimo para evitar que identifiquen al usuario.

 **Nota:** Las estadísticas de llamadas, los informes y los eventos seguirán teniendo la anonimización de datos para apoyar los análisis e informes.

La anonimización de datos PII ocurre cuando:

- se elimina la cuenta de un usuario
- se elimina a un usuario invitado o su cuenta expira


 **Nota:** El contenido de Onsight Workspace es propiedad del cliente. Como tal, la empresa es responsable de todo el contenido. Cuando se elimina un usuario, la cuenta de Workspace también se elimina automáticamente. El cliente debe optar por borrar el contenido del usuario según sea necesario.

Además, si se solicita, Librestream puede:

- **Anonymize previously deleted users from your domain:** los usuarios previamente eliminados no aparecerán dentro de su lista de usuarios, pero sus datos seguirán disponibles para la elaboración de informes si no se anonimizan.
- **Anonymize active user data:** si se habilita esta opción, los datos dejarán de estar asociados al usuario activo. Los datos seguirán mostrando el uso dentro del periodo de tiempo establecido.

9.2.5. Anonimización programada

La opción **Scheduled Anonymization** se puede habilitar a petición, para que su dominio convierta automáticamente los datos personales activos en datos anónimos según lo definido por un **Data Retention Period (DRP)**. En su siguiente ciclo, los datos serán anonimizados. Esto elimina la necesidad del procesamiento manual para los clientes.

 **Nota:** La anonimización programada está deshabilitada de forma predeterminada. **Una vez que los datos se anonimizan, no se pueden revertir.**

9.3. Usuarios

Figura 9-5 Página de usuarios

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **USERS**. La página **USERS** le permite establecer la configuración global de los invitados y usuarios externos para el dominio. La página **USERS** incluye las siguientes secciones: **USER ACCOUNTS**, **EXTERNAL GUEST USERS**, **GLOBAL DIRECTORY** y **CUSTOM FIELDS**.

Referencia relacionada


[Usuarios, mejores prácticas \(en la página 120\)](#)

9.3.1. Cuentas de usuario

Figura 9-6 Página de usuarios

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **USERS**. La página **USERS** le permite modificar la configuración **USER ACCOUNT** para:

- **Default Time Zone:** seleccione la zona horaria deseada para todas las cuentas de usuario en el menú desplegable. Todos los datos comunicados por los clientes de Onsight al OPM se basan en la hora universal coordinada (UTC); sin embargo, la configuración de la zona horaria predeterminada ajustará los datos de la marca temporal dentro del OPM solo para fines de visualización.
- **Default Language:** establezca el idioma predeterminado en el menú desplegable.

 **Nota:** Los dispositivos Onsight deben tener la fecha y hora exactas para utilizar el servicio de Onsight Connect. El HTTPS se basa en la precisión de la fecha y la hora para realizar la autenticación.

Referencia relacionada

[Usuarios, mejores prácticas \(en la página 120\)](#)

9.3.2. Usuarios invitados externos

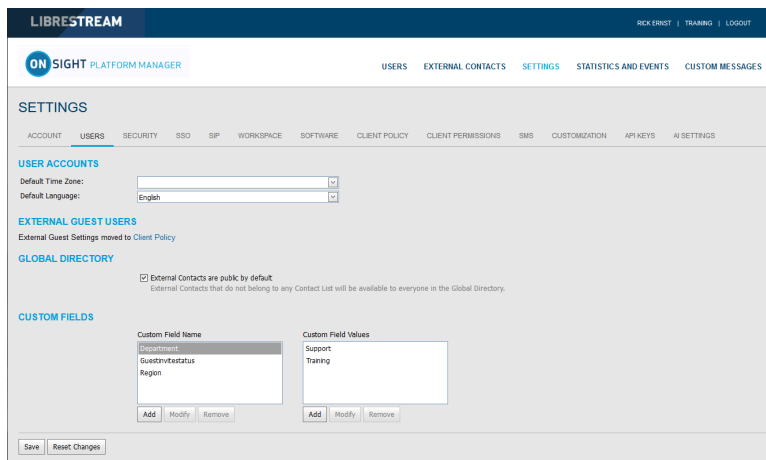


Figura 9-7 Página de usuarios

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **USERS**. La página **USERS** contiene una sección **EXTERNAL GUEST USERS** que le permite hacer clic en el acceso directo **Client Policy** para modificar esta configuración.



Nota: Todas las configuraciones de los usuarios invitados externos se trasladan a **Client Policy**.

Referencia relacionada

[Usuarios, mejores prácticas \(en la página 120\)](#)

[Política del cliente, mejores prácticas \(en la página 124\)](#)

[Permisos de cliente, mejores prácticas \(en la página 136\)](#)

9.3.3. Directorio global

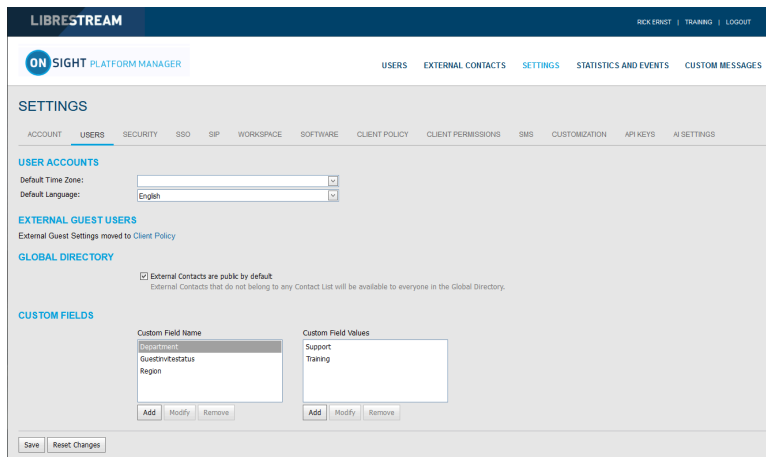


Figura 9-8 Página de usuarios

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **USERS**. La página **USERS** contiene una sección **GLOBAL DIRECTORY** que controla cómo se muestran los contactos externos dentro del Directorio global. Los usuarios y los grupos automáticamente aparecerán en el Directorio global en un Cliente de OnSight. Los contactos externos son contactos creados que no son usuarios de OnSight, incluyendo endpoints de video externos o de terceros.

Habilite la casilla de verificación **External Contacts are public by default** para controlar si los contactos externos que no pertenecen a ninguna lista de contactos estarán disponibles para todos en el Directorio global.

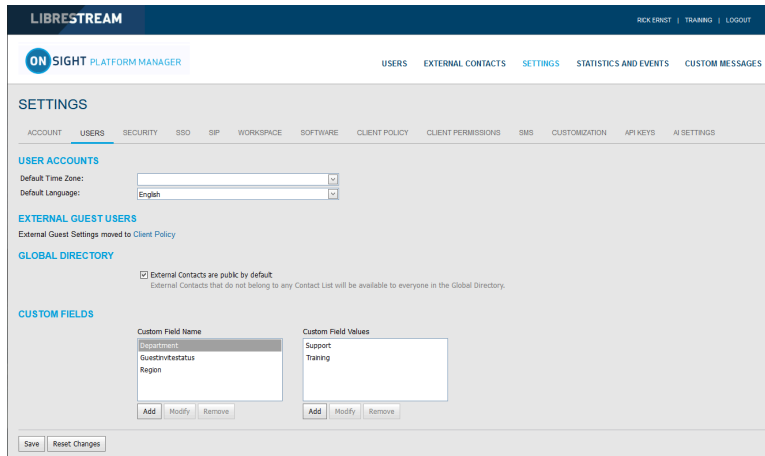


Nota: Este tiene un comportamiento independiente de la configuración de **External Guest Users** que puede deshabilitar el acceso al directorio global. Esta configuración controla el acceso del usuario estándar a **External Contacts** en el directorio global.

Referencia relacionada

Usuarios, mejores prácticas (en la página 120)

9.3.4. Campos personalizados



The screenshot shows the 'LIBRESTREAM' interface with the 'ON SIGHT PLATFORM MANAGER' header. The main navigation includes 'USERS', 'EXTERNAL CONTACTS', 'SETTINGS', 'STATISTICS AND EVENTS', and 'CUSTOM MESSAGES'. The 'SETTINGS' page has a sub-menu with 'ACCOUNT', 'USERS', 'SECURITY', 'SSO', 'SIP', 'WORKSPACE', 'SOFTWARE', 'CLIENT POLICY', 'CLIENT PERMISSIONS', 'SMS', 'CUSTOMIZATION', 'API KEYS', and 'AI SETTINGS'. The 'USERS' section is active, showing 'USER ACCOUNTS' with 'Default Time Zone' and 'Default Language' dropdowns. Below is 'EXTERNAL GUEST USERS' with a note 'External Guest Settings moved to Client Policy'. The 'GLOBAL DIRECTORY' section has a checked option 'External Contacts are public by default'. The 'CUSTOM FIELDS' section contains two tables: 'Custom Field Name' with entries 'Department', 'GuestInvitationStatus', and 'Region'; and 'Custom Field Values' with entries 'Support' and 'Training'. Each table has 'Add', 'Modify', and 'Remove' buttons. At the bottom are 'Save' and 'Reset Changes' buttons.

Figura 9-9 Página de usuarios

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **USERS**. La página **USERS** contiene la sección **CUSTOM FIELDS**. Puede crear campos personalizados para conocer mejor a sus invitados y mejorar los datos de los informes. Los campos personalizados pueden aparecer en la página **PROFILE** de un usuario. Los **Custom Fields** requieren un:

- **Custom Field Name:** Agregar, modificar o eliminar el nombre del campo personalizado.
- **Custom Field Value:** Agregar, modificar o eliminar los valores del campo **Custom Field Value**. Los valores de los campos personalizados se incluyen en un informe del usuario exportado.

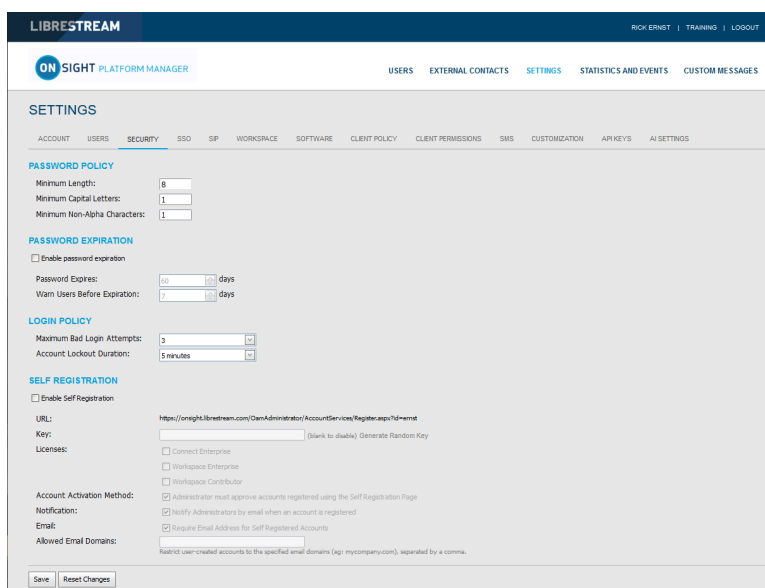


Nota: Los campos personalizados se incluyen en un informe del usuario exportado.

Referencia relacionada

Usuarios, mejores prácticas (en la página 120)

9.4. Seguridad



The screenshot shows the 'LIBRESTREAM' interface with the 'ON SIGHT PLATFORM MANAGER' header. The main navigation includes 'USERS', 'EXTERNAL CONTACTS', 'SETTINGS', 'STATISTICS AND EVENTS', and 'CUSTOM MESSAGES'. The 'SETTINGS' page has a sub-menu with 'ACCOUNT', 'USERS', 'SECURITY', 'SSO', 'SIP', 'WORKSPACE', 'SOFTWARE', 'CLIENT POLICY', 'CLIENT PERMISSIONS', 'SMS', 'CUSTOMIZATION', 'API KEYS', and 'AI SETTINGS'. The 'SECURITY' section is active, showing 'PASSWORD POLICY' with 'Minimum Length' (8), 'Minimum Capital Letters' (1), and 'Minimum Non-Alphabetical Characters' (1). Below is 'PASSWORD EXPIRATION' with 'Enable password expiration' (unchecked), 'Password Expires' (30 days), and 'Warn Users Before Expiration' (7 days). The 'LOGIN POLICY' section has 'Maximum Bad Login Attempts' (5) and 'Account Lockout Duration' (5 minutes). The 'SELF REGISTRATION' section has 'Enable Self Registration' (unchecked), 'URL' (https://onight.librestream.com/OnAdministrator/AccountServices/Register.aspx?d=xxxx), 'Key' (Generate Random Key), and 'Licenses' (Connect Enterprise, Workspace Enterprise, Workspace Contributor). The 'Account Activation Method' section has 'Notification' (checked), 'Email' (checked), and 'Allowed Email Domains' (Restrict user-created accounts to the specified email domains (eg: mycompany.com), separated by a comma).

Figura 9-10 Seguridad

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SECURITY**. Se muestra la página **SECURITY** que le permite modificar las políticas de su contraseña y de inicio de sesión. Están disponibles las siguientes secciones: **PASSWORD POLICY**, **PASSWORD EXPIRATION**, **LOGIN POLICY** y **SELF REGISTRATION**.

Referencia relacionada

[Seguridad, mejores prácticas \(en la página 121\)](#)

9.4.1. Política de contraseña

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SECURITY**. Se muestra la página **SECURITY**. Busque la sección **PASSWORD POLICY** en donde podrá establecer la política del dominio y del cliente para las contraseñas que incluyen:

- **Minimum Length** (caracteres): introduzca un valor numérico.
- **Minimum Capital Letters** (caracteres): introduzca un valor numérico.
- **Minimum Non-Alpha Characters**: introduzca un valor numérico.

Referencia relacionada

[Seguridad, mejores prácticas \(en la página 121\)](#)

9.4.2. Expiración de la contraseña

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SECURITY**. Se muestra la página **SECURITY**. Busque la sección **PASSWORD EXPIRATION** y modifique los siguientes parámetros:

- Casilla de verificación **Enable password Expiration**: habilite esta opción para forzar la expiración de la contraseña.
- **Minimum**: introduzca un valor en días. Por ejemplo, mínimo: 1 día, máximo: 365 días.
- **Warn Users Before Expiration**: establezca la duración en días como **Minimum**: 0 días, o **Maximum**: 365 días.

Referencia relacionada

[Seguridad, mejores prácticas \(en la página 121\)](#)

9.4.3. Política de inicio de sesión

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SECURITY**. Busque la sección **LOGIN POLICY** en donde podrá modificar su política de inicio de sesión para:

- **Maximum Bad Login Attempts**: establezca el número de intentos permitidos antes de que el usuario se bloquee.
- **Account Lockout Duration**: establezca la duración del período de bloqueo como: **5, 15, 30** minutos, o **Forever** si es necesario.



Nota: La opción **Forever** requiere que el administrador desbloquee la cuenta para conceder el acceso.

Referencia relacionada

[Seguridad, mejores prácticas \(en la página 121\)](#)

9.4.4. Autorregistro

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SECURITY**. Se muestra la página **SECURITY**. Busque la sección **SELF REGISTRATION**. Esta configuración permite que los usuarios se autorregistren para obtener una cuenta navegando a una URL de autorregistro. La URL debe ser distribuida por el administrador y puede estar protegida por una clave de autorregistro. Están disponibles los siguientes parámetros:

- La casilla de verificación **Enable Self Registration**: le permite al usuario introducir la información de su propia cuenta, incluyendo el nombre de usuario, la contraseña inicial, el nombre, los apellidos, el correo electrónico y la clave de autorregistro (si se requiere).
- **URL**: la URL de autorregistro generada por el sistema. Esta debe distribuirse a los usuarios que deseen autorregistrarse.
- **Key**: introduzca una clave de registro para protegerse del acceso no autorizado a estas cuentas de usuario. Esta clave debe distribuirse a los usuarios que deseen autorregistrarse.
- **Licenses**: seleccione las licencias que se asignarán a cada usuario autorregistrado. Debe haber licencias disponibles para que el registro sea exitoso.
- **Account Activation Method**: cuando se habilita, el administrador debe aprobar las cuentas registradas mediante la página de autorregistro.
- **Notification**: habilita la casilla de verificación **Administrator must approve accounts register using the Self Registration Page** para asegurarse de que le notifiquen por correo electrónico al administrador cuando se registre una nueva cuenta.
- **Email**: habilita la opción para **Require Email Address for Self-registered Accounts**.
- **Allowed Email Domains**: introduce una lista de valores separados por comas de los dominios de correo electrónico permitidos para los usuarios registrados. Use esta opción combinada con la configuración **Required Email** para restringir el acceso a las cuentas autorregistradas.

Referencia relacionada

[Seguridad, mejores prácticas \(en la página 121\)](#)

9.5. Inicio de sesión único

LIBRESTREAM
ON SIGHT PLATFORM MANAGER

USERS EXTERNAL CONTACTS SETTINGS

SETTINGS

ACCOUNT USERS SECURITY **SSO** SIP WORKSPACE SOFTWARE CLIENT POLICY CLIENT PERMISSIONS SMS CUSTOMIZATION

SINGLE SIGN-ON

Enable Single Sign-On

Single Sign-On State: **DISABLED**

Standard Users: Required Optional (allow Onsight credential login)

Administrators: Required Optional (allow Onsight credential login)

Offline Login: Allow clients to operate offline

SAML CONFIGURATION

LOCAL SERVICE PROVIDER SETTINGS

SSO Domain: ernst

Entity ID: https://onsight.librestream.com/OamAdministrator/ernst/

ACS URL: https://onsight.librestream.com/OamAdministrator/SSO/SAML/ACS/ernst/

Local SAML Certificate SHA1 Hash: e40f779f421a9b02025170a1819c25864400f9195

Export SP Metadata Download SP Certificate

PARTNER IDENTITY PROVIDER SETTINGS

Entry ID:

Single Sign-on URL:

Single Sign-on Binding: HTTP Redirect

Request Signature: Sign Authentication Requests

Signature Algorithm: RSA-SHA1

Digest Algorithm: SHA-1

Response Signature: Require Signed Responses

Assertion Signature: Require Signed Assertions

Assertion Encryption: Require Encrypted Assertions

IDP Signing Certificate: None specified

Import IDP Metadata Upload IDP Certificate

Notification: Require Signed Assertions

Assertion Encryption: Require Encrypted Assertions

IDP Signing Certificate: None specified

Import IDP Metadata Upload IDP Certificate

USER IDENTITY FEDERATION

USER IDENTITY MAPPING

Onsight Account Field: User Name

Mapped IDP Attribute: Subject Name ID

SELF REGISTRATION

Automatically create account for new users on login

Notification: Notify Administrators by email when an account is registered

Email: Require Email Address for Self Registered Accounts

Allowed Email Domains: Prompt on First Login

Name: Same as User Name

Password: Auto-generate

USER PROVISIONING LINKS

SSO Client Login: https://onsight.librestream.com/OamAdministrator/SSO/SAML/Login/?ernst\$sessiontoken=client

Windows Client Download: https://onsight.librestream.com/OamAdministrator/Download/Download.aspx?Mode=Download&FullName=&UserName=&Domain=ernst&Language=en&OsVersion=

Mobile Client Download: https://onsight.librestream.com/OamAdministrator/AccountServices/Default.aspx?getid=ernst


Save Reset Changes

Figura 9-11 Configuración SSO

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SSO**. Se muestra la página **SSO** que le permite modificar los parámetros del inicio de sesión. Están disponibles las siguientes secciones: **SINGLE SIGN-ON**, **SAML CONFIGURATION**, y **USER IDENTITY FEDERATION**.

Onsight Platform Manager admite el Inicio de sesión único (SSO) usando el Lenguaje de marcado de aserción de seguridad (SAML v2.0). SAML es un complemento con licencia para clientes de Enterprise y es un estándar abierto para el intercambio de datos de autenticación y de autorización entre dos partes: Un proveedor de servicio (SP) y el proveedor de identidad (IdP). En este caso, OPM actúa como el SP para su SSO IdP.

Si usted está migrando usuarios existentes de Onsight a SSO, puede hacer clic en el enlace de la derecha **Send Instructions**, para seleccionar a los usuarios a los que les enviará las instrucciones. Puede seleccionar usuarios individuales o grupos. Ellos recibirán un correo electrónico con las instrucciones para iniciar sesión.

 **Nota:** Los usuarios invitados externos siempre deben iniciar sesión con las credenciales de Onsight, es decir, el nombre de usuario y la contraseña. Los usuarios invitados externos pueden iniciar sesión con el enlace de inicio de sesión que está en el correo electrónico de invitación o el mensaje SMS que recibieron. El nombre de usuario y la contraseña también están incluidos en el correo electrónico de invitación.


 **Consejo:** Comuníquese con <mailto:support@librestream.com> para configurar el SSO.

9.5.1. Inicio de sesión único

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SSO**. Se muestra la página **SSO**. Busque la sección **SINGLE SIGN-ON**.

Para **Standard Users** y **Administrators**:

- Elija **Required** u **Optional** para seleccionar si desea que los usuarios solo inicien sesión con SSO (requerido) o que tengan la opción de firmar con su Cuenta de Onsight (opcional).

 **Nota:** El propietario de cuenta siempre puede iniciar sesión con sus credenciales de la cuenta Onsight, independientemente de la opción que haya establecido.

- **Offline Login:** Habilite la opción **Allow clients to operate offline** si desea que los usuarios puedan iniciar sesión como clientes de Onsight cuando el acceso a la red no está disponible. En este caso, si un usuario no puede acceder al Proveedor de identidad (IdP), podrá iniciar sesión en Onsight Connect.

9.5.2. Configuración del lenguaje de marcado de aserción de seguridad

El Lenguaje de Marcado de Aserción de Seguridad (SAML, por sus siglas en inglés), es un complemento con licencia para clientes de Enterprise y es un estándar abierto para el intercambio de datos de autenticación y de autorización entre dos partes.

9.5.2.1. Proveedor de servicio local

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SSO**. Se muestra la página **SSO**. Busque **LOCAL SERVICE PROVIDER SETTINGS** en la sección **SAML CONFIGURATION**.

Esta configuración permite que Onsight Platform Manager sea **Service Provider** (SP) de su **Identity Provider** (IdP).

- **SSO Domain:** proporciona el nombre del dominio SSO que será utilizado por Onsign. Este valor es igual al nombre de dominio Onsign.
- **Entity ID:** proporciona el nombre OPM de la identificación de la entidad para el IdP.
- **ACS URL:** proporciona el nombre OPM de la identificación de la URL de ACS para el IdP.

9.5.2.2. Configuración de sus ajustes de IdP

Inicie sesión en OPM y seleccione **SETTINGS** en el menú principal y haga clic en la pestaña **SSO**. Se muestra la página **SSO**. Busque **PARTNER SERVICE PROVIDER SETTINGS** en la sección **SAML CONFIGURATION**.

Para configurar manualmente los ajustes de su IdP, deberá:

1. Presione el botón **Export SP Metadata** para exportar el archivo de metadatos del proveedor de servicio (SP): `SPMetadata.xml`.
2. Cargue el archivo `SPMetadata.xml` a su (IdP) **SSO Identify Provider**.
3. Descargue el archivo de metadatos de IdP desde su IdP.



Nota: Si necesita una comunicación cifrada entre OPM y su IdP, deberá importar el certificado de SP OPM a su IdP.

4. Presione el botón **Download SP Certificate** para descargar el archivo del certificado público (SP) de **Service Provider**.
5. Cargue el archivo `SP Certificate` en su (IdP) **SSO Identify Provider**. Esto completa el procedimiento.

9.5.2.3. Proveedor de servicio de socio

The screenshot shows the Onsign Platform Manager SSO configuration page. The page is divided into two main sections: LOCAL SERVICE PROVIDER SETTINGS and PARTNER IDENTITY PROVIDER SETTINGS. The LOCAL SERVICE PROVIDER SETTINGS section includes fields for SSO Domain, Entity ID, ACS URL, and Local SAML Certificate SHA1 Hash. The PARTNER IDENTITY PROVIDER SETTINGS section includes fields for Entity ID, Single Sign-on URL, Single Sign-on Binding, Request Signature, Signature Algorithm, Digest Algorithm, Response Signature, Assertion Signature, Assertion Encryption, and IDP Signing Certificate. There are also buttons for 'Export SP Metadata' and 'Download SP Certificate'. The right side of the screenshot shows the USER IDENTITY FEDERATION section, which includes USER IDENTITY MAPPING, SELF REGISTRATION, and USER PROVISIONING LINKS.

Figura 9-12 Configuración SSO

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SSO**. Se muestra la página **SSO**. Busque **PARTNER SERVICE PROVIDER SETTINGS** en la sección **SAML CONFIGURATION**.

La configuración del proveedor de servicios de socio informa a OPM sobre cómo comunicarse con el **SSO Identity Provider** (IdP). En la mayoría de los casos, puede usar los botones **Import IdP Metadata** y **Upload IdP Certificate** para configurar OPM con la configuración del proveedor de identificación de socio.

La importación de los metadatos proporcionará lo siguiente:

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

Deberá configurar las siguientes opciones para que coincidan con la configuración de su IdP:

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

Haga clic en **Import IdP Metadata** para importar el archivo de **IdP metadata** que descargó de su proveedor de identidad. El archivo metadatos contendrá normalmente el certificado público IdP.

Haga clic en **Upload IdP Certificate** para cargar el **IdP Certificate** (público). Esta opción se ofrece en caso de que necesite cargar el certificado IdP manualmente. En la mayoría de los casos, el certificado IdP se proporcionará en el archivo metadatos que se obtiene de su IdP.

9.5.2.4. Configure manualmente sus ajustes IdP

Inicie sesión en OPM y seleccione **SETTINGS** en el menú principal y haga clic en la pestaña **SSO**. Se muestra la página **SSO**. Busque **LOCAL SERVICE PROVIDER SETTINGS** en la sección **SAML CONFIGURATION**.

Para configurar manualmente sus ajustes de IdP:

1. Introduzca su **Entity ID** o su IdP.
2. Introduzca su **Single Sign-on URL** o su IdP.
3. Introduzca su **Sign-on Binding type** (HTTP post o redirección).
4. Si es necesario, abajo de solicitud de firma, habilite **Sign Authentication Requests**.
5. Si es necesario, seleccione el **Signature Algorithm** utilizado por su IdP.
6. Si es necesario, seleccione el **Digest Algorithm** utilizado por su IdP.
7. Si es necesario, habilite **Require Signed Responses**.
8. Si es necesario, habilite **Require Signed Assertions**.
9. Si es necesario, habilite **Require Encrypted Assertions**.

9.5.3. Federación de identidad del usuario

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SSO**. Se muestra la página **SSO**. Busque **USER IDENTITY FEDERATION** en la sección **SAML CONFIGURATION**.

La configuración de la federación de identidad del usuario define cómo asignar los usuarios de SSO Enterprise a las cuentas de usuario de Onsignt.

9.5.3.1. Asignación de identidad de usuario

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SSO**. Se muestra la página **SSO**. Busque **USER IDENTITY FEDERATION** en la sección **SAML CONFIGURATION**.

La asignación de identidad proporciona el enlace entre la información del usuario enviada a través de la aserción SAML y los correspondientes campos de cuenta Onsignt.

La asignación le indica a OPM qué cuenta de usuario de Onsignt se está autenticando por SSO. Los atributos asignados deben tener el mismo valor, por ejemplo, el **NameID** de la aserción SAML debe ser igual al **Username** de Onsignt si estos dos atributos están asignados. El nombre y los valores de atributo distinguen entre mayúsculas y minúsculas.

Elija uno de los siguientes métodos de asignación:

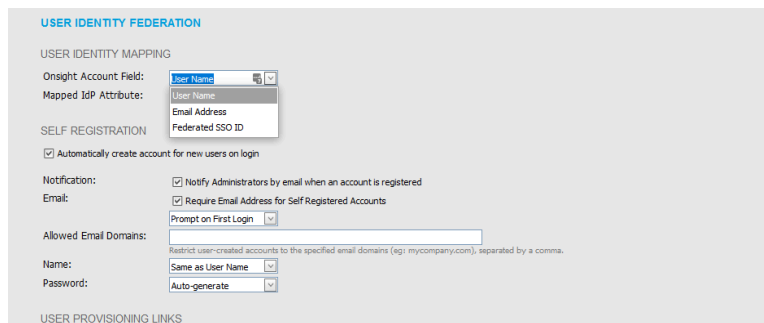
- **Username Mapping**
- **Email Mapping**
- **Federated SSO ID mapping**

9.5.3.2. Asignación del nombre de usuario

Inicie sesión en OPM y seleccione **SETTINGS** en el menú principal y haga clic en la pestaña **SSO**. Se muestra la página **SSO**. Busque **USER IDENTITY MAPPING** en la sección **USER IDENTITY FEDERATION**.

Para aplicar la asignación del nombre de usuario, deberá:

1. Seleccionar el menú desplegable **Onsignt Account Field** para comparar sus valores con los de **Mapped IdP Attribute**:
 - **User Name**: nombre de usuario de la cuenta Onsignt
 - **Email Address**: dirección de correo electrónico de la cuenta Onsignt
 - **Federated SSO Id**: ID de SSO federado asociado del usuario de Onsignt. Esto lo define el administrador de Onsignt y se puede incluir como parte de la lista de usuarios importados. Esto se puede asignar a la ID del nombre del sujeto o a un atributo de la aserción SAML.



The screenshot shows the 'USER IDENTITY FEDERATION' configuration page. Under the 'USER IDENTITY MAPPING' section, there are two dropdown menus: 'Onsignt Account Field' and 'Mapped IdP Attribute', both currently set to 'User Name'. Below these are sections for 'SELF REGISTRATION' (with a checked box for 'Automatically create account for new users on login'), 'Notification' (with a checked box for 'Notify Administrators by email when an account is registered'), 'Email' (with a checked box for 'Require Email Address for Self Registered Accounts' and a 'Prompt on First Login' dropdown), 'Allowed Email Domains' (with a text input field and a note to restrict user-created accounts), 'Name' (with a 'Same as User Name' dropdown), and 'Password' (with an 'Auto-generate' dropdown). The bottom of the page shows 'USER PROVISIONING LINKS'.

Figura 9-13 Campo de cuenta Onsignt

2. Seleccione el menú desplegable **Mapped IdP Attribute** para comparar sus valores con los de **Onsignt Account Field**:
 - **ID del nombre del sujeto**
 - **Attribute**: establece el nombre del atributo del atributo a comparar con el campo de la cuenta Onsignt

Figura 9-14 Atributo de IdP asignado



Nota: Importar usuario: si utiliza la **Federated SSO ID** para proporcionar un asignación de identidad entre los usuarios de Enterprise y las cuentas de usuario de Onsight, debe completar el campo **Federated SSO ID** para cada usuario que se enumera en el archivo UserImport.csv.

Esto completa el procedimiento.

9.5.3.3. Asignación del correo electrónico

Inicie sesión en OPM y seleccione **SETTINGS** en el menú principal y haga clic en la pestaña **SSO**. Se muestra la página **SSO**. Busque **USER IDENTITY MAPPING** en la sección **USER IDENTITY FEDERATION**.

Para aplicar la asignación del correo electrónico, deberá:

1. Seleccionar **Email Address** en el menú desplegable **Onsight Account Field**.

Figura 9-15 Dirección de correo electrónico

2. Seleccione **Attribute** en el menú desplegable **Mapped IdP Attribute**.
3. Introduzca el nombre del atributo dentro del campo **Attribute Name**, por ejemplo, **Email**. Esto completa el procedimiento.

9.5.3.4. Asignación de ID de SSO federado

Inicie sesión en OPM y seleccione **SETTINGS** en el menú principal y haga clic en la pestaña **SSO**. Se muestra la página **SSO**. Busque **USER IDENTITY MAPPING** en la sección **USER IDENTITY FEDERATION**.

Para modificar su configuración de asignación de ID de SSO federado, deberá:

1. Seleccionar **Federated SSO ID** en el menú desplegable **Onsight Account Field**.

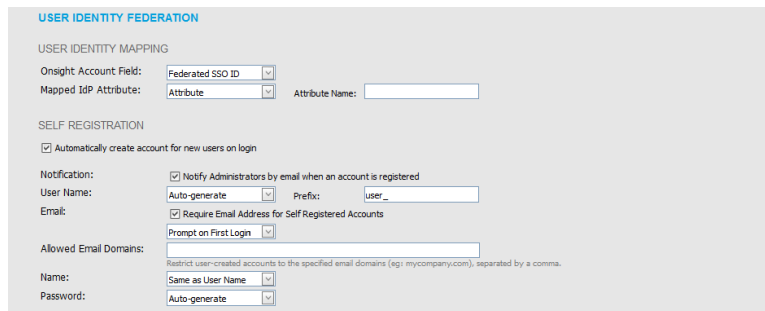


Figura 9-16 ID de SSO federado

2. Seleccione **Attribute** en el menú desplegable **Mapped IdP Attribute**.

3. Introduzca el nombre del atributo dentro del campo **Attribute Name**, por ejemplo, OPMUSER. (Podría definir el nombre de atributo que desee).
Esto completa el procedimiento.

9.5.4. Autorregistro de SSO

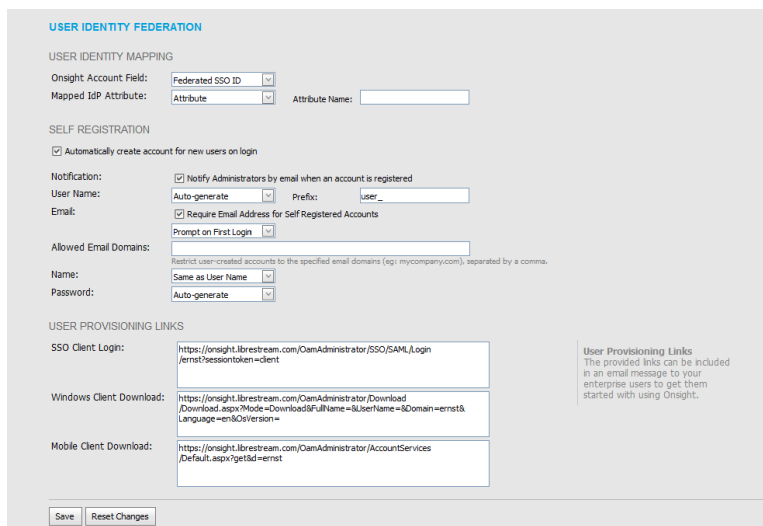


Figura 9-17 Autorregistro de SSO

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SSO**. Se muestra la página **SSO**. Busque **SELF REGISTRATION** en la sección **USER IDENTITY FEDERATION**.

Para habilitar el autorregistro, habilite la casilla de verificación **Automatically create account for new users on login**.



Nota: Por lo general, si un usuario se conecta por primera vez usando SSO y no existe ya como un usuario de Onsight, automáticamente se le creará una cuenta de Onsight.

Información general sobre el autorregistro de SSO

Para habilitar el autorregistro de SSO:

1. Establezca sus preferencias para **Notification** e **Email**:

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

2. Defina el método para crear el **User Name**:

- **Attribute:** usa el atributo asignado como nombre de usuario de Onsignt.
 - **Attribute Name:** establece el nombre del atributo que se usará como nombre de usuario de Onsignt.
- **Auto-generate:** crea el nombre de usuario de Onsignt.
 - **Prefix:** establece el prefijo para los nombres de usuario de Onsignt generados automáticamente.
- **Prompt on First Login:** solicita al usuario que introduzca un nombre de usuario de Onsignt.

3. Establezca el método **Email** que se usará para establecer la dirección de correo electrónico del usuario:

- Seleccione **Attribute** y **Attribute Name** que se usará para la dirección de correo electrónico del usuario.
- Seleccione **Prompt on First Login**, lo que requerirá que el usuario introduzca su dirección de correo electrónico la primera vez que inicie sesión en Onsignt Connect.



Nota: Su configuración de seguridad dicta si se requiere una dirección de correo electrónico para los usuarios autorregistrados.

4. Establezca el nombre personal del usuario:

- Igual que el **User Name**.
- **Attribute:** introduzca los atributos **First Name** y **Last Name** que le asignará al nombre.
- **Prompt on First Login:** solicita al usuario que introduzca el nombre y apellido.

5. Establezca la opción de crear **Password:**

- **Auto-generate:** el usuario no necesitará saber la contraseña de su cuenta de usuario de Onsignt. Esta opción solo debe usarse cuando el inicio de sesión SSO está configurado como obligatorio y es el método de inicio de sesión admitido.
- **Prompt on First Login:** esta opción debe seleccionarse si se seleccionó Opcional (permitir el inicio de sesión con credenciales de Onsignt). Los usuarios podrán iniciar sesión en Onsignt Connect directamente sin utilizar sus credenciales SSO.

9.5.5. Enlaces de aprovisionamiento de usuario

Figura 9-18 Enlaces de aprovisionamiento de usuario

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SSO**. Se muestra la página **SSO**. Busque **USER PROVISIONING LINKS** en la sección **USER IDENTITY FEDERATION**.

Los siguientes enlaces sirven como referencia. Puede incluir estos enlaces en el correo electrónico de instrucciones de implementación de su cuenta de Onsignt para sus usuarios:

- **SSO Client Login:** enlace a la página de inicio de sesión del SSO.
- **Windows Client Download:** enlace de descarga de OnSight Connect para Windows.
- **Mobile Client Link:** enlace para la página de descarga de OnSight Connect para dispositivos móviles.

9.5.6. Notificar a los usuarios existentes

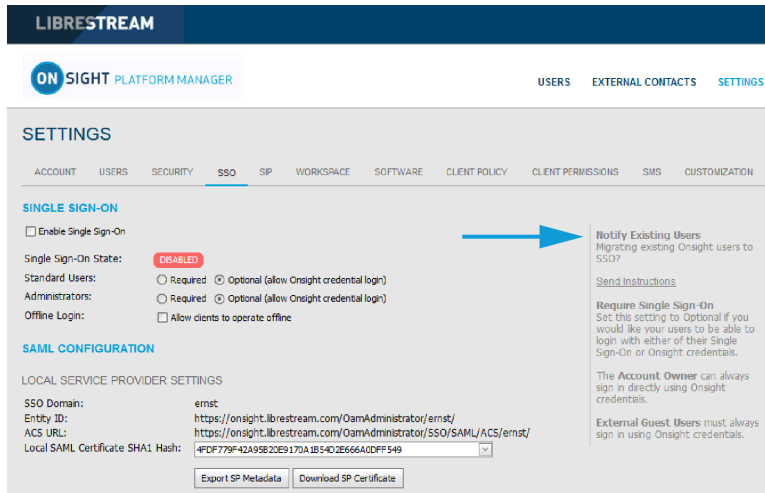


Figura 9-19 Notificar a los usuarios existentes

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SSO**. Se muestra la página **SSO**. Busque la sección **Notify Existing Users** en el lado derecho.

Una vez que complete la configuración SSO, les puede enviar instrucciones a sus usuarios existentes mediante correo electrónico.

1. Pulse el enlace **Send Instructions** en la sección **Notify Existing Users**.

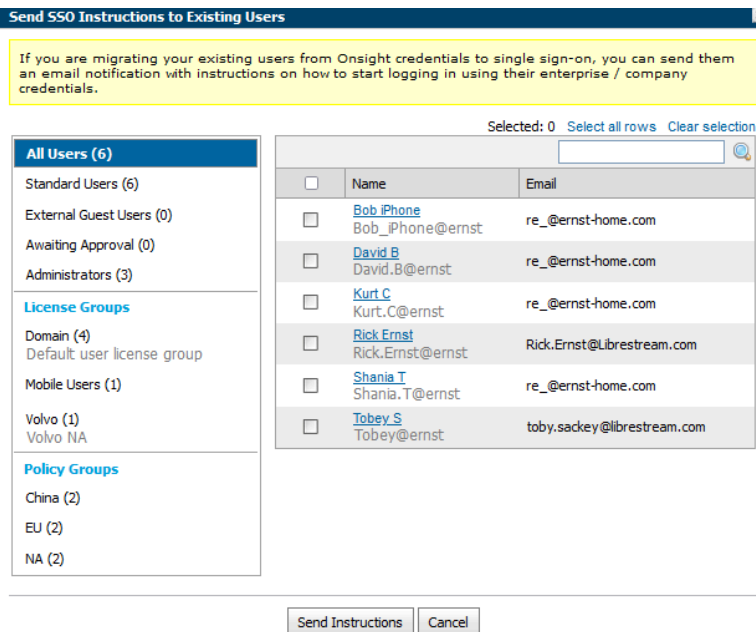


Figura 9-20 Enviar instrucciones SSO a los usuarios existentes

2. Seleccione a los usuarios que desee notificar y presione el botón **Send Instructions**. Puede pulsar el enlace **Select all rows** para seleccionar a todos los usuarios o puede también clasificarlos en función de los grupos enumerados en la columna de la izquierda.

9.5.7. Local: configuración del certificado SSO

Para OPM local, el OPM de alojamiento de servidores debe tener un certificado instalado apto para cifrado y firma SAML. El certificado SSO debe tener **Digital Signature** y las extensiones de uso de clave de **Key encipherment**, así como el **Extended key usage set** a crítico.

1. Para configurar el OPM para utilizar el certificado SSO, vaya a **Site Administration > Server Settings > General**.
2. En la sección SSO, pegue la huella digital SHA1 del certificado en el cuadro de texto SHA1 del certificado de proveedor de servicio local.
3. Para verificar el certificado, vaya a **Customer Portal > Settings > SSO**.
4. Verifique que el certificado esté disponible para su uso por parte del OPM. Haga clic en el botón **Download SP Certificate**.
5. El certificado debería descargarse correctamente.

Consulte la guía de instalación de Onsight Platform Manager local para obtener información sobre cómo implementar certificados del servidor.

9.6. Protocolo de inicio de sesión

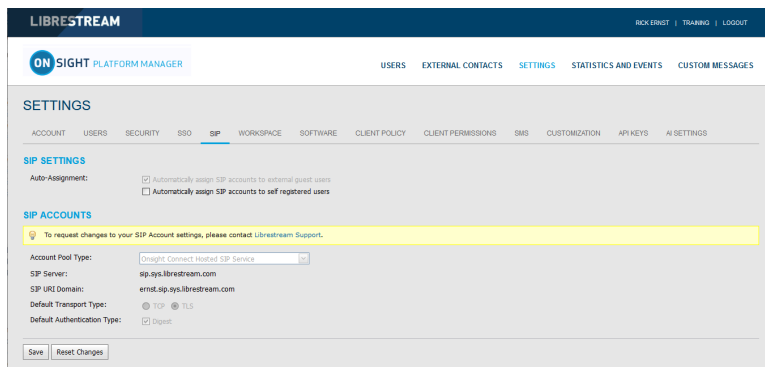


Figura 9-21 Configuración SIP

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SIP**. La página **SIP** incluye las secciones **SIP SETTINGS**, y **SIP ACCOUNTS**.

El Protocolo de inicio de sesión (SIP) es el protocolo básico de control de llamadas que conecta todas las sesiones de Onsight Connect. A cada usuario de Onsight Connect se le asignará automáticamente una cuenta SIP. Esta sección describe la configuración SIP para todos los usuarios.

Consejo: Para solicitar el cambio en la configuración de su cuenta SIP, comuníquese con <mailto:support@librestream.com> para configurar el SSO.

9.6.1. Configuración SIP

Asignación automática de autorregistro

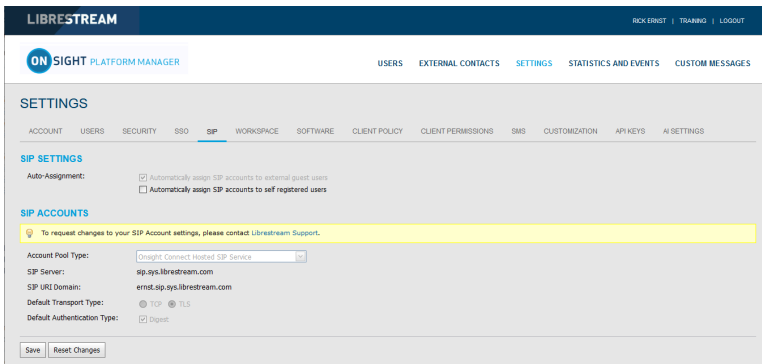


Figura 9-22 Asignación automática

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SIP**. Se muestra la página **SIP**. Busque la sección **SIP SETTINGS**.

Cuando habilite la opción **Automatically assign SIP Accounts to self-registered users** se vinculará un usuario recién registrado a una cuenta SIP. Esta opción debe habilitarse cuando se utiliza el autorregistro.

9.6.2. Cuenta SIP

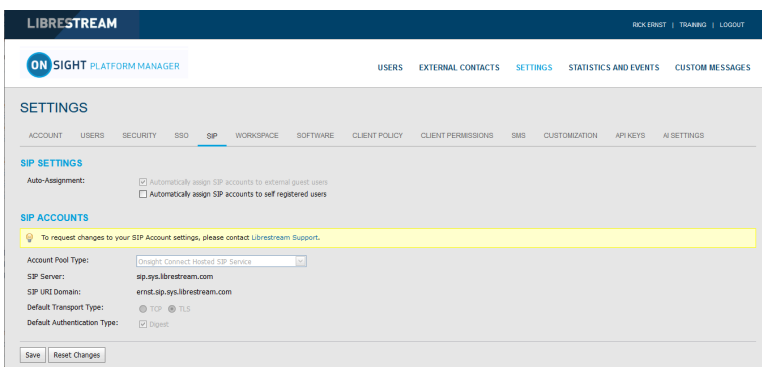


Figura 9-23 Cuenta SIP

Hay tres opciones para configurar el servidor SIP a las que se puede acceder desde el menú desplegable **Account Pool Type**:

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

Cuando un cliente aloja un servidor SIP de Enterprise, las cuentas SIP se introducen en el grupo de asignación automática, usando varias cuentas o una cuenta compartida.

Cuando se usa una cuenta compartida, el servidor SIP debe admitir nombres de usuario comodín. El SIP URI (Dirección SIP) se genera automáticamente a partir del dominio de SIP URI y del nombre de usuario asociado con la cuenta de usuario de Onsight.

El transporte seleccionado (TCP o TLS) debe coincidir con la configuración del servidor SIP al que se está registrando. Por seguridad, se recomienda TLS. La precisión de la fecha y la hora en el endpoint es un requisito para TLS.

Cada usuario puede estar asignado a dos cuentas SIP: Una pública y una privada. Esto es para permitir el registro del SIP dependiendo de la ubicación de la red. Si un usuario es interno al Firewall, será registrado en el servidor privado. Si son externos al Firewall, serán registrados en el servidor público, por ejemplo, Cisco VCS Expressway y control.

Los usuarios que se registren solo a un Servidor SIP (público o privado) solo necesitan proporcionar la configuración SIP para el único servidor. Use la configuración SIP pública como cuenta principal SIP.

9.6.2.1. Servicio de SIP alojado Onsight Connect

Servicio de SIP alojado Onsight Connect es el servicio de SIP predeterminado que se utiliza cuando está suscrito al servicio alojado Onsight de Librestream.

Los ajustes son solo de lectura, ya que la información de la cuenta SIP la administra de manera automática Onsight Platform Manager en su dominio. Las cuentas SIP se asignan automáticamente a cada usuario cuando el administrador de OPM crea una cuenta de usuario.

La configuración SIP incluye:

- **SIP Server:** enumera el servidor SIP de Librestream asignado a su dominio.
- **SIP URI Domain:** enumera el dominio de SIP URI y se muestra como la porción del dominio para la dirección SIP del usuario; por ejemplo, user@sipuridomain.com.
- **Default Transport Type:** TCP o TLS, el predeterminado es TLS. Este proporciona comunicación cifrada para el protocolo SIP.
- **Default Authentication Type:** resumen proporcionado como referencia de solo lectura.

9.6.2.2. Varias cuentas

Se usan varias cuentas cuando usted aloja su propio servidor SIP de Enterprise y tiene un número fijo de cuentas SIP disponibles para usar con Onsight Connect. Cada cuenta SIP se crea en su servidor SIP de Enterprise con un nombre de autenticación único, contraseña y URI. Luego, se agrega de forma manual al grupo SIP de OPM para utilizarla a medida que se agregan usuarios de Onsight Connect.

9.6.2.2.1. Crear varias cuentas

Inicie sesión en OPM y seleccione **SETTINGS** en el menú principal y haga clic en la pestaña **SIP**.

Para crear varias cuentas SIP, deberá:

1. Adquirir la información de su cuenta SIP Enterprise del Administrador del servidor SIP. La información de la cuenta SIP debe incluir la dirección de servidor SIP (público o privado), el nombre de autenticación, la contraseña, el nombre de usuario y el dominio SIP (el nombre de usuario y el dominio de SIP se combinan para crear la SIP URI).
2. En la sección **SIP Settings**, seleccione **Automatically assign SIP accounts to self-registered users**.
3. Establezca **Account Pool Type** en **Multiple Accounts**.
4. Establezca **Public Server** en la dirección de servidor público que proporciona el administrador del servidor SIP.
5. Seleccione **TCP** o **TLS** como el tipo de transporte. Se recomienda TLS.
6. Agregue la información de las cuentas SIP para cada usuario haciendo clic en el botón **New**.
 - En la pestaña Public, ingrese SIP URI (SIP URI = username & sip domain, por ejemplo, user@sip.librestream.com), Nombre de autenticación y Contraseña de autenticación.
7. Repita los pasos del 4 al 6 para el servidor privado si es necesario.
8. **Save** los cambios.
Esto completa el procedimiento.

9.6.2.3. Cuenta compartida

Las cuentas compartidas se usan cuando se dispone de cuentas SIP comodín para usarlas con Onsight Connect. Primero se crea la cuenta SIP comodín en el servidor SIP y luego se agrega manualmente al grupo SIP de OPM para usarla a medida que se agregan usuarios de Onsight Connect. Cada cuenta SIP comparte el mismo nombre de autenticación y la misma contraseña de autenticación, pero tienen un SIP URI único. EL SIP URI se crea automáticamente combinando el nombre de usuario de Onsight y el dominio de SIP, por ejemplo: jdoe@sipdomain.com.

9.6.2.3.1. Crear una cuenta compartida

Inicie sesión en OPM y seleccione **SETTINGS** en el menú principal y haga clic en la pestaña **SIP**.

1. Adquirir la información de su cuenta SIP del administrador del servidor SIP. La información de la cuenta SIP debe incluir **Server Address, SIP URI Domain, Authentication Name y Authentication Password**.
2. En la sección SIP settings, seleccione **Automatically assign SIP accounts to self-registered users**.
3. Establezca el **Account Pool Type** en **Shared Account**.
4. En la pestaña **Public Server**, establezca la **Server Address** a la dirección que proporciona el administrador de su servidor SIP.
5. Seleccione **TCP** o **TLS** como el transporte. Se recomienda TLS.
6. Establezca **SIP URI Domain** en el dominio que proporciona el administrador SIP.
7. Introduzca **Authentication User Name** y **Authentication Password**.
8. Repita los pasos del 3 al 7 en la pestaña **Private Server**, si es necesario.
9. Haga clic en **Save**.
Esto completa el procedimiento.

9.6.2.4. Asignación manual de cuentas SIP a usuarios

Las cuentas SIP se asignan cuando se crea una cuenta de usuario nueva. La casilla de verificación **Automatically assign a SIP account to this user** está habilitada de forma predeterminada.

Las cuentas SIP también pueden asignarse en la pestaña Usuario y grupos al seleccionar a un usuario existente (marcando la casilla de verificación junto a su nombre) y luego, seleccionar **Assign/Restore SIP Account** en el menú desplegable **More**.

Una vez que se asigne o restablezca la configuración SIP, los ajustes de la cuenta SIP del usuario estarán disponibles para su uso tan pronto como la cuenta OnSight reciba los nuevos ajustes. Esto sucederá en el siguiente inicio de sesión o si ya inició sesión durante la siguiente actualización del servidor (en los siguientes 60 segundos).

9.7. OnSight Workspace

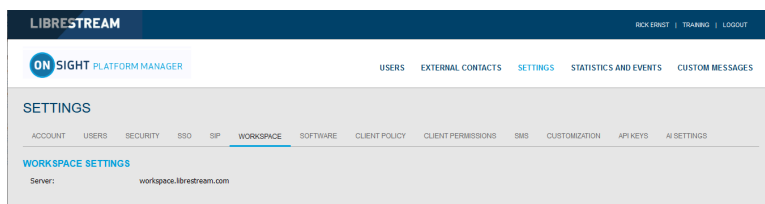


Figura 9-24 OnSight Workspace

Cuando OnSight Workspace está habilitado para su dominio, el servidor de Workspace se muestra para referencia en la página de configuración. Como administrador, usted debe asignarse una licencia Workspace Enterprise para configurar los ajustes de Workspace.

Al utilizar OnSight Workspace, los usuarios autorizados pueden cargar, ver, compartir y administrar datos, imágenes y grabaciones OnSight, así como contenido externo como manuales de productos y esquemas. Con controles de permiso detallados, las empresas pueden garantizar que solo los equipos y personas autorizadas puedan acceder a contenido específico.

Workspace se integra con la plataforma completa de OnSight al proporcionar una solución práctica para ayudar en la administración del conocimiento y requisitos de pista de auditoría. Las características clave de Workspace incluyen:

- Carga automática o manual de datos, imágenes o grabaciones desde OnSight
- Controles de carga opcionales para administrar situaciones de campo como consumo de datos móviles
- Opción de agregado rápido para almacenar manuales de productos, esquemas u otros archivos
- Etiquetado de contenido para búsqueda y recuperación rápidas
- Control automático de versiones de contenido con capacidades de auditoría incorporadas

- Arquitectura segura y controles de permiso detallados
- Informes avanzados para auditoría de contenido y uso en toda la empresa
- Acceder a contenido y datos en sus sistemas de gestión interna con API de Workspace
- Seleccionar tipos de licencia Enterprise o Contributor para controlar y extender la recopilación de datos de Workspace

Referencia relacionada

Política del cliente, mejores prácticas (en la página 124)

Permisos de cliente, mejores prácticas (en la página 136)

9.7.1. Habilitar el acceso a Workspace para usuarios

Iniciar sesión en OPM.

Para habilitar el acceso a Workspace para sus usuarios, deberá:

1. Acceder a la página **Users** y seleccionar los usuarios que desea que tengan acceso a Workspace.

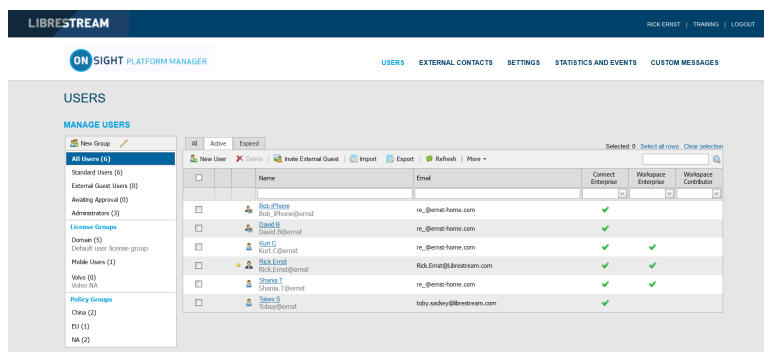


Figura 9-25 Usuarios

2. Luego, seleccione **More > Assign/Restore Workspace Account**.

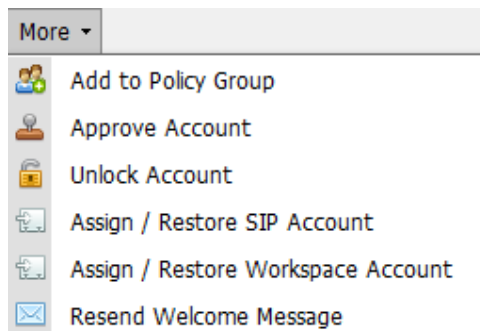




Figura 9-26 Menú desplegable Más

3. Coloque a los usuarios del Workspace en un grupo. También puede optar por usar un grupo existente, como **All Users**.
4. El paso final es habilitar el Workspace en una **Groups Client Policy** para los usuarios.
5. Seleccione el grupo y haga clic en el icono  **Modify Group** (icono de lápiz).
6. Seleccione la pestaña **CLIENT POLICY**.
7. Haga clic en  **Choose Settings**.
8. Seleccione la configuración del **Workspace** a habilitar en **Client Policy** que incluye:
 - **Access**: otorga acceso al Workspace.
 - **Upload Path**: establece la ruta de carga predeterminada en el Workspace.

- **Auto Upload Media:** habilita la carga automática de todos los medios capturados durante una llamada cuando finaliza la llamada.
- **Maximum Upload Bit Rate (Kbps):** establece el ancho de banda máximo dedicado a la transmisión de carga.
- **Restrict Upload Folder Access to the Owner:** solo permite el acceso a la carpeta de carga del propietario.
- **Allow Cellular/Mobile Data Usage:** permite el uso de datos móviles/celulares para cargar medios en el Workspace.

9. Haga clic en **OK**.

10. En la sección **Workspace** establezca los valores deseados. Esto completa el procedimiento.

Referencia relacionada

[Política del cliente, mejores prácticas \(en la página 124\)](#)

[Permisos de cliente, mejores prácticas \(en la página 136\)](#)

9.8. Workspace Webhooks

WEBHOOKS CONFIGURATION

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

Figura 9-27 Webhooks

Las soluciones locales de Onsight Workspace y OPM admiten un mecanismo de notificaciones por Webhooks que permiten que un sistema externo le notifique cuando se realicen cambios en los activos del Workspace. Las notificaciones están en forma de devoluciones de llamada HTTP que se inician desde Onsight Workspace hasta su servicio externo designado cuando se produce un evento. Los eventos para los activos y documentos de Workspace se desencadenan cuando se crea, modifica o elimina un elemento. Las notificaciones por Webhooks permiten que varias plataformas externas se integren. Para obtener más detalles, consulte la Guía de Webhooks de Onsight Workspace.

Los Workspace Webhooks son creados y administrados por un administrador de OPM cuando el Workspace está habilitado y configurado para su cuenta.

9.8.1. Crear y modificar la configuración de un Webhook

Inicie sesión en OPM como un administrador. Haga clic en **Settings > Workspace**.


Para crear o modificar una configuración Webhook, deberá:

1. Acceder a la tabla **Webhooks CONFIGURATION** para mostrar una lista de Webhooks.

WEBHOOKS CONFIGURATION

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

Figura 9-28 Configuración Webhooks



2. Haga clic en el icono  **New** para agregar la configuración de un webhook. Aparece el formulario New Webhook Configuration.

Los campos editables incluyen:

- **Name** (Obligatorio): un nombre descriptivo para el webhook que se utiliza con fines de visualización.
- **Description:** una descripción opcional para el webhook.
- **Consumer URI:** el URI absoluto para el servicio de destino que recibirá notificaciones de devolución de llamada.

- **HTTP Headers:** proporciona una lista de pares de clave-valor para encabezados HTTP que se incluirán con cada notificación que se envía a un URI del consumidor.
- **Administrator Email:** la dirección de correo electrónico del administrador de esta configuración de webhook. Todas las notificaciones de estado o fallas en la entrega se enviarán a esta dirección de correo electrónico.
- **Batch Frequency:** la duración máxima de los eventos de webhook que se agruparán en una sola notificación en minutos. Si es 0, los eventos se agruparán con una duración mínima de 10 segundos.
- **User Name/Password:** si se establece, la notificación usará la autenticación básica HTTP con estas credenciales.
- **Active:** si no se marca, no se entregarán notificaciones para este webhook.
- **Events:** los tipos de eventos que activarán las notificaciones de webhook para esta configuración. Debe seleccionar un evento.

Figura 9-29 Nueva configuración Webhooks

- Introduzca todos los campos obligatorios y haga clic en **OK** para guardar la configuración Webhook.
- Haga clic en el icono **Edit**  para mostrar la ventana emergente **Edit Webhook Configuration**. Esta es idéntica a la ventana emergente New Webhook Configuration y le permite hacer cambios a una configuración existente.
- Seleccione una o más configuraciones de webhook de la tabla y haga clic en el icono  **Delete** para eliminar permanentemente los webhooks. Después de la eliminación, no se enviarán más notificaciones a los servicios del consumidor para esas configuraciones.
- Haga clic en el botón **Test Workbook** en la tabla **WEBHOOK CONFIGURATIONS** o en la ventana emergente **New/Edit Webhook Configuration** para probar la configuración.
 - Una notificación de evento de prueba se activará de inmediato y se envía al URI del consumidor desde el Workspace.
 - OPM mostrará los resultados de la prueba, incluyendo la duración de la prueba y el código de estado devuelto a Workspace desde su servicio al cliente.

Esto completa el procedimiento.

9.9. Actualizaciones de software

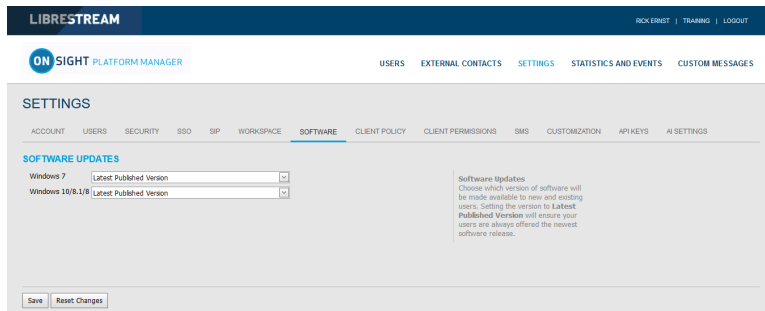


Figura 9-30 Página de software

La distribución de Software para OnSight Connect para Windows, OnSight Cube, el 5000HD y el Hub de Collaboration es administrada por OnSight Platform Manager. Librestream proporciona actualizaciones como parte del proceso de liberación del Software.

Referencia relacionada

[Software, mejores prácticas \(en la página 123\)](#)

9.9.1. OnSight Connect para Windows

El administrador de OPM puede seleccionar qué versión de OnSight Connect para Windows está disponible para que los usuarios de OnSight Connect la descarguen. Puede seleccionar **Latest Published Version** o una **Specific Version** en la lista desplegable.

Dependiendo de su selección, los usuarios recibirán **Welcome emails** o **External Guest Invites** con enlaces para descargar las versiones seleccionadas de OnSight Connect para Windows.

Referencia relacionada

[Software, mejores prácticas \(en la página 123\)](#)

9.9.2. Notificaciones de liberación nueva

Cuando se selecciona la última versión publicada en la página de actualizaciones de software, los usuarios de Windows recibirán notificaciones en la ventana de inicio de sesión de OnSight Connect cuando una versión nueva se publique y esté disponible para descargar.

Los usuarios de Android y de iOS recibirán actualizaciones de la aplicación a través de las tiendas de aplicaciones. Los usuarios pueden configurar sus teléfonos para recibir actualizaciones automáticas de las tiendas de aplicaciones. Consulte las instrucciones de la tienda de aplicaciones de su teléfono para actualizaciones automáticas.

Referencia relacionada

[Software, mejores prácticas \(en la página 123\)](#)

9.9.3. Actualizaciones para OnSight Cube, Hub de Collaboration y 5000HD

Librestream publica las actualizaciones de OnSight Cube y Hub de Collaboration. Estas están disponibles a través de OnSight Platform Manager como parte del proceso regular de liberación de software.

Cuando una nueva versión está disponible, los usuarios pueden **Buscar actualizaciones** para descargar e instalar la última liberación del software seleccionando:

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

9.9.4. Actualizaciones de software local

Consulte OnSight Platform Manager: guía de instalación para obtener información sobre cómo implementar paquetes de actualización para OnSight Connect para Windows, OnSight 5000HD y Hub de OnSight Collaboration. Las actualizaciones del cliente de OnSight móvil están disponibles en las tiendas de aplicaciones para instalaciones locales.

9.10. Política y permisos del cliente

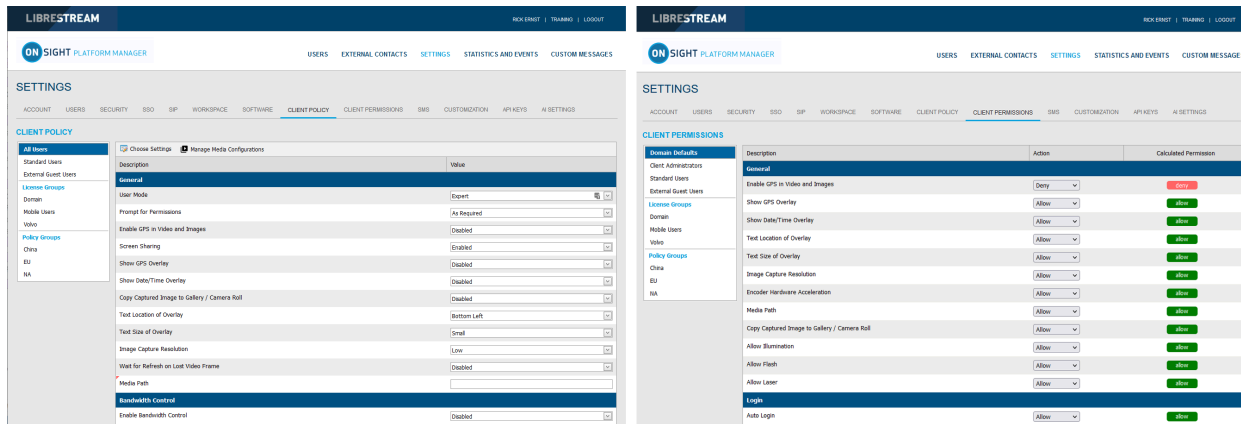


Figura 9-31 Política del cliente y permisos del cliente

CLIENT POLICY y **CLIENT PERMISSIONS** se pueden configurar al hacer clic en **SETTINGS** > **CLIENT POLICY** o **CLIENT PERMISSIONS** y se aplican al grupo **All Users**. El grupo Todos los usuarios contiene a todos los usuarios en el dominio.

Client Policy le permite al administrador de OPM elegir qué ajustes de configuración son aplicables a un endpoint de OnSight según la membresía de grupo (Grupo de política) o una Política del cliente de usuario asignada individualmente.

Group Client Policy se aplica a cada miembro de un grupo. Seleccione la configuración para cada ajuste con base en los grupos. Los usuarios pueden pertenecer a varios grupos y prevalecen los ajustes de mayor prioridad.

User Client Policy es la política asociada directamente con una cuenta de usuario. Se usa para anular cualquier **Group Policy** que rige según la membresía de grupo. Si un usuario pertenece a varios grupos, cada uno regido por su propia **Client Policy**, el usuario estará sujeto a los ajustes de la política en función de la configuración **prioritaria** entre los ajustes de la política del cliente de usuario y la de grupo para ese usuario. La política del cliente de usuario predeterminada para un usuario es la configuración **Inherit all**, lo cual significa que la **Group Policy** prevalece. Cada categoría de **Client Policy** se puede configurar en **Inherit**, **Override** o **Clear**.

Editar política del cliente

Para editar **Client Policy** para un usuario, seleccione **Usuario** y luego, seleccione la pestaña **CLIENT POLICY**. Ajuste la política para cada configuración en **Action**. Están disponibles las siguientes opciones:

- **Inherit**: aplica la configuración de la política del grupo para el usuario. Este es el valor predeterminado para cada ajuste cuando se crea un usuario nuevo.
- **Override**: aplica el ajuste que se configuró en la página de Política del cliente de usuario, no el del grupo de política.
- **Clear**: no aplica ninguna política para los ajustes, en su lugar use el valor actual en el endpoint.

Referencia relacionada

[Política del cliente y precedencia de prioridad \(en la página 113\)](#)


[Política del cliente, mejores prácticas \(en la página 124\)](#)

[Permisos de cliente, mejores prácticas \(en la página 136\)](#)


9.10.1. Usuarios invitados externos

The screenshot shows the 'CLIENT POLICY' settings page in the OnSight Platform Manager. The page is divided into several sections: 'All Users', 'Standard Users', 'External Guest Users', 'License Groups', 'Domain', 'Mobile Users', 'VoVo', 'Policy Groups', and 'China'. The 'External Guest Users' section is currently selected, showing a table of settings. The settings include: 'Allow users to invite external guests' (Enabled), 'Allow text message guest invitations' (Disabled), 'SMS Max Message to User Length' (100), 'Guest users must change temporary password on initial login' (Disabled), 'Send "Invitation Sent" confirmation to host' (Enabled), 'Disable recording of images and video' (Enabled), 'Disable global directory access' (Disabled), 'Expiry' (1 days), 'User can choose expiry time when inviting guests' (Disabled), 'Deactivate guest user account when removed from contact list' (Disabled), 'Include option for guest to call host immediately' (Enabled), 'From Email' (Default), 'Custom Fields' (Department, GuestInviteStatus), and 'Allow Setting User Mode while inviting guest' (Disabled).


Figura 9-32 Política del cliente de grupo

 **Nota:** Ahora el comportamiento del usuario invitado está establecido en el nivel del grupo. Ya no es una configuración del nivel de dominio.


- **Allow users to invite external guest:** les permite a los usuarios invitar a participantes. **Default: Enabled.**
- **Allow text message guest invitations:** les permite a los usuarios utilizar mensaje de texto para las invitaciones de participantes. **Default: Enabled.**
- **SMS Max Message to User Length:** establece el número de caracteres que se permiten para el mensaje SMS. **Default: 100.**

 **Nota:** Los mensajes SMS tienen un límite máximo de 160 caracteres, según el conjunto de caracteres que se usen. Superar este límite puede romper los vínculos que contiene el mensaje SMS. Respete este límite cuando haga cambios en los mensajes SMS. Consulte la Ayuda para mensajes personalizados en la página PERSONALIZACIÓN.

- **Password:** controla si los usuarios invitados externos deben cambiar la contraseña temporal en el inicio de sesión inicial. La opción **Default** está **Enabled**.

 **Nota:** Es posible que desee deshabilitar esta característica para los usuarios invitados para simplificar su experiencia de Llamada en OnSight.

- **Confirmation:** controla si quien invita recibirá un correo electrónico de confirmación cuando se envía la invitación. Incluirá una copia del mensaje de invitación. Los colores ayudan para indicar el estado de una invitación. Por ejemplo:
 - **Yellow:** la invitación se envió y el estado es desconocido. Por lo general, esto indica que el proveedor del servicio de correo electrónico o de SMS no ha confirmado la recepción del mensaje.
 - **Green:** el participante recibió la invitación.
 - **Red:** La invitación no se entregó.

 **Nota:** El estado de invitación de participante se informa al lado del nombre del invitado en la lista de contactos de quien invita.

- **Permissions:** establece **Disable recording of images y video** para evitar que un invitado haga grabaciones o capturas de imágenes fijas de OnSight. La opción **Default** está **Enabled**, es decir que los usuarios invitados externos no pueden grabar imágenes ni video.

i Consejo: Si lo desea, establezca **Disable global directory access** para evitar que un invitado busque el **Global Contacts Directory. Default: Disabled**, es decir que los usuarios **External Guest** pueden acceder al **Global Directory**.

Referencia relacionada

[Política del cliente, mejores prácticas \(en la página 124\)](#)

[Permisos de cliente, mejores prácticas \(en la página 136\)](#)

9.10.2. Valores predeterminados de invitación de invitado externo

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

Figura 9-33 Política del cliente de invitado externo

Estos ajustes controlan los mensajes de invitación de participante:

- **Expiry:** establece la expiración predeterminada para la cuenta de usuarios invitados externos que se crea cuando se envía la invitación de participante. **Default:** 1 día. **Minimum:** 1 día, **Maximum:** 365 días. Los usuarios pueden elegir el tiempo de expiración cuando invitan a los participantes: controla si los usuarios pueden elegir el tiempo de expiración distinto al valor predeterminado. La opción **Default** está **Disabled**.
 - **Deactivate guest user account when removed from contact list:** controla si la cuenta de usuario de invitado se desactiva automáticamente cuando quien invita elimina al invitado de su lista de contactos. **Default: Disabled**.
 - **Include option for guest to call host immediately:** controla si se le pide al usuario invitado que llame a quien invita la primera vez que inicia sesión. La opción **Default** está **Enabled**.
 - **From Email Address:** establece la dirección para responder que se muestra en el correo electrónico de invitación de participante. Puede elegir el valor predeterminado del sistema o dirección de correo electrónico de quien invita como la dirección para responder. **Default** de OnSight Platform Manager es `no-reply@librestream.com`
- i Nota:** Quien invita debe tener un correo electrónico configurado para su cuenta, si no tiene un correo electrónico se utilizará el valor predeterminado del sistema.
- **Custom Fields:** establece **Custom Fields** para incluir en el formulario de invitación de participante.
 - **Allow Setting User Mode while inviting guest:** establece el modo de invitado como **Expert** o **Field**.

Referencia relacionada

[Política del cliente, mejores prácticas \(en la página 124\)](#)

[Permisos de cliente, mejores prácticas \(en la página 136\)](#)

9.10.3. Precedencia de políticas

A los usuarios que pertenezcan a varios grupos se les aplicarán los ajustes de la configuración, dándole precedencia a la configuración **priorizada** de **Client Policy**. Por ejemplo, si Bob pertenece a dos grupos: **Ventas** y **Soporte**. El grupo de ventas tiene el modo **Encryption** configurado en **Off**, pero el grupo de Soporte tiene el modo **Encryption** configurado en **Auto**. Por lo tanto, cuando Bob inicie sesión, su configuración se establecerá en **Encryption Auto**. Para que Bob reciba una configuración de política del cliente

establecida como **Encryption Off**, podría ser **eliminado del grupo de Soporte**, o la configuración **Encryption** podría establecerse como **Override** en la configuración **Client Policy** del usuario de Bob.

Por lo general, todos los usuarios del dominio de cuenta OnSight pertenecen al grupo **All Users**. En el ejemplo anterior, establezca el modo de cifrado como **On** en la política de **All Users**. Cuando Bob inicie sesión, su configuración puede estar en **Encryption On**, ya que tiene una mayor prioridad que la configuración del Cifrado, ya sea en el **Grupo de ventas** o en el **Grupo de soporte**. Dado que no se puede eliminar a Bob del grupo **All Users**, la única forma de darle una configuración de cifrado de menor prioridad podría ser seleccionando **Override** en la configuración **Client Policy** del usuario de Bob.

Referencia relacionada

[Política del cliente y precedencia de prioridad \(en la página 113\)](#)

[Política del cliente, mejores prácticas \(en la página 124\)](#)

[Permisos de cliente, mejores prácticas \(en la página 136\)](#)

9.10.3.1. Configurar la política del cliente

Inicie sesión en OPM y haga clic en **SETTINGS** en el menú principal y seleccione la pestaña **CLIENT POLICY**.

1. Seleccione un **Grupo** en la sección **CLIENT POLICY** de la izquierda para aplicar una política.

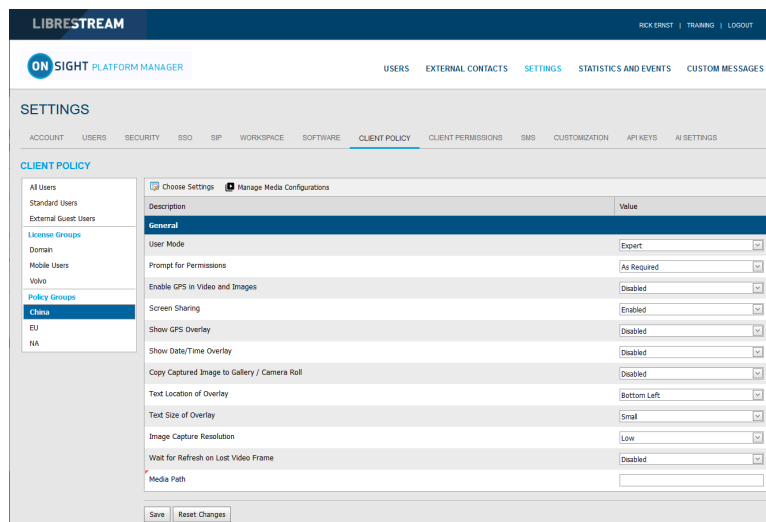


Figura 9-34 Política del cliente de grupo

2. Hacer clic en el icono  **Choose Settings**. Se presentará la ventana **Choose Settings**.

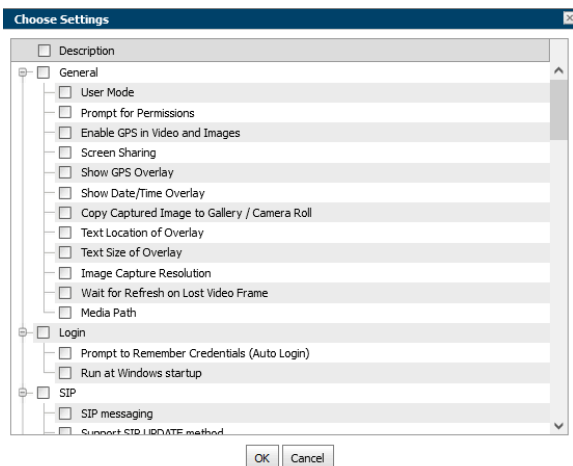


Figura 9-35 Elegir configuración

3. En cada categoría, seleccione cada configuración que le gustaría administrar o haga clic en el título **Sección de la categoría** para habilitar todo. Haga clic en **OK**.
4. Haga clic en **Save**.

5. Establezca el valor apropiado para cada configuración.

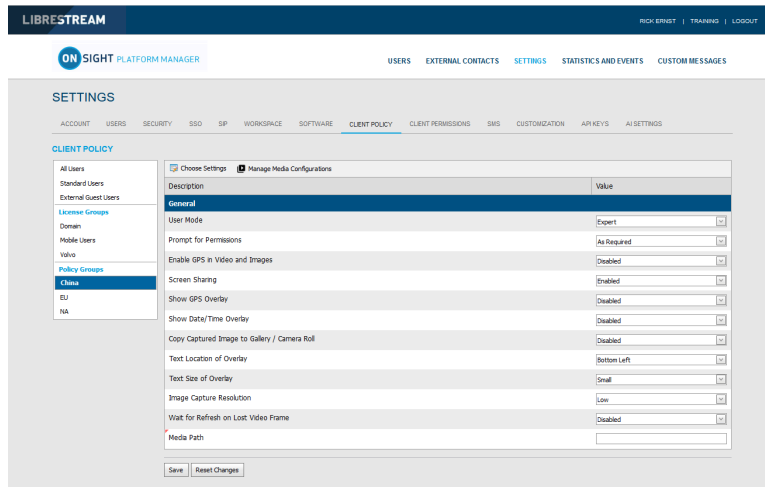


Figura 9-36 Configuración de valores

6. Repita el proceso para cada grupo al que desee aplicar una **Client Policy**.



Nota: Las políticas del cliente se pueden aplicar a usuarios invitados externos, lo que le permite administrar la configuración de privacidad.

Esto completa el procedimiento.

Referencia relacionada

[Política del cliente, mejores prácticas \(en la página 124\)](#)

[Permisos de cliente, mejores prácticas \(en la página 136\)](#)

9.10.3.2. Configurar los permisos de cliente

Inicie sesión en OPM y haga clic en **SETTINGS** en el menú principal y seleccione la pestaña **CLIENT PERMISSIONS**.

1. Seleccione el **Group** que desea administrar.

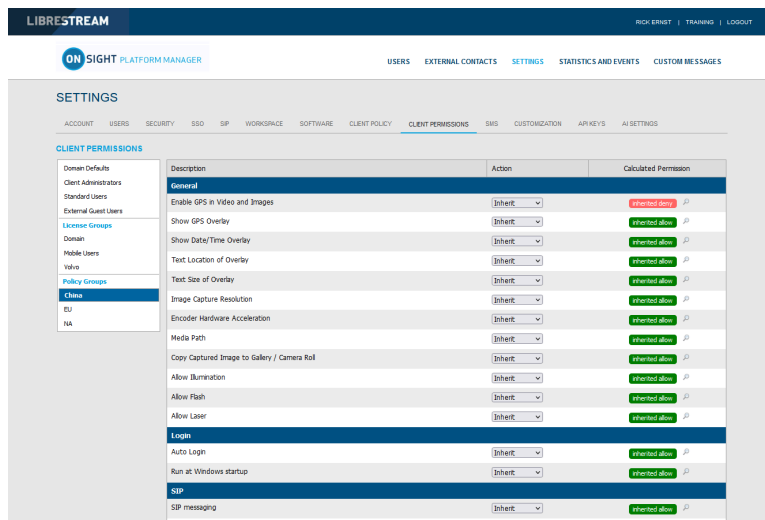


Figura 9-37 Configurar los permisos de grupo

2. Para cada configuración en **Description**, aplique la acción que desea para el permiso.

- **Allow:** permite a los usuarios editar la configuración.
- **Deny:** deshabilita la capacidad de edición y no permite que los usuarios editen la configuración.
- **Inherit** (disponible solo si el grupo es un grupo secundario de un grupo principal).

- Haga clic en **Save**.
Esto completa el procedimiento.

Consulte la sección **Client Policy** y **Permissions** para obtener detalles.

Referencia relacionada

[Política del cliente, mejores prácticas \(en la página 124\)](#)
[Permisos de cliente, mejores prácticas \(en la página 136\)](#)

Información relacionada

[Política y permisos del cliente \(en la página 78\)](#)

9.10.4. Política y permisos del cliente de grupo

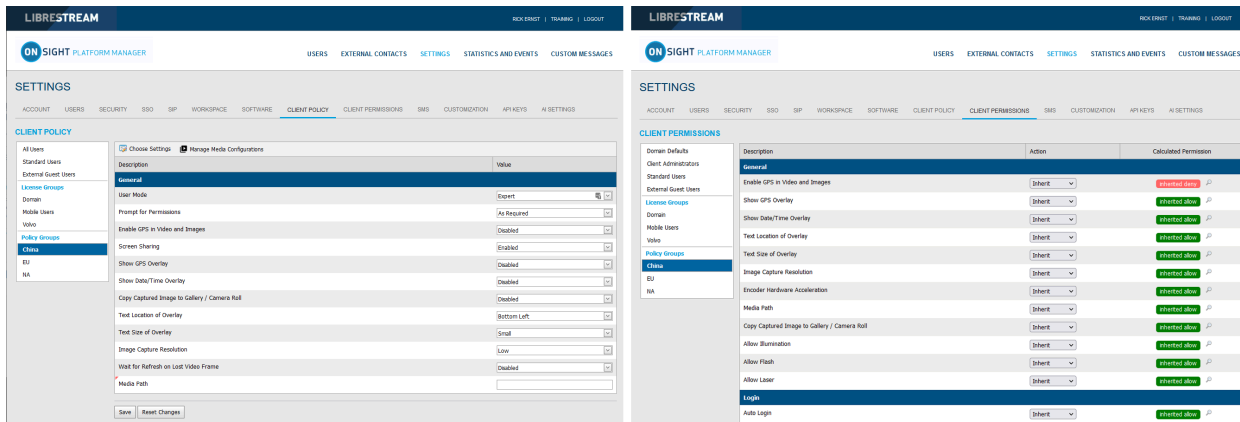


Figura 9-38 Política y permisos del cliente de grupo

La política del cliente de grupo se administra en la página **USERS** mediante la edición de grupos. Cuando se crea una política del cliente de grupo, esta se aplica a los miembros del grupo cada vez que inician sesión en un endpoint de OnSight Connect. Ya sea que los usuarios inicien sesión a través de una **PC con Windows, iOS, Teléfono inteligente Android** o de una **Cámara inteligente de OnSight**, se aplicará su **Client Policy** asignada.

La Plantilla de configuración predeterminada de OnSight Platform Manager describe cada ajuste disponible y proporciona pautas de mejores prácticas. Está disponible en la sección OPM, bajo **Manuals and Guides** en [OnSight Support website](#).

Client Permissions de grupo determina la autorización para que el usuario acceda a ajustes en un endpoint de OnSight. Para cada ajuste, puede seleccionar **Allow**, **Deny** o **Inherit** para establecer el acceso al permiso para el ajuste. Cuando un usuario inicia sesión en el software de OnSight Connect, **Allow** le permitirá editar el ajuste, **Deny** impedirá el acceso e **Inherit** le dará el permiso con base en el tutor del grupo de **Client Permissions** actual. Todos los grupos de **Client Permissions** heredarán del grupo tutor Valores predeterminados de dominio. Consulte la sección Precedencia de políticas [RE Insert XREF] para obtener información.

Referencia relacionada

[Política del cliente, mejores prácticas \(en la página 124\)](#)
[Permisos de cliente, mejores prácticas \(en la página 136\)](#)

Información relacionada

[Política y permisos del cliente \(en la página 78\)](#)

9.10.5. Privacidad de video remoto

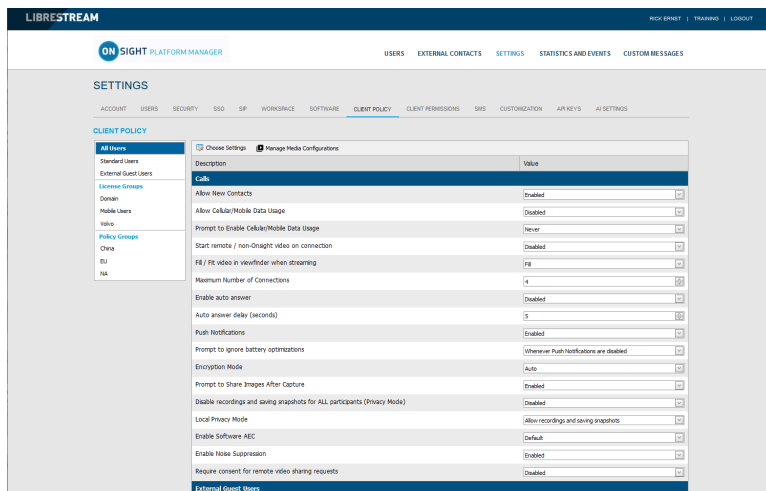


Figura 9-39 Configuración de privacidad

Las configuraciones de privacidad de OnSight requieren el consentimiento para solicitudes remotas de uso compartido de video durante una llamada de OnSight. Al habilitarla, da a los clientes un mayor control sobre el uso compartido de video y los usuarios deben dar su consentimiento antes de que un participante remoto pueda ver el video desde su cámara.

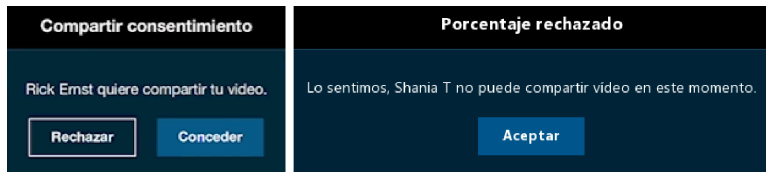


Figura 9-40 Requerir el consentimiento

La privacidad de los videos se mejora en ubicaciones sensibles al requerir que los usuarios den su consentimiento antes de compartir videos. Afecta la privacidad de video remoto:

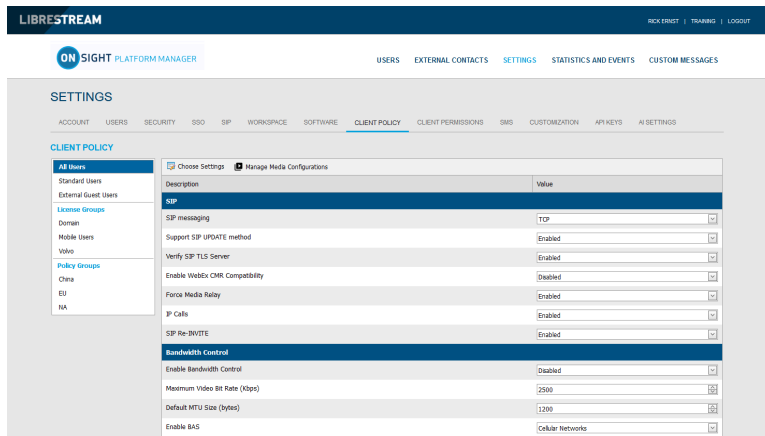
- **Client Policy > Calls:** requieren el consentimiento para solicitudes remotas de uso compartido de videos. Las opciones incluyen:
 - **Enabled:** obliga al usuario a conceder el permiso para transmitir contenido desde su cámara.
 - **Disabled** (de forma predeterminada): automáticamente concede el permiso para transmitir contenido desde su cámara.
- **Client Permissions > Calls:** requieren el consentimiento para solicitudes remotas de uso compartido de videos. Las opciones incluyen:
 - **Allow:** concede el permiso para compartir la cámara.
 - **Decline** (de forma predeterminada): niega el acceso a la cámara con el mensaje: "Lo sentimos, no puede compartir video en este momento".

Referencia relacionada

[Política del cliente, mejores prácticas \(en la página 124\)](#)

[Permisos de cliente, mejores prácticas \(en la página 136\)](#)

9.10.6. Compatibilidad con CMR de WebEx



The screenshot shows the 'CLIENT POLICY' settings page. On the left, there is a sidebar with categories like 'All Users', 'Standard Users', 'External Guest Users', 'License Groups', 'Domain', 'Mobile Users', 'Voice', 'Policy Groups', 'China', 'EU', and 'NA'. The main area displays a table of settings. The 'SIP' section is expanded, showing various SIP-related settings. The 'Enable WebEx CMR Compatibility' setting is highlighted in blue, and its value is 'Disabled'. Other settings in the SIP section include 'SIP messaging' (TZP), 'Support SIP UPDATE method' (Enabled), 'Verify SIP TLS Server' (Enabled), 'Force Media Relay' (Enabled), and 'SIP Re-INVITE' (Enabled). Below the SIP section is the 'Bandwidth Control' section, which includes 'Enable Bandwidth Control' (Disabled), 'Maximum Video Bit Rate (Kbps)' (2500), 'Default MTU Size (bytes)' (1200), and 'Enable BAS' (Cellular Networks).

Figura 9-41 Política del cliente

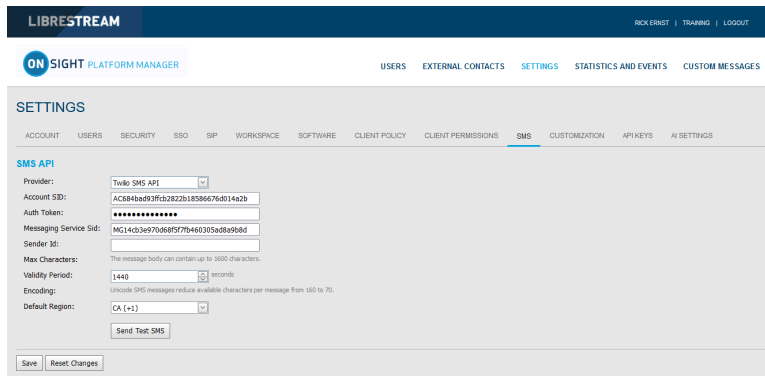
Acceda a **Client Policy** y busque la sección **SIP** para habilitar **WebEx CMR Compatibility**. **WebEx CMR Compatibility** permite que los endpoints de Onsight llamen a las salas de reuniones de WebEx y actúen como un endpoint de transmisión de audio/video. Las salas de reuniones de WebEx no aceptarán llamadas de Onsight, a menos que esta función esté habilitada.

Referencia relacionada

[Política del cliente, mejores prácticas \(en la página 124\)](#)

[Permisos de cliente, mejores prácticas \(en la página 136\)](#)

9.11. Servicio de mensaje de texto




The screenshot shows the 'SMS' settings page. The 'SMS API' section is active, displaying various configuration fields. The 'Provider' is set to 'Twilio SMS API'. The 'Account SID' is 'AC384ba93f02822b18386676d014a2b'. The 'Auth Token' is masked with asterisks. The 'Messaging Service Sid' is 'MG1403a97066577b460305a08a9080'. The 'Sender ID' is empty. The 'Max Characters' is set to 160. The 'Validity Period' is 1440 seconds. The 'Encoding' is set to 'Unicode'. The 'Default Region' is 'CA (+1)'. There is a 'Send Test SMS' button and 'Save' and 'Reset Changes' buttons at the bottom.

Figura 9-42 Configuración SMS

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **SMS**. La página **SMS** incluye la sección **SMS API** para configurar el servicio de mensajes. Esto se incluye como parte de las suscripciones de la plataforma Enterprise y Pro.

Los SMS permiten a los usuarios enviar invitaciones de participantes externos a través del servicio de mensajes de SMS para clientes de telefonía móvil.

 **Nota:** Librestream configura la página de configuración de SMS para el cliente, no se deben realizar cambios en esta configuración. Comuníquese con el soporte de Librestream para obtener ayuda si tiene algún problema con las invitaciones de participantes por SMS.

Información relacionada

[CONTACTO DE SOPORTE \(en la página 111\)](#)

9.12. Personalización

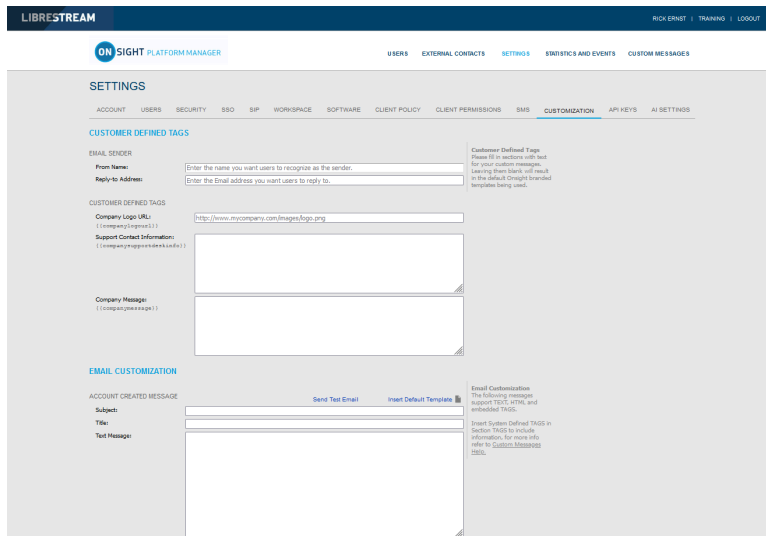


Figura 9-43 Personalización

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **CUSTOMIZATION**. La página **CUSTOMIZATION** incluye las siguientes secciones: **CUSTOMER DEFINED TAGS**, **EMAIL CUSTOMIZATION** y **SMS CUSTOMIZATION**.

La personalización le permite personalizar mensajes de correo electrónico y SMS que los usuarios de OnSight Connect reciben del dominio OnSight de su empresa.

Los mensajes se envían para los siguientes eventos:

- **Account Created**
- **Account Deleted**
- **Account Registered**
- **External Guest Invitation**
- **External Guest Confirmation**
- **SSO Enabled Instructions**
- **Password Reset Request**
- **Password Changed Confirmation**

CUSTOMER DEFINED TAGS se usan para acceder a información específica de la empresa y del usuario para la colocación en los mensajes. Para obtener más información, consulte **Custom Messages Help** en la página **CUSTOMIZATION**.

Para ver los mensajes predeterminados, haga clic en **Insert Default Template** que se encuentra al lado del cuadro de texto del mensaje. Puede editar la plantilla del mensaje predeterminado o crear sus propios mensajes. Presione **Save** para conservar sus cambios.

9.13. Claves de interfaz de programación de aplicaciones

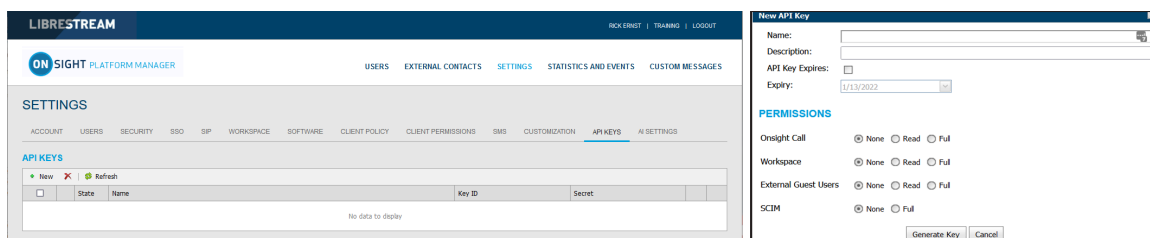



Figura 9-44 Página de claves de API

Haga clic en **SETTINGS** en el menú principal y haga clic en la pestaña **APIKEYS**. La página **API KEYS** le permite administrar el acceso a las API REST de Llamada en Onsight y de Workspace.

Haga clic en el icono  **New** para generar una nueva clave de autorización de API. Proporcione la siguiente información para cada clave:

1. **Name**.
2. **Description**.
3. **API Key Expires** seguida de una **Expiry Date**.
4. Establezca los permisos para **Onsight Call**, **Workspace**, **External Guest Users**, etc., como:
 - **None**: sin acceso.
 - **Read**: solo lectura.
 - **Full**: acceso de lectura/escritura.
5. Haga clic en **Generate Key**.

9.13.1. Clave generada por API

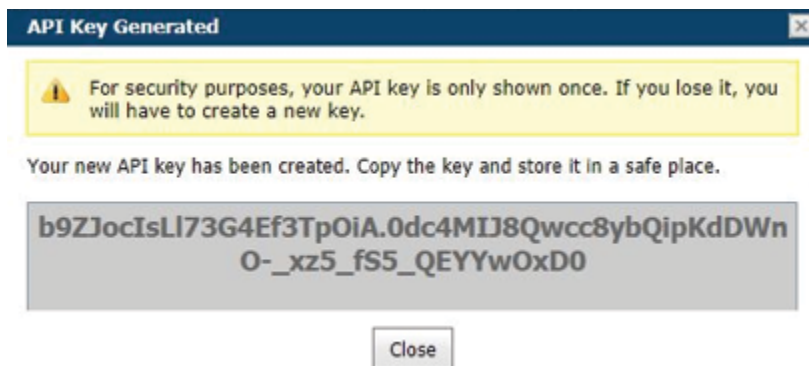


Figura 9-45 Clave generada por API

Una vez que se genere la clave, se mostrará la ventana API Key Generated. Esta indicará:

Por motivos de seguridad, su clave de API solo se muestra una vez. Si la pierde, deberá crear una clave nueva.

Cuando haya creado su clave nueva de API, cópiela y guárdela en un lugar seguro. Usted necesitará esta clave para acceder a los endpoints de API REST.

Luego de su creación, la clave no puede visualizarse de nuevo, pero puede editar sus propiedades asociadas, como **Name**, **Description**, **Expiry** o **Permissions**. Haga clic en el botón **Edit** para cambiar las propiedades de la clave de API.

Puede bloquear la clave desde el acceso a los endpoints de API REST al presionar el botón **Lock**. Desbloquee la clave para restablecer el acceso a los servicios.

Consulte las Guías de API de Onsight para obtener información sobre el uso de la clave de API REST.

9.14. Configuración de inteligencia artificial

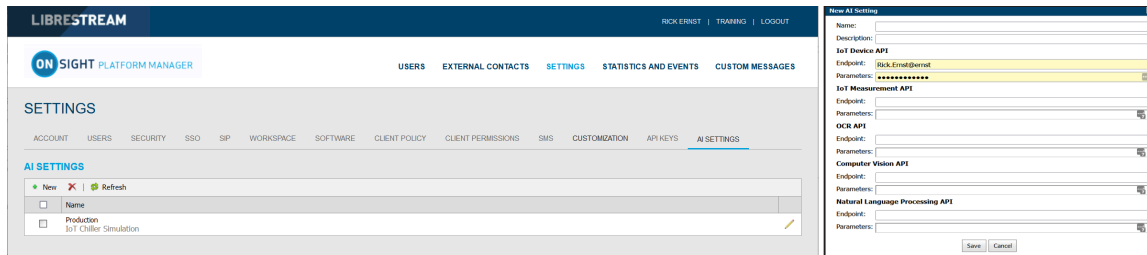



Figura 9-46 Nueva configuración de IA

Use la página de Configuración de inteligencia artificial (IA) para configurar sus endpoints y parámetros de API de inteligencia artificial. La configuración de IA se puede agregar a **Client Policy** para permitirles a los clientes el acceso a los servicios de IA, incluyendo **Computer Vision (CV)**, **Optical Character Recognition (OCR)**, **Internet of Things (IoT)** y **Natural Language Processing (NLP)**.

Presione el icono  **New** para crear una nueva configuración de IA. Introduzca la siguiente información:

1. **Name.**
2. **Description.**
3. **IoT Device API:**
 - a. **Endpoint:** introduzca la URL.
 - b. **Parameters:** introduzca las credenciales.
4. **IoT Measurement API:**
 - a. **Endpoint:** introduzca la URL.
 - b. **Parameters:** introduzca las credenciales.
5. **API de OCR**
 - a. **Endpoint:** introduzca la URL.
 - b. **Parameters:** introduzca las credenciales.
6. **API de visión de la computadora**
 - a. **Endpoint:** introduzca la URL.
 - b. **Parameters:** introduzca las credenciales.
7. **API de procesamiento natural del idioma**
 - a. **Endpoint:** introduzca la URL.
 - b. **Parameters:** introduzca las credenciales.
8. **Transcription API**
 - a. **Endpoint:** introduzca la URL.
 - b. **Parameters:** introduzca las credenciales.

Una vez creados los perfiles de configuración de IA, están disponibles para selección en la política del cliente en la lista desplegable **Artificial Intelligence > AI Settings Profiles**. Debe agregar **AI settings** a la política antes de configurarla. Haga clic  **Choose Settings** en la página **Client Policy**.

Un usuario debe pertenecer a un grupo que incluya un **AI Setting Profile** para acceder a los servicios de IA.

Puede elegir combinar o separar cada servicio de IA en un perfil de configuración de IA personalizado. Por ejemplo, los servicios de IoT se pueden configurar mediante un perfil de configuración de AI que solo describa los endpoints y parámetros API del dispositivo IoT. Sin embargo, solo un perfil de configuración de AI puede aplicarse a una política del cliente, por lo que todos los servicios de AI deben combinarse en un **único perfil de configuración de IA** si desea que los miembros de un grupo accedan a más de un servicio de IA.

10. ESTADÍSTICAS Y EVENTOS

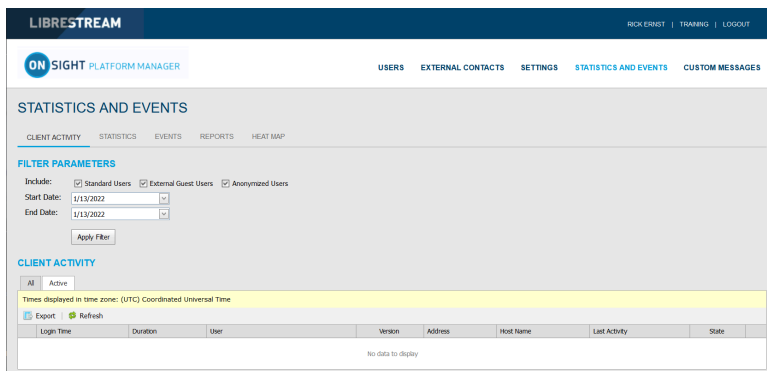


Figura 10-1 Estadísticas y eventos

Haga clic en **STATISTICS AND EVENTS** en el menú principal para configurar las opciones que le permitan generar informes de la actividad del cliente y eventos para su organización. **STATISTICS AND EVENTS** le permite acceder a las siguientes secciones: **CLIENT ACTIVITY**, **STATISTICS**, **EVENTS**, **REPORTS** y **HEAT MAP**. La actividad del cliente y los eventos se pueden ver en la página **STATISTICS AND EVENTS**.

PARÁMETROS DEL FILTRO

En términos generales, modifique los **FILTER PARAMETERS** usando la casilla de verificación para filtrar su información, seguido de los menús desplegables para definir sus parámetros específicos y haga clic en **Apply Filter** para generar un informe

10.1. Actividad del cliente

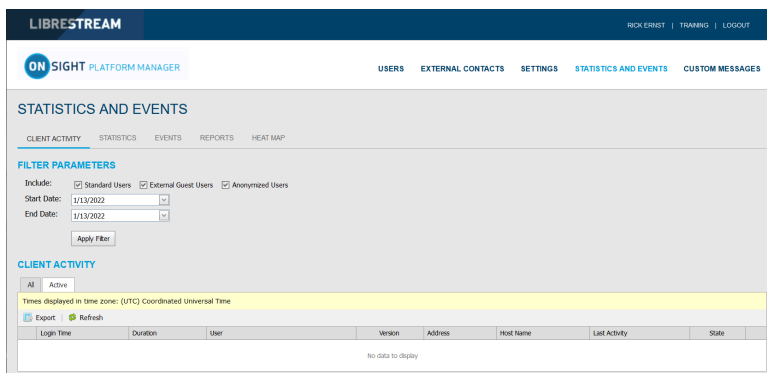


Figura 10-2 Actividad del cliente

Haga clic en **STATISTICS AND EVENTS** en el menú principal para acceder a su página **CLIENT ACTIVITY**. La página **CLIENT ACTIVITY** contiene **FILTER PARAMETERS** y una sección de **CLIENT ACTIVITY**.

Actividad del cliente

La sección Actividad del cliente muestra todos los resultados dentro de una tabla y hace un seguimiento de la actividad del usuario para el servicio de Onsite Connect. El administrador puede visualizar estos resultados usando las pestañas. Seleccione entre:

- **All**: muestra toda la actividad
- **Active**: muestra quiénes están conectados.

10.1.1. Generar run informe de actividad del cliente

Inicie sesión en OPM y seleccione **STATISTICS AND EVENTS** en el menú principal y seleccione la pestaña **CLIENT ACTIVITY**.

Para generar un informe de actividad del cliente, deberá modificar **FILTER PARAMETERS**.

1. Determine qué usuarios incluir al activar una o más casillas de verificación para:

- **Standard Users**
- **External Guest Users**
- **Anonymized Users**

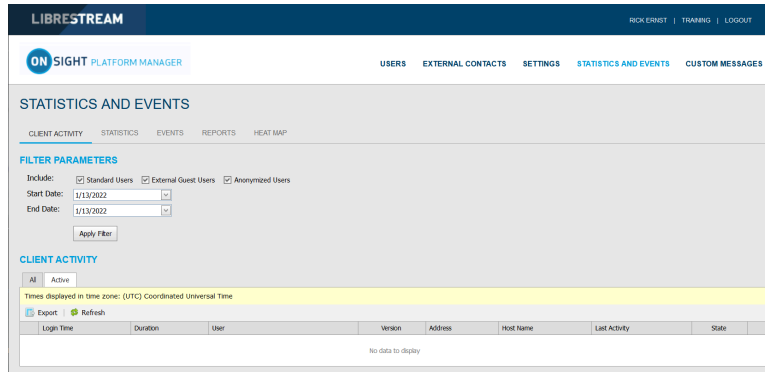


Figura 10-3 Filtrar usuarios

2. Establezca sus parámetros de **fecha**. Haga clic en el menú desplegable y seleccione una:

- a. **Start Date** utilizando la ventana emergente **Calendar**.
- b. **End Date** utilizando la ventana emergente **Calendario**.

3. Haga clic en **Apply Filter** para mostrar los resultados en la pestaña **CLIENT ACTIVITY ALL**.

4. **CLIENT ACTIVITY** muestra:

- a. **Login Time**
- b. **Duration**
- c. **User**
- d. **Version** del software de endpoint
- e. **IP Address**
- f. **Host Name**
- g. **Last Activity**
- h. **State**

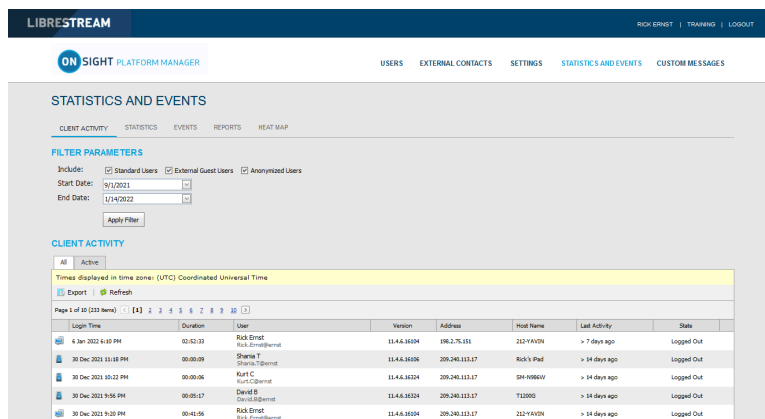


Figura 10-4 Resultados de la actividad del cliente

5. Al hacer clic en **Refresh** se actualiza la lista.

- Hacer clic en **Export** permite que guarde un archivo separado por comas (CSV) del informe. Esto completa el procedimiento.

10.2. Estadísticas

The screenshot shows the Librestream 'STATISTICS AND EVENTS' page. The 'CALLS' section is active, displaying a table of call records. A 'Call Details' window is open on the right, showing information for a specific call on 16 Jul 2021 at 1:18:12 PM. The call details include start and end times, duration, encryption status, and participant information.

Start Time	Duration	Calling Participant	Called Participant	Called User
16 Jul 2021 1:18:12 PM	00:52:13	Rick Ernst Rick.Ernst@ernst.sp.sys.librestream.com	Tobey Sadeky Tobey.Sadeky@ernst.sp.sys.librestream.com	Tobey Bernst
26 Jul 2021 1:28:32 PM	00:00:07	Rick Ernst Rick.Ernst@ernst.sp.sys.librestream.com	Rick Field	
26 Jul 2021 3:07:57 PM	00:01:56	Rick Ernst Rick.Ernst@ernst.sp.sys.librestream.com	Rick Field	
26 Jul 2021 3:10:28 PM	00:00:39	Rick Field	Rick Ernst Rick.Ernst@ernst.sp.sys.librestream.com	Rick.Ernst@ernst
26 Jul 2021 3:14:18 PM	00:00:06	Rick Field	Rick Ernst Rick.Ernst@ernst.sp.sys.librestream.com	Rick.Ernst@ernst
26 Jul 2021 3:25:57 PM	00:03:28	Rick Ernst Rick.Ernst@ernst.sp.sys.librestream.com	Rick Field	
4 Aug 2021 12:30:44 PM	01:22:02	Rick Ernst Rick.Ernst@ernst.sp.sys.librestream.com	Rick Field	

Figura 10-5 Informe de estadísticas

Haga clic en **STATISTICS AND EVENTS** en el menú principal y haga selección de la pestaña **STATISTICS**. La página **STATISTICS** contiene la sección **FILTER PARAMETERS** y la sección **CALLS**.

La página **STATISTICS** le permite generar informes para las estadísticas relacionadas con las llamadas. Las estadísticas relacionadas con las llamadas están disponibles para los usuarios con licencia de **Connect Enterprise**.



Nota: Haga clic en el icono **Call Details** (lupa) para mostrar la información adicional.

10.2.1. Generar run informe estadístico

Inicie sesión en OPM y seleccione **STATISTICS AND EVENTS** en el menú principal y seleccione la pestaña **STATISTICS**.

Para generar un informe estadístico, deberá modificar sus **FILTER PARAMETERS**.

- Determine qué usuarios incluir al activar una o más casillas de verificación para:
 - Standard Users**
 - External Guest Users**
 - Anonymized Users**

The screenshot shows the Librestream 'STATISTICS AND EVENTS' page with the 'FILTER PARAMETERS' section expanded. The 'Include' section has three checkboxes: 'Standard Users' (checked), 'External Guest Users' (unchecked), and 'Anonymized Users' (unchecked). The 'Start Date' and 'End Date' are set to 1/14/2022.

Figura 10-6 Filtrar usuarios

- Establezca sus parámetros de fecha. Haga clic en el menú desplegable y seleccione una:
 - Start Date** utilizando la ventana emergente Calendario.
 - End Date** utilizando la ventana emergente Calendario.

3. Haga clic en **Apply Filter** para mostrar los resultados en la sección **CALLS**.

4. **CALLS** muestra los siguientes campos:

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

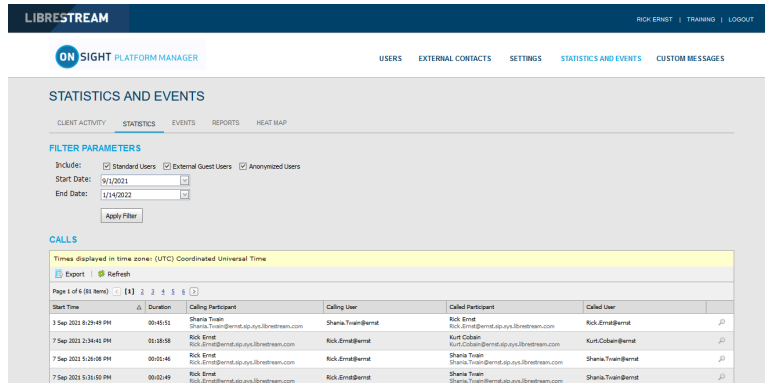


Figura 10-7 Resultados del informe estadístico

5. Al hacer clic en **Refresh** se actualiza la lista.

6. Hacer clic en **Export** permite que guarde un archivo separado por comas (CSV) del informe.

Mostrar detalles de llamada

7. Para ver los detalles de un usuario, haga clic en el icono **Call Details** (lupa).

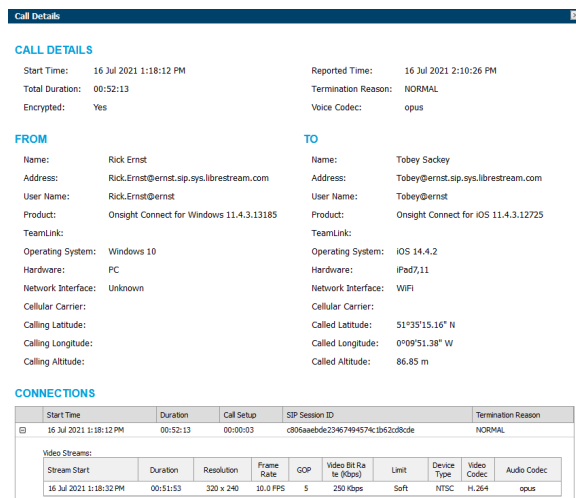


Figura 10-8 Detalles estadísticos de llamada

8. La página **Call Details** muestra:

- a. **CALL DETAILS:**
 - i. **Start Time**
 - ii. **Total Duration**

- iii. **Encrypted**
- iv. **Reported Time**
- v. **Termination Reason**
- vi. **Voice Codec**

9. **FROM:**

- a. **Name**
- b. **Address** (SIP)
- c. **User Name**
- d. **Product** (Cliente)
- e. **TeamLink**
- f. **Operating System**
- g. **Hardware**
- h. **Network Interface**
- i. **Cellular Carrier**
- j. **Calling Latitude**
- k. **Calling Longitude**
- l. **Calling Altitude**

10. **TO:**

- a. **Name**
- b. **Address**
- c. **User Name**
- d. **Product** (Cliente)
- e. **TeamLink**
- f. **Operating System**
- g. **Hardware**
- h. **Network Interface**
- i. **Cellular Carrier**
- j. **Called Latitude**
- k. **Called Longitude**
- l. **Called Altitude**

11. **CONNECTIONS:**

- a. **Start Time**
 - i. **Duration**
 - ii. **Call Setup**

iii. SIP Session ID

iv. Termination Reason

b. Stream Start

c. Duration

d. Resolution

e. Frame

f. DNT

g. Video Bit Rate

h. Limit

i. Device Type

j. Video Codec

k. Audio Codec

12. Salga de la página cuando termine de verla.
Esto completa el procedimiento.

10.3. Eventos

The screenshot shows the 'STATISTICS AND EVENTS' page in the Librestream SIGHT Platform Manager. The 'FILTER PARAMETERS' section is active, showing filters for severity (Information, Warning, Error, Fatal) and include (Standard Users, External Guest Users, API Users). The 'EVENT LOG' section displays a table of events with columns for Time, User, API Key, Description, and Details. The table shows several events, including user logins and group policy updates.

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

Figura 10-9 Eventos

Haga clic en **STATISTICS AND EVENTS** en el menú principal y seleccione la pestaña **EVENTS**. Esta página contiene **FILTER PARAMETERS** y una sección de **EVENT LOG**.

La página **EVENTS** hace un seguimiento de la actividad del administrador y del usuario en OPM, así como de los mensajes de eventos basados en servidor. Establezca los **FILTER PARAMETERS** y haga clic en **Apply Filter** para visualizar los resultados en la sección **EVENT LOG**.

10.3.1. Generar un informe de eventos

Inicie sesión en OPM y seleccione **STATISTICS AND EVENTS** en el menú principal y seleccione la pestaña **EVENTS**.

Para generar un informe de **Eventos**, deberá modificar sus **FILTER PARAMETERS**.

1. Defina las opciones de **Severity** activando las casillas de verificación de:

- **Information**
- **Warning**
- **Error**
- **Fatal**

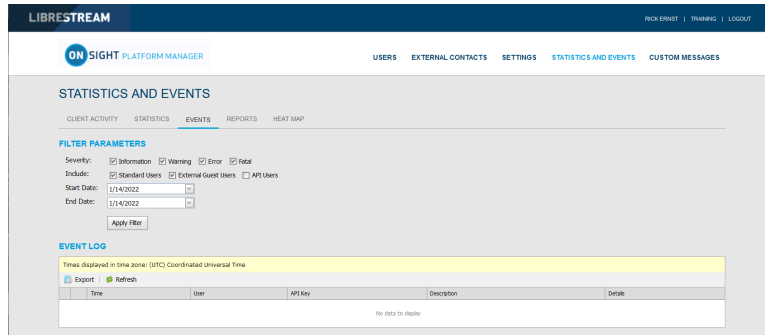


Figura 10-10 Filtrar por severidad y usuarios

2. Determine qué usuarios incluir al activar una o más casillas de verificación para:

- **Standard Users**
- **External Guest Users**
- **API Users**

3. Establezca sus parámetros de **fecha**. Haga clic en el menú desplegable y seleccione una:

- a. **Start Date** utilizando la ventana emergente Calendario.
- b. **End Date** utilizando la ventana emergente Calendario.

4. Haga clic en **Apply Filter** para mostrar los resultados en la sección **EVENT LOG**.

5. El registro de evento muestra:

- a. **Time**
- b. **User**
- c. **API Key**
- d. **Description**
- e. **Details**

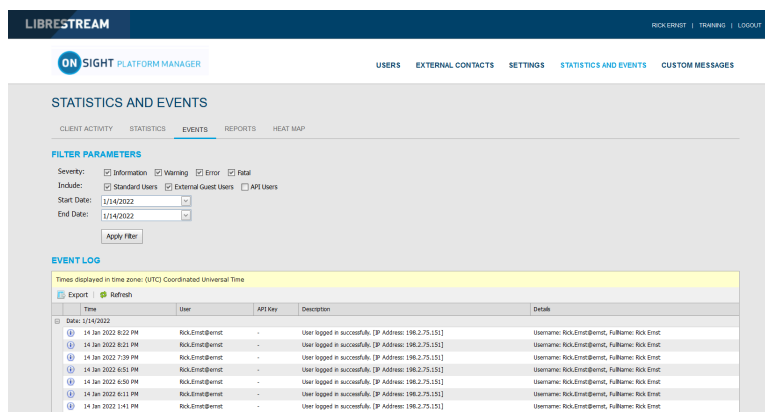


Figura 10-11 Resultados del informe estadístico

6. Al hacer clic en **Refresh** se actualiza la lista.

7. Hacer clic en **Export** permite que guarde un archivo de Valor separado por comas (CSV) del informe. Esto completa el procedimiento.

10.4. Informes

The screenshot displays the 'LIBRESTREAM SIGHT PLATFORM MANAGER' interface. The main navigation bar includes 'USERS', 'EXTERNAL CONTACTS', 'SETTINGS', 'STATISTICS AND EVENTS', and 'CUSTOM MESSAGES'. The 'STATISTICS AND EVENTS' section is active, with sub-tabs for 'CLIENT ACTIVITY', 'STATISTICS', 'EVENTS', 'REPORTS', and 'HEAT MAP'. The 'REPORT PARAMETERS' section contains several dropdown menus and a 'Run Report' button. The 'RESULTS' section shows a table titled 'TOP USAGE (CALLS)' with the following data:

Name	# of Calls	Duration (mins)
Eric Ernst eric.ernst@ernst	92	74:07:28
Sharna T sharna.t@ernst	42	46:13:48
Kurt C kurt.c@ernst	19	13:22:23


Figura 10-12 Informes

Haga clic en **STATISTICS AND EVENTS** en el menú principal y seleccione la pestaña **REPORTS**. La página **REPORTS** contiene la sección **FILTER PARAMETERS**. Cuando se genera un informe, se muestra la sección **RESULTS** con los datos del informe.


Los informes le permiten generar estadísticas de uso, como quién se conectó al software, cuántas llamadas realizó y recibió una persona y la duración total y promedio de las llamadas para ayudar a determinar el grado de adopción de la tecnología. Algunos de los beneficios de la revisión periódica del uso máximo y mínimo son:

- Identificación de los mejores usuarios como líderes potenciales.
- Identificación de los candidatos para tutorías/capacitación.
- Lo que subraya el apoyo y el interés de la dirección por la nueva tecnología.

Los informes de resumen de licencia y uso general muestran la cantidad de licencias utilizadas o la cantidad de llamadas realizadas durante un período.

 **Nota:** Si la anonimización de datos está activada para su dominio, cualquier dato que supere el período de retención de datos (DRP) se anonimizará. Los registros de llamadas anonimizados pueden ser:

- Utilizados para proporcionar tendencias históricas.
- Incluidos en los recuentos de informes de llamadas.
- Atribuirse a los grupos del usuario, país, campos personalizados y otros filtros.
- Incluirse en un archivo CSV exportado.
- Visibles en la tabla de actividad del cliente.
- Filtrados usando campos personalizados.

 **Nota:** El historial de llamadas se almacena localmente en los clientes y no se anonimiza. Pueden ser eliminados cuando se desinstala la aplicación. Los datos de los usuarios previamente eliminados pueden ser anonimizados, si se solicita.

10.4.1. Generar un informe

Inicie sesión en OPM y seleccione **STATISTICS AND EVENTS** en el menú principal y seleccione la pestaña **REPORTS**.

Para generar un informe, deberá modificar los **FILTER PARAMETERS**.

1. Seleccione el nombre del informe a ejecutar dentro del menú desplegable **Report Name**. Seleccione entre:
 - a. **Top Usage** (Llamadas)
 - b. **Least Usage** (Llamadas)
 - c. **Top Usage** (Inicios de sesión)
 - d. **Least Usage** (Inicios de sesión)
 - e. **Top Usage** (Ancho de banda)
 - f. **Least Usage** (Ancho de banda)
 - g. **License Usage Summary**: proporciona una lista del número de licencias que se utilizan durante el período.
 - h. **Guest Invite Summary**: proporciona una lista del número de invitaciones de participantes que se envían durante el período, incluyendo el remitente, el participante, el estado de la invitación, etc.
 - i. **Overall Usage Summary**: proporciona una lista del número de llamadas y la duración total del período.

The screenshot shows the 'STATISTICS AND EVENTS' section of the Librestream SIGHT Platform Manager. The 'REPORTS' tab is active. The 'REPORT PARAMETERS' form is displayed with the following fields and values:

- Report Name: Top Usage (Calls)
- Start Date: 1/14/2022
- End Date: 1/14/2022
- User Account Type: Optional (default to All User Account Type)
- Groups: Optional (default to All User)
- Country: Optional (default to All Country)
- Custom Fields: Add Custom Fields For Filtering
- Call Duration: any
- Number of Results: 10
- Include anonymous records
- Run Report button

Figura 10-13 Parámetros del informe

2. Defina **Start Date** y **End Date** del informe haciendo clic en los menús desplegables para acceder a la ventana emergente **Calendar**.
3. Defina el tipo de usuario en el menú desplegable **User Account Type**. Seleccione entre:
 - **Standard Users**
 - **External Guest Users**
 - **All Users**
4. (Opcional) Haga clic para habilitar las casillas de verificación para que los **Groups** se incluyan en el informe. La opción predeterminada es **All Users**.
5. (Opcional) Haga clic para habilitar las casillas de verificación de **Country** que va a filtrar. La opción predeterminada es **All Countries**.
6. (Opcional) Seleccione **Custom Fields** para filtrar (opcional; la opción predeterminada incluye todos los campos personalizados).
7. Establezca **Call Duration** utilizando el menú desplegable. Seleccione entre:
 - a. **any**
 - b. **greater o equal**

c. **less o equal**

d. **between**

- Establezca el **Number of Results** utilizando el menú desplegable para incluirlo en el informe. Seleccione **10, 25, 50 100**, etc.
- Habilite la opción de la casilla de verificación **Include anonymous records**, según sea necesario.
- (Opcional) Haga clic en **Run Report** para mostrar los resultados.

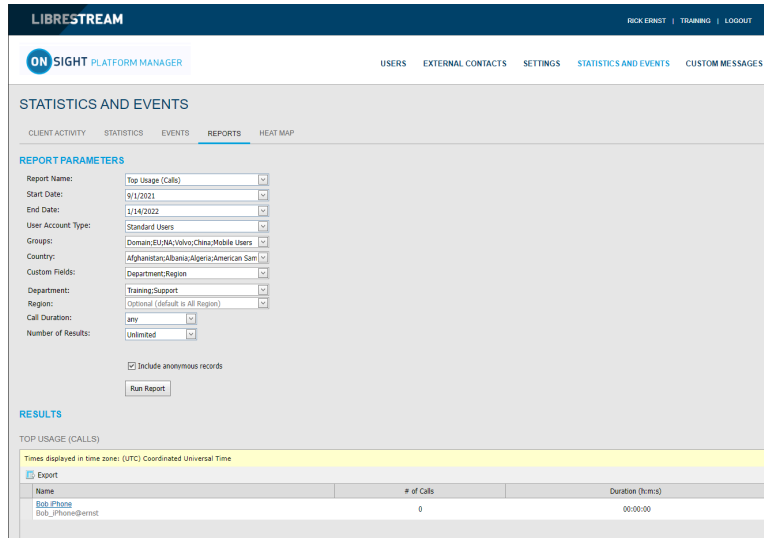


Figura 10-14 Resultados del informe

- (Opcional) Haga clic en **Export** para guardar, descargar y ver los resultados como un archivo de valores separados por comas (CSV). Esto completa el procedimiento.

10.5. Mapas térmicos

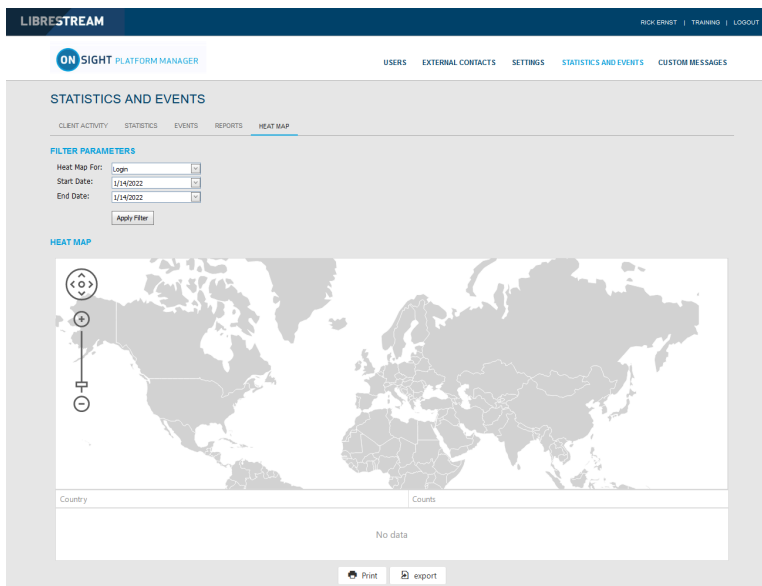



Figura 10-15 Página de mapa térmico

Haga clic en **STATISTICS AND EVENTS** en el menú principal para acceder a la página **HEAT MAP**. La página **HEAT MAP** contiene una sección **FILTER PARAMETERS** y una sección **HEAT MAP**.

Los mapas térmicos presentan las cantidades de llamadas o de inicios de sesión que se filtran por ubicación de la dirección IP y por cantidad. Las llamadas se pueden filtrar para mostrar **Caller**, **Callee**, o **Both** en el mapa.

 **Nota:** El mapa térmico representa un recuento de conexiones del cliente con base en una dirección IP aparente. Puede haber alguna variación debido al enrutamiento a torres de telefonía móvil o a la entrada de firewall al Internet público.

10.5.1. Generar un informe del mapa térmico

Inicie sesión en OPM y seleccione **STATISTICS AND EVENTS** en el menú principal y seleccione la pestaña **HEAT MAP**.

Para generar un informe del mapa térmico deberá modificar sus **FILTER PARAMETERS**.

1. Use el menú desplegable **Heat Map For** para elegir la fuente de información a partir de la cual se genera el informe. Seleccione entre:

- **Llamada**
- **Iniciar sesión**

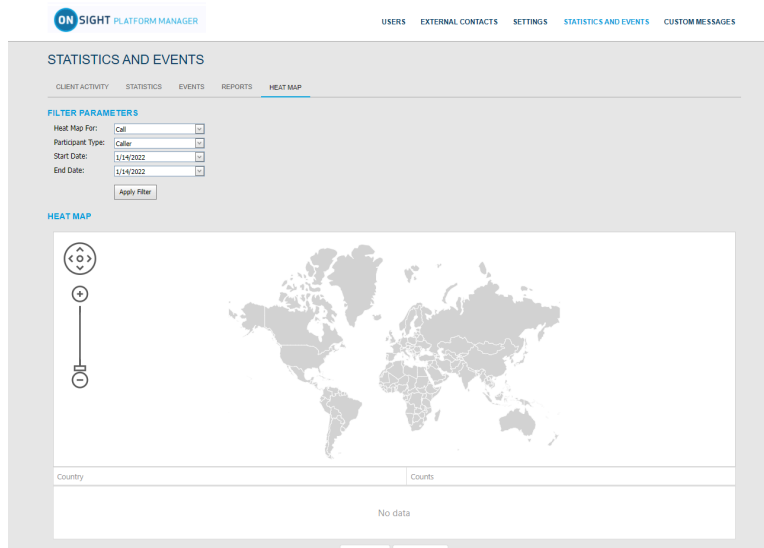


Figura 10-16 Parámetros del filtro del mapa térmico

2. **Call Option Only** (Solo opción Call): permite seleccionar también **Participant Type** como:

- **Persona que llama**
- **Destinatario de llamada**
- **Ambos**

3. Defina **Start Date** y **End Date** del informe haciendo clic en los menús desplegables para acceder a la ventana emergente de calendario.

4. Haga clic en **Apply Filter** para ejecutar el informe.

Se mostrará el mapa térmico indicando la ubicación y la cantidad de llamadas/inicios de sesión.

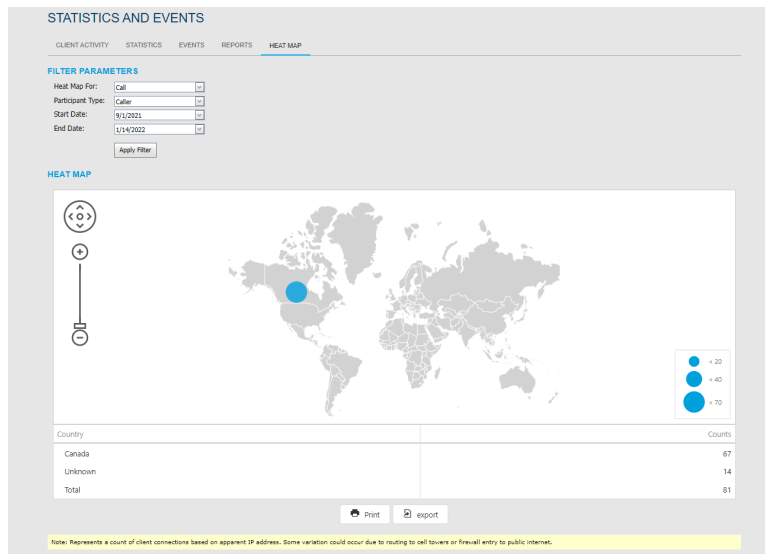


Figura 10-17 Resultados del informe del mapa térmico

5. (Opcional) Haga clic en **Print** para imprimir una copia PDF del mapa.
6. (Opcional) Haga clic en **Export** para guardar, descargar y ver los resultados como un archivo de valores separados por comas (CSV).
 Esto completa el procedimiento.

11. SOPORTE DE IDIOMA

Onsight Connect admite los siguientes idiomas para **Windows, Teléfonos inteligentes y Tabletas**:

- Inglés
- Francés
- Chino (Simplificado)
- Japonés
- Alemán
- Italiano
- Portugués (Portugal y Brasil)
- Español
- Sueco
- Ruso
- Coreano

OPM mostrará las páginas solicitadas por Onsight Connect en función del idioma del sistema del cliente. La configuración no es obligatoria ni su dominio Onsight.

Actualmente, Onsight Platform Manager está disponible en inglés únicamente, pero muestra páginas localizadas en el navegador del cliente para lo siguiente:

1. Invite Guest

- **Onsight Connect for Windows** descargar
- **Register for an Account**
- **Forgot Password**
- **Reset Password**
- **SSO** iniciar sesión

2. Los correos electrónicos procedentes de OPM están localizados e incluyen:

- Cuenta registrada (HTML, texto)
- Confirmación de usuario invitado (texto)
- Invitación de usuario participante (HTML, texto, SMS)
- Solicitud de restablecimiento de contraseña (texto, SMS)
- Cambió la contraseña del usuario (texto, SMS)

12. MENSAJES PERSONALIZADOS

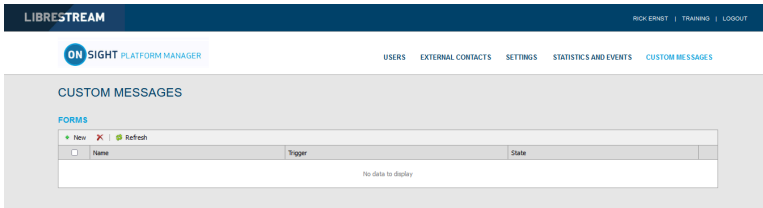



Figura 12-1 Mensajes personalizados

Los **Custom Messages** se pueden mostrar dentro de la aplicación OnSight Connect al iniciar sesión o antes de empezar una grabación. Los **Custom Messages** deben ser reconocidos por un usuario antes de terminar el inicio de sesión o de empezar una grabación. Si el usuario no acepta el mensaje, entonces la acción no se permitirá. Los usuarios deben presionar **OK** para continuar o el usuario volverá a la ventana de inicio de sesión y la grabación no empezará.

i Consejo: Por lo general, los mensajes personalizados se utilizan para mostrar las condiciones de uso para usar OnSight Connect dentro de su empresa.

12.1. Crear un mensaje personalizado (formulario)

Inicie sesión en OPM y haga clic en **CUSTOM MESSAGES** en el menú principal para administrar los formularios de mensajes personalizados.

1. Presione el icono  **New** para crear un nuevo mensaje personalizado.

New Form

Name
Enter form name

Available for use

Title
Enter form title

Message
Enter message

Trigger
 Login
 Recording

Button Styles
 Ok/Cancel

Message Options
 Allow "Don't show again" option

OK Cancel

Figura 12-2 Formulario nuevo

2. Introduzca los siguientes parámetros:
 - a. **Name:** este campo solo es visible dentro de OPM.
 - b. Habilite la casilla de verificación **Available for Use** si desea que el formulario esté disponible para su uso en **Client Policy**.
 - c. **Title:** este campo se muestra en la aplicación.
 - d. **Message:** este es el mensaje que verán los usuarios. Tiene un límite de 500 caracteres.
 - e. **Trigger:** seleccione el evento que activará la visualización del mensaje, **Login** o **Recordings**.

- f. **Button Styles:** seleccione el estilo de los botones de respuesta que desea mostrar. **OK/Cancel** actualmente es la única opción.
- g. **Message Options:** establezca si desea que el usuario pueda seleccionar la opción **Don't show again**. Si desea que se le pregunte a un usuario cada vez que inicie sesión o realice una grabación, deshabilite esta opción.
- h. Haga clic en **OK** para guardar su mensaje personalizado. Haga clic en **Cancel** si no desea guardar sus cambios.



Esto completa el procedimiento.

12.2. Mensajes personalizados y política del cliente

Los mensajes personalizados se pueden agregar a **Client Policy** para visualizarlos dentro de Onsite Connect. Puede visualizar uno o más mensajes personalizados dentro de la aplicación, es decir que ambos mensajes **Login** y **Recording** se pueden utilizar en la misma política del cliente.

12.2.1. Modificación de la política del cliente para admitir mensajes personalizados

Iniciar sesión en OPM.

1. Haga clic en **USERS** en el menú principal y seleccione un grupo.
2. Presione el icono  **New Group**.
3. Seleccione la pestaña **CLIENT POLICY**.
4. Seleccione  **Choose Settings**.
 - a. Seleccione **Login** si desea mostrar el mensaje de inicio de sesión.
 - b. Seleccione **Recording** si desea mostrar el mensaje de grabación.
5. Haga clic en **OK** para volver a la sección **Client Policy**.
6. Desplácese hacia abajo en la página hasta la sección **Custom Messages**.
 - a. Seleccione el mensaje **Login** que desea mostrar.
 - b. Seleccione el mensaje **Recording** que desea mostrar.

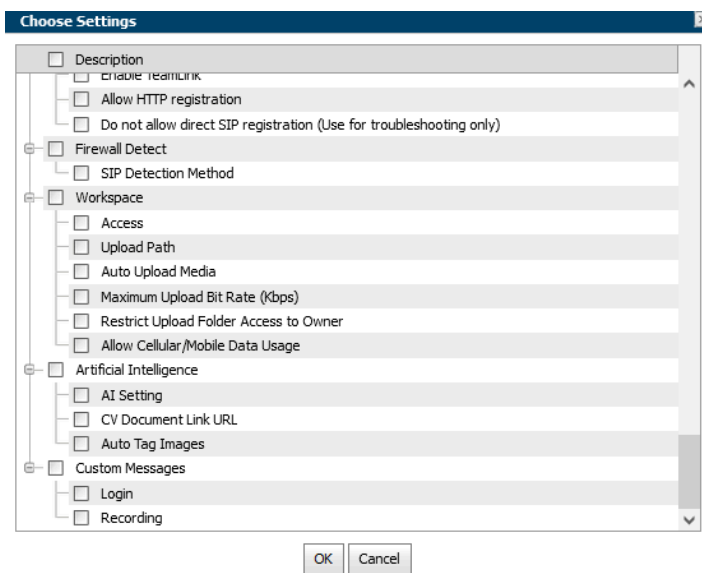


Figura 12-3 Elegir configuración

7. Presione **Save** para conservar sus cambios.
Esto completa el procedimiento.

13. ACUERDO DE LICENCIA DE USUARIO FINAL

Este software tiene licencia de conformidad con los términos de un Acuerdo de licencia de usuario final (EULA), cuya última versión se puede encontrar en:

<https://librestream.com/support-archives/termsfuse/>

14. CONTACTO DE SOPORTE



Figura 14-1 Comuníquese con el código QR de soporte

Para consultas de soporte:

- **Correo electrónico:** <mailto:support@librestream.com>
- **Página web:** <https://librestream.com/contact-us-support/>
- **Teléfono:** 1.800.849.5507 o +1.204.487.0612

APPENDICES

Política del cliente y precedencia de prioridad

Elementos de la política del cliente	Prioridad (alta a baja)
General	
User Mode (Modo de usuario)	<ol style="list-style-type: none"> 1. Field (Campo) 2. Expert (Experto)
Prompt for Permissions (Solicitud de permisos)	<ol style="list-style-type: none"> 1. On Login (Al Iniciar sesión) 2. As Required (Según sea necesario)
Enable GPS Location in Video and Images (Habilitar la ubicación GPS en videos e imágenes)	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Show GPS Overlay (Mostrar superposición de GPS)	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Show Date/Time Overlay (Mostrar superposición de fecha y hora)	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Copy Captured Image to Gallery / Camera Roll (Copie la imagen capturada en la galería y carrete de la cámara)	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Text Location of Overlay (Ubicación del texto de la superposición)	<ol style="list-style-type: none"> 1. Bottom Left (Parte inferior izquierda) 2. Bottom Right (Parte inferior derecha) 3. Top Left (Parte superior izquierda) 4. Top Right (Parte superior derecha)
Text Size of Overlay (Tamaño del texto de la superposición)	<ol style="list-style-type: none"> 1. Large (Grande) 2. Medium (Mediano) 3. Small (Pequeño)
Image Capture Resolution (Resolución de captura de imagen)	<ol style="list-style-type: none"> 1. Max (Máxima) 2. High (Alta) 3. Medium (Mediano) 4. Low (Baja)
Media Path (Ruta de medios)	Undefined: esta configuración acepta el valor del último grupo de la lista.
Login (Iniciar sesión)	
Prompt to Remember Credentials (Auto Login) [Solicitud para recordar las credenciales (inicio de sesión automático)]	<ol style="list-style-type: none"> 1. Disabled (Deshabilitada) 2. Enabled (Habilitada)
Run at Windows startup (Ejecutar al inicio de Windows)	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
SIP	

Elementos de la política del cliente	Prioridad (alta a baja)
SIP messaging (Mensajes de SIP)	<ol style="list-style-type: none"> 1. UDP 2. TCP
Support SIP UPDATE method (Admite el método de ACTUALIZACIÓN de SIP)	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Verify SIP TLS Server (Verificar el servidor de TLS de SIP)	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Enable WebEx CMR Compatibility (Habilitar compatibilidad con CMR de WebEx)	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Force Media Relay (Forzar relé de medios)	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Media Configurations (Configuraciones de medios)	
Custom Media Configurations (Configuraciones de medios personalizadas)	Lista combinada de todos los grupos
Bandwidth Control (Control de ancho de banda)	
Enable Bandwidth Control (Habilitar el control del ancho de banda)	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Maximum Video Bit Rate (Kbps) [Tasa máxima de bits de video (Kbps)]	<ol style="list-style-type: none"> 1. Lower Value (Valor más bajo) 2. Higher Value (Valor más alto)
Enable BAS (Habilitar BAS)	<ol style="list-style-type: none"> 1. On (Activado) 2. Cellular Networks (Redes celulares) 3. Off (Desactivada)
Media Configuration on Connection (Configuración de medios en la conexión)	Undefined: esta configuración acepta el valor del último grupo de la lista.
Pause Video While Transferring Image (Pausar el video mientras transfiere la imagen)	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Preferred Voice Codec (Códec de voz preferido)	<ol style="list-style-type: none"> 1. Low Bandwidth (Ancho de banda bajo) (GSM) 2. Default (Predeterminado) (G.711)
Preferred Subject Audio Codec (Códec de audio de sujeto preferido)	<ol style="list-style-type: none"> 1. Deshabilitada 2. Low Bandwidth (Ancho de banda bajo) (GSM) 3. Default (Predeterminado) (G.711)
Audio Efficiency (Eficiencia de audio)	<ol style="list-style-type: none"> 1. Lower bandwidth (Ancho de banda más bajo) 2. Mid (Medio) 3. Lower latency (Latencia más baja)
Calls (Llamadas)	
Allow Cellular/Mobile Data Usage (Permitir el uso de datos celulares/móviles)	<ol style="list-style-type: none"> 1. FALSE 2. TRUE

Elementos de la política del cliente	Prioridad (alta a baja)
Prompt to Enable Cellular/Mobile Data Usage (Solicitud para habilitar el uso de datos móviles/celulares)	<ol style="list-style-type: none"> 1. On Every Login (En cada inicio de sesión) 2. On First Login (Al iniciar sesión por primera vez) 3. Never (Nunca)
Start remote/non-Onsight video on connection (Iniciar video remoto/no Onsight en la conexión)	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Fill/Fit video in viewfinder when streaming (Rellenar/ajustar video en el visor al transmitir)	<ol style="list-style-type: none"> 1. Fill (Rellenar) 2. Fit (Ajustar) 3. Actual Size (Tamaño real)
Maximum Number of Connections (Cantidad máxima de conexiones)	<ol style="list-style-type: none"> 1. Lower Value (Valor más bajo) 2. Higher Value (Valor más alto)
Enable auto answer (Habilitar respuesta automática)	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Auto answer delay (seconds) [Retardo de respuesta automática (segundos)]	<ol style="list-style-type: none"> 1. Lower Value (Valor más bajo) 2. Higher Value (Valor más alto)
Push Notifications (Notificaciones push)	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Prompt to ignore battery optimizations (Solicitud para ignorar las optimizaciones de la batería)	<ol style="list-style-type: none"> 1. Solo cuando el usuario desactiva las notificaciones push 2. Siempre que las notificaciones push estén deshabilitadas
Encryption Mode (Modo de cifrado)	<ol style="list-style-type: none"> 1. On (Activado) 2. Auto (Automático) 3. Off (Desactivada)
Prompt to Share Images After Capture (Solicitud para compartir imágenes después de la captura)	<ol style="list-style-type: none"> 1. FALSE 2. TRUE
Disable recordings and saving snapshots for ALL participants (Privacy Mode) [Desactivar las grabaciones y guardar instantáneas para TODOS los participantes (modo de Privacidad)]	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Local Privacy Mode (Modo de privacidad local)	<ol style="list-style-type: none"> 1. Desactivar las grabaciones y guardar instantáneas 2. Desactivar las grabaciones 3. Desactivar guardar instantáneas 4. Permitir grabaciones y guardar instantáneas
Networking (Redes)	
Diffserv DSCP (Voice) (Voz)	<ol style="list-style-type: none"> 1. Voice (Voz) 2. Audio/Video/Garantizado 3. Carga controlada 4. Mejor esfuerzo

Elementos de la política del cliente	Prioridad (alta a baja)
Diffserv DSCP (Video)	<ol style="list-style-type: none"> 1. Voice (Voz) 2. Audio/Video/Garantizado 3. Carga controlada 4. Mejor esfuerzo
Diffserv DSCP (Subject Audio) (audio de sujeto)	<ol style="list-style-type: none"> 1. Voice (Voz) 2. Audio/Video/Garantizado 3. Carga controlada 4. Mejor esfuerzo
Diffserv DSCP (Data Stream) (flujo de datos)	<ol style="list-style-type: none"> 1. Audio de voz 2. Video 3. Mejor esfuerzo de carga controlada garantizada
TeamLink	
Enable (Habilitar) TeamLink	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Allow HTTP registration (Permitir registro HTTP)	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Do not allow direct SIP registration (User for troubleshooting only) [No permitir el registro directo del SIP (usuario solo para la resolución de problemas)]	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Firewall Detect (Detección de firewall)	
SIP Detection Method (Método de detección de SIP)	<ol style="list-style-type: none"> 1. Servidor SIP, completo 2. Servidor SIP, básico 3. TeamLink
Workspace	
Access (Acceso)	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Upload Path (Ruta de carga)	Undefined: esta configuración acepta el valor del último grupo de la lista.
Auto Upload Media (Carga automática de medios)	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Maximum Upload Bit Rate (Kbps) [Velocidad máxima de bits de carga (Kbps)]	<ol style="list-style-type: none"> 1. Lower Value (Valor más bajo) 2. Higher Value (Valor más alto)
Restrict Upload Folder Access to Owner (Restringir el acceso a la carpeta de carga al propietario)	<ol style="list-style-type: none"> 1. TRUE 2. FALSE
Allow Cellular/Mobile Data Usage (Permitir el uso de datos celulares/móviles)	<ol style="list-style-type: none"> 1. TRUE 2. FALSE

Elementos de la política del cliente	Prioridad (alta a baja)
Custom Messages (Mensajes personalizados)	
Login (Iniciar sesión)	Undefined: esta configuración acepta el valor del último grupo de la lista.
Recording (Grabación)	Undefined: esta configuración acepta el valor del último grupo de la lista.

Información relacionada

[Política y permisos del cliente \(en la página 78\)](#)

[Precedencia de políticas \(en la página 80\)](#)

Best Practices

15.2.1. Cuenta, mejores prácticas

Tabla 15-2 Cuenta, mejores prácticas


Configuración		Descripción	Mejores prácticas/ consejos
ACCOUNT INFORMATION (INFORMACIÓN DE LA CUENTA)			
Company Name (Nombre de la empresa):		Ingrese el nombre de la empresa	
Customer Domain (Dominio del cliente):		Ingrese el dominio de la empresa	
Account Owner (Propietario de cuenta):			
Customer Created (Creación del cliente):		Fecha y hora de creación del cliente	
Customer Expires (Expiración del cliente):		Fecha en que expira el uso de la cuenta	
Super Administrator Access (Acceso de superadministrador):		Capacidad de eliminar el acceso a la cuenta de las operaciones internas de Librestream.  Nota: Permitir el acceso cuando el soporte de Librestream necesite revisar su configuración de OPM	
ACTIVATION (ACTIVACIÓN): se muestra solo en las instalaciones locales.			
Status (Estado):		Indica el estado actual de la licencia.	
Type (Tipo):		Indica el tipo de instalación.	
Expires (Expiración):		Muestra la fecha de expiración de la licencia.	
LICENSES (LICENCIAS)		Las licencias activas en el dominio.	
LICENSES > Onsight Users (LICENCIAS > Usuarios de ONSIGHT)			
Connect Enterprise		Número de las licencias de usuario de dominio	
Workspace Enterprise		Número de las licencias de usuario de Workspace	
Workspace Contributor		Número de las licencias de usuario de Workspace Contributor	
User Expiry (Expiración del usuario)		Soporte para las fechas de expiración de la cuenta de usuario.	
External Guest Users (Usuarios invitados externos)		Habilita los usuarios invitados externos	
Advanced External Guest Expiry (Expiración anticipada de invitados externos)			
License Group (Grupo de licencias)		Permite asignar grupos de licencias, cada grupo administra su propio grupo de licencias.	

Tabla 15-2 Cuenta, mejores prácticas

Configuración		Descripción	Mejores prácticas/ consejos
LICENSES > Client Functionality (Funcionalidad del cliente)			
User Mode (Expert/Field) [Modo de Usuario (Experto/Campo)]		Permite los modos Experto y Campo para los usuarios.	
TeamLink		Cuando está habilitado, Onsight Platform Manager determinará si el firewall permite el registro directo del SIP o si debe utilizar HTTPS para mensajes de SIP proxy a través de los servidores TeamLink.	
Multiparty Calling (Llamadas multiusuario)		Permite el alojamiento de conferencias en PC con Windows.	
Bandwidth Control (Control de ancho de banda)		Permite el control del ancho de banda para la política del cliente.	
Content Privacy (Privacidad de contenido)		Permite controlar la privacidad de las grabaciones e imágenes.	
Onsight 5000HD Updates (Actualizaciones de Onsight 5000HD)		Permite la actualización del software 5000HD.	
Onsight Collaboration Hub Updates (Actualizaciones del Hub de Onsight Collaboration)		Permite las actualizaciones del software Onsight Collaboration Hub.	
Cube Updates (Actualizaciones de Cube)		Permite actualizar el software de Onsight Cube.	
LICENSES > Hosted Features (Funciones alojadas)			
Call Statistics (Estadísticas de llamadas)		Permite la recopilación de datos de las estadísticas de llamadas.	
Advanced Reporting (Generación de informes avanzados)		Permite la generación de informes avanzados de las estadísticas de llamadas.	
Customization (Personalización)		Permite la personalización de los mensajes.	
SMS		Permite las invitaciones de invitados externos por SMS.	
Client Permissions (Permisos del cliente)		Permite el control de los permisos del cliente.	
Custom Media Configurations (Configuraciones de medios personalizadas)		Permite la configuración de medios personalizados para la política del cliente.	
SSO		Permite el soporte de SSO.	
Custom Email (SMTP) [Correo electrónico personalizado (SMTP)]		Permite el envío de correos electrónicos desde el servidor de correos del cliente.	
Custom Messages (Mensajes personalizados)		Permite el uso de los mensajes personalizados.	
LICENSES > Common Actions (Acciones comunes)			
Change Account Owner (Cambiar Propietario de cuenta)		Permite asignar un Propietario de cuenta a partir de una lista de usuarios actuales.	

Tabla 15-2 Cuenta, mejores prácticas

Configuración		Descripción	Mejores prácticas/ consejos
Disable Super Admin Access (Desactivar el acceso del superadministrador)		Esto deshabilita la capacidad de Librestream para acceder al dominio con fines de soporte. El acceso lo puede conceder su administrador de OPM si es necesario.	

Información relacionada

[Cuenta \(en la página 52\)](#)

15.2.2. Usuarios, mejores prácticas

Tabla 15-3 Usuarios, mejores prácticas

CUENTAS DE USUARIO	Valor	Predeterminada	Descripción	Mejores prácticas/consejos
Default Time Zone (Zona horaria predeterminada):	(UTC) Hora coordinada		Establezca la zona horaria predeterminada para su región.	Si opera en varias regiones, establezca la zona horaria en la que reside el administrador.
Default Language (Idioma predeterminado):	Alemán, chino, coreano, español, inglés, italiano, japonés, portugués, portugués (Brasil), ruso y sueco	Inglés		
EXTERNAL GUEST USERS (USUARIOS INVITADOS EXTERNOS)				
External Guest Settings moved to Client Policy (La configuración de invitados externos se trasladó a la política del cliente)	Trasladado a la Política del cliente [ENLACE]			
GLOBAL DIRECTORY (DIRECTORIO GLOBAL)				
Global Directory Availability (Disponibilidad de directorio global)	<input checked="" type="checkbox"/> External Contacts are public by default (Los contactos externos son públicos de forma predeterminada) (los contactos externos que no pertenezcan a ninguna lista de contactos estarán disponibles para todos en el directorio global)	habilitada predeterminada	Si está marcada, todos los contactos que no estén en una lista definida se podrán ver en el directorio global; si no está marcada, sólo los contactos que pertenezcan a una lista de contactos se podrán ver en el directorio global.	Esto permite que tenga contactos que no se pueden ver para todos, pero que el administrador puede agregar manualmente a las listas de contactos de los usuarios. Deje esta opción sin marcar si quiere que los contactos que no están en una lista no aparezcan en el directorio global.

Tabla 15-3 Usuarios, mejores prácticas

CUENTAS DE USUARIO	Valor	Predeterminada	Descripción	Mejores prácticas/consejos
CUSTOM FIELDS (CAMPOS PERSONALIZADOS)		Opcional		Los campos personalizados se incluyen en un informe de usuario exportado.
Custom Field Name (Nombre del campo personalizado)		Departamento, Región	Ingrese un nombre	Puede crear campos personalizados que se pueden utilizar como filtros de los informes.
Custom Field Value (Valor del campo personalizado)		Nula	Ingrese un valor o una lista de valores	Cree un valor o una lista de valores que puedan utilizarse en los informes.

Información relacionada

[Usuarios \(en la página 57\)](#)

15.2.3. Seguridad, mejores prácticas

Tabla 15-4 Seguridad, mejores prácticas

Configuración	Valor	Descripción	Mejores prácticas/consejos
PASSWORD POLICY (POLÍTICA DE CONTRASEÑA)			
Minimum Length (Longitud mínima):	8	Establezca la longitud mínima de las contraseñas permitidas.	Siga la política de seguridad de su empresa.
Minimum Capital Letters (Letras en mayúscula mínimas):	1	Establezca el número obligatorio mínimo de letras en mayúscula.	
Minimum Non-Alpha Characters (Caracteres mínimos que no sean letras):	1	Establezca el número obligatorio mínimo de caracteres que no sean letras.	
PASSWORD EXPIRATION (EXPIRACIÓN DE LA CONTRASEÑA)			
Password Expiration (Expiración de la contraseña):	<input type="checkbox"/> Enable password expiration (Habilitar expiración de la contraseña)	deshabilitada predeterminada	Siga la política de seguridad de su empresa.
Password Expires (Expiración de la contraseña):	60 días		
Warn Users Before Expiration (Advertir a los usuarios antes de la expiración):	3 días		

Tabla 15-4 Seguridad, mejores prácticas

Configuración	Valor	Descripción	Mejores prácticas/consejos
LOGIN POLICY (POLÍTICA DE INICIO DE SESIÓN)			
Máximo de intentos incorrectos para iniciar sesión:	3	predeterminada 3	Siga la política de seguridad de su empresa.
Account Lockout Duration (Duración del bloqueo de la cuenta):	5 minutos	predeterminada 5 minutos	
SELF REGISTRATION (AUTORREGISTRO)	deshabilitada predeterminada	La configuración del autorregistro se aplica a las cuentas creadas mediante la página de autorregistro y a las cuentas aprovisionadas automáticamente a través del inicio de sesión único	
Enable Self Registration (Habilitar el autorregistro)	habilitada predeterminada <input checked="" type="checkbox"/> Enable self registration page (Habilitar la página de autorregistro)	Habilitar la página de autorregistro	El autorregistro puede facilitar la preparación de las sesiones de formación y el despliegue, ya que no es necesario tener una lista de todos los usuarios por adelantado. Por lo general, solo hay que enviar por correo electrónico las instrucciones de autoinscripción.
URL:	https://onsight.librestream.com/OamDev/AccountServices/Register.aspx?id=librestream.com	id=domain, identifica el dominio del cliente en el que el usuario se está autorregistrando. En el ejemplo proporcionado el dominio = librestream.com	Distribuya la URL a los asociados que tendrán que registrarse para obtener una cuenta de Onsite.
Key (Clave):	xxxxxxxxxxxxxxxx: deshabilitada predeterminada	Cuando se rellena con un valor, el usuario debe introducir esta clave para autorregistrarse en una cuenta de Onsite.	Establezca una clave para garantizar que los usuarios están autorizados para solicitar una cuenta. Utilice Generate Random Key para introducir un valor.
Licenses (Licencias):	<input type="checkbox"/> predeterminada deshabilitada	Si el autorregistro está habilitado, puede especificar el tipo de licencia	
Account Activation Method (Método de activación de la cuenta):	habilitada predeterminada <input checked="" type="checkbox"/> Administrator must approve accounts registered using the Self Registration key (El administrador debe aprobar las cuentas registradas con la clave de autorregistro)	Cuando está habilitada, todas las solicitudes de cuenta deben ser aprobadas por un administrador antes de ser asignadas.	Se recomienda habilitar esta opción, sin embargo, si un número significativo de usuarios se autorregistran y no quiere aprobar cada solicitud de cuenta, déjela sin marcar. Se recomienda utilizar Self Registration Key y establecer Allowed Email domains como precaución adicional.
Notification: (Notificación)	habilitada predeterminada <input checked="" type="checkbox"/> Notify Administrators by email when an account is registered (Notificar a los administradores por correo electrónico cuando se registra una cuenta)	Los administradores de OPM recibirán correos electrónicos cada vez que un usuario se registre.	

Tabla 15-4 Seguridad, mejores prácticas

Configuración	Valor	Descripción	Mejores prácticas/consejos
Email (Correo electrónico)	habilitada predeterminada <input checked="" type="checkbox"/> Require Email Address for Self Registered Accounts (Requerir dirección de correo electrónico para las cuentas autorregistradas)	Las direcciones de correo electrónico son obligatorias para las notificaciones de los usuarios.	<p>Requerir las direcciones de correo electrónico debe estar habilitada para que se reciban las notificaciones de los usuarios.</p> <p>Es obligatorio si quiere que la función Forgot Password esté disponible para todos los usuarios. Normalmente, el único caso en el que no se requieren contraseñas para las cuentas de los usuarios es cuando su política de seguridad no permite que las direcciones de correo electrónico se almacenen fuera del sitio.</p>
Allowed Email Domains (Dominios de correo electrónico permitidos):	company.com	La lista de dominios de correo electrónico permitidos desde los que un usuario puede registrarse.	Establezca esto en el dominio de su empresa y en el de cualquier otro socio de terceros para restringir el acceso.

Información relacionada
[Seguridad \(en la página 59\)](#)

15.2.4. Software, mejores prácticas

Tabla 15-5 Software, mejores prácticas

ACTUALIZACIONES DE SOFTWARE	Predeterminada	Descripción	Mejores prácticas/consejos
Onsight Connect for Windows (Onsight Connect para Windows)	Latest Published Version (Última versión publicada)	Establezca la versión de software que desea que instalen los usuarios de PC con Windows y los usuarios invitados externos.	Puede elegir "La más reciente..." o una versión específica. La instalación estándar se aplicará si los usuarios no tienen derechos de administrador.
Onsight 5000HD	Latest Published Version (Última versión publicada)	Establezca la versión de software que desea instalar en los dispositivos Onsight 5000HD.	

Información relacionada
[Actualizaciones de software \(en la página 77\)](#)

15.2.5. Política del cliente, mejores prácticas

Tabla 15-6 Política del cliente, mejores prácticas

Configuración	Valor	Descripción	Mejores prácticas/consejos
External Guest Users (Usuarios invitados externos)			
Allow users to invite external guests (Permitir a los usuarios invitar a invitados externos)	<input checked="" type="checkbox"/> predeterminada habilitada	Permite a los usuarios enviar invitaciones para invitados	
Allow text message guest invitations (Permitir invitaciones por mensaje de texto para los invitados)	<input checked="" type="checkbox"/> predeterminada habilitada	Permite a los usuarios enviar invitaciones por texto para los invitados.	
SMS Max Message to User Length (Longitud máxima de mensaje SMS a usuario)	100	Longitud máxima de caracteres	
Guest users must change temporary password on initial login (Los usuarios invitados deben cambiar la contraseña temporal en el primer inicio de sesión)	<input type="checkbox"/> predeterminada deshabilitada		
Send 'Invitation Sent' confirmation to host (includes copy of invite) (Enviar la confirmación de "Invitación enviada" al anfitrión (incluye una copia de la invitación))	<input checked="" type="checkbox"/> predeterminada habilitada	Le permite ver una copia de la invitación	
Disable recording of images and video (Deshabilitar la grabación de imágenes y video)	<input checked="" type="checkbox"/> predeterminada habilitada		
Disable global directory access (Deshabilitar el acceso al directorio global)	<input checked="" type="checkbox"/> predeterminada deshabilitada	No está habilitada para usuarios invitados	
Expiry (Expiración)	1	Día	
User can choose expiry time when inviting guests (El usuario puede elegir la fecha de expiración cuando invita a los invitados)	<input type="checkbox"/> predeterminada deshabilitada		
Deactivate guest user account when removed from contact list (Desactivar la cuenta de usuario de participante cuando se elimine de la lista de contactos)	<input type="checkbox"/> predeterminada deshabilitada	Cuando está habilitada, y quien invita elimina a un contacto invitado de la lista de contactos y luego, selecciona Deactivate la cuenta de invitado de este usuario. Si la anonimización de datos está habilitada, los datos personales del usuario invitado serán anónimos.	Si se habilita esta opción, las licencias estarán disponibles cuando la cuenta de invitado ya no sea necesaria.

Tabla 15-6 Política del cliente, mejores prácticas

Configuración	Valor	Descripción	Mejores prácticas/consejos
Include option for guest to call host immediately (Incluir la opción para que el invitado llame al anfitrión inmediatamente)	<input checked="" type="checkbox"/> predeterminada habilitada	Cuando se habilita, esta configuración permite al invitado llamar a quien lo invitó tan pronto como sea posible. También ofrece el enlace Join Call en el formulario. Cuando se deshabilita, la opción Join call se sustituye por la de Inicie una sesión en Onsite Connect.	Deje esta configuración como habilitada para facilitar que el invitado se una a la llamada.
From Email (Desde el correo electrónico)	Predeterminada	Determina si la invitación para los invitados proviene del correo electrónico del sistema o del correo electrónico personal de quien invita.	Configurarla en la dirección de correo electrónico de quien invita puede ayudar a identificar los correos electrónicos que provienen de una fuente confiable.
Custom Fields (Campos personalizados)	Obligatorio	Cuando se establece como obligatoria, quien invita debe completar los campos personalizados al enviar las invitaciones para los invitados.	Deje esta configuración según sea necesario para proporcionar más información al generar los informes.
Allow Setting User Mode while inviting guest (Permitir configurar el Modo de usuario al invitar a los invitados)	<input type="checkbox"/> Deshabilitada	Cuando se deshabilita, el usuario no puede especificar un modo de usuario al invitar a un invitado. Cuando se habilita, el usuario puede especificar modo Experto (usuario con experiencia) o Campo (usuario con experiencia limitada).	Habilite esta configuración cuando desee que sus usuarios tengan más flexibilidad en cuanto a la asignación de modos de usuario a los invitados.
User Mode (Modo de usuario)	Expert o Field	Establece el modo de usuario predeterminado para las invitaciones de los invitados.	Establezca el modo de usuario predeterminado que se adapte mejor a sus necesidades de uso.
General			
User Mode (Modo de usuario)	Expert	Establece el modo en el que opera el usuario cuando inicia sesión en un dispositivo Onsite.	La mayoría de los usuarios serán Experto. Puede considerar el uso del modo Campo para los invitados externos o para el personal de servicios de campo.
Prompt for Permissions (Solicitud de permisos)	As Required (Según sea necesario)*	Los usuarios de teléfonos inteligentes deben conceder permisos para acceder a recursos como el uso de datos e imágenes.	
Allow GPS in Video and Images (Permitir GPS en video e imágenes)	<input type="checkbox"/> Deshabilitada*	Los metadatos del GPS se incorporarán a las grabaciones e imágenes	
Screen Sharing (Compartir pantalla)	<input checked="" type="checkbox"/> Habilitada*	Permite compartir pantalla entre los participantes.	
Show GPS Overlay (Mostrar superposición de GPS)	<input type="checkbox"/> Deshabilitada*		

* Todos los valores predeterminados están marcados con un asterisco.

Tabla 15-6 Política del cliente, mejores prácticas


Configuración	Valor	Descripción	Mejores prácticas/consejos
Show Date/Time Overlay (Mostrar superposición de fecha y hora)	<input type="checkbox"/> Deshabilitada*		
Copy Captured Image to Gallery/Camera Roll (Copie la imagen capturada en la galería y carrete de la cámara)	<input type="checkbox"/> Deshabilitada*	Si está habilitada, las copias de las fotos/ videos se colocarán en la galería y carrete de la cámara	
Text Location of Overlay (Ubicación del texto de la superposición)	Parte inferior izquierda*		
Text Size of Overlay (Tamaño del texto de la superposición)	Pequeño*		
Image Resolution (Resolución de imagen)	Baja*	Establece la resolución de imagen máxima a la que se capturarán las imágenes localmente. Esta configuración también determinará la imagen de mayor resolución que se puede compartir en una llamada de Onsite con imágenes. Las imágenes de la galería o carrete de la cámara se compartirán con la resolución original con la que se capturaron. Las resoluciones se definen en función de la altura de la imagen en píxeles: baja (768), media (1080), alta (1440) y máxima (depende de la resolución máxima de la cámara del dispositivo).	<p>Cuando se comparte una imagen durante una llamada, se compartirá inicialmente con la resolución baja predeterminada de 1024x768. Si la imagen se capturó a una resolución más alta localmente, la imagen de mayor resolución está disponible durante una sesión de intercambio de imágenes que permite al usuario solicitar la imagen de mayor resolución al presionar el botón de alta resolución en el visor.</p> <p> Nota: Las imágenes de la galería o carrete de la cámara se comparten con su resolución original al presionar el botón de alta resolución.</p>
Copy captured images to Gallery/ Camera Roll (Copia de las imágenes capturadas en la galería o carrete de la cámara)	Desactivada*	Copia todas las imágenes capturadas en la galería o carrete de la cámara del usuario	

Tabla 15-6 Política del cliente, mejores prácticas


Configuración	Valor	Descripción	Mejores prácticas/consejos
Wait for Refresh on Lost Video Frame (Esperar para Actualizar el cuadro de video recuperado)	<input type="checkbox"/> Deshabilitada*	Cuando está habilitada, esta configuración mejora la calidad del video al incluir ajustes en la Unidad de Transmisión Máxima (MTU) que optimiza la distribución de paquetes multimedia en entornos difíciles. Esta capacidad le permite mostrar la última mejor imagen hasta que se reciba el marco completo de los paquetes de video.	Esta capacidad es ideal en situaciones en las que la calidad de la imagen es más importante que el movimiento.  Nota: Esta configuración requiere que los usuarios de Onsite Connect descarguen e instalen la última versión del software de Onsite Connect y que activen la configuración de Esperar para actualizar en el paquete recuperado. Dentro de Onsite Connect, haga clic en SETTINGS > CALLS > Video y habilite la opción Wait for refresh on packet loss.
Media Path (Ruta de medios)	{ApplicationData}	Establece la ruta predeterminada para el almacenamiento de medios de Onsite en la PC con Windows del usuario.	El almacenamiento de la ruta de medios debe ser lo suficientemente rápido como para aceptar velocidades de escritura de archivos en tiempo real con el fin de mantener el ritmo para guardar los flujos de video como grabaciones. La imposibilidad de mantener la velocidad de escritura hará que se pierdan marcos en la grabación y podría causar la corrupción del archivo. Los retrasos en la red pueden afectar a la calidad de la grabación.
Login (Iniciar sesión)			
Prompt to Remember Credentials (Auto Login) [Solicitud para recordar las credenciales (inicio de sesión automático)]	<input type="checkbox"/> Deshabilitada*	Los usuarios pueden introducir sus credenciales para iniciar sesión, para permitir un inicio de sesión automático cuando se inicie la aplicación.	No se recomienda para los usuarios que comparten dispositivos.
Run at Windows startup (Ejecutar al inicio de Windows)	<input type="checkbox"/> Deshabilitada*		
SIP			
SIP messaging (Mensajes de SIP)	TCP*	El transporte predeterminado para el protocolo SIP.	
Support SIP UPDATE method (Admite el método de ACTUALIZACIÓN de SIP)	<input checked="" type="checkbox"/> Habilitada*	Una característica de compatibilidad de SIP que algunos servidores de SIP utilizan para actualizar los parámetros de la sesión.	

Tabla 15-6 Política del cliente, mejores prácticas

Configuración	Valor	Descripción	Mejores prácticas/consejos
Verify SIP TLS Server (Verificar el servidor de TLS de SIP)	<input checked="" type="checkbox"/> Habilitada*	Determina si los servidores de SIP deben tener sus certificados verificados como auténticos antes de permitir las llamadas. Esto significa que el endpoint debe tener el certificado público de la Autoridad de Certificación (CA) que emitió y firmó el certificado del servidor de SIP.	Al estar habilitada puede bloquear algunas llamadas si el servidor de SIP de terceros utiliza certificados autofirmados. El certificado público autofirmado de la CA debe estar instalado para que la verificación tenga éxito y, por supuesto, usted debe confiar en la CA que autofirma.
Enable WebEx CMR Compatibility (Habilitar compatibilidad con CMR de WebEx)	<input type="checkbox"/> Deshabilitada*	Es necesario para la compatibilidad con CMR de WebEx.	Al hacer la llamada Onsite al CMR, parecerá que se está produciendo una "doble llamada", pero la llamada se conectará con éxito. La doble llamada se da cuando la llamada inicial se contesta pero se desconecta de inmediato, Onsite volverá a llamar inmediatamente para conectarse a WebEx con los parámetros de llamada admitidos.
Force Media Relay (Forzar relé de medios)	<input checked="" type="checkbox"/> Habilitada*	Obliga a que todos los medios pasen por los servidores de medios en lugar de permitir el enrutamiento de medios entre pares cuando los clientes están en la misma subred.	Esta se habilita de forma predeterminada para evitar que el tráfico de medios sea bloqueado por redes que no permiten el tráfico de red entre pares. Puede deshabilitar si está seguro de que el tráfico entre pares está permitido, si sus clientes se retrasan para utilizar las "Redes de invitados" en ubicaciones de terceros, podrían tener sus llamadas bloqueadas si no está permitido entre pares.
Media Configurations (Configuraciones de medios)			
Custom Media Configurations (Configuraciones de medios personalizadas)	Administrar configuraciones de medios	Cree las configuraciones de medios personalizadas y selecciónelas para distribuir las a través de la política del cliente.	Las configuraciones de medios personalizadas se pueden definir en función de la ubicación o la situación. Por ejemplo, usted sabe que un grupo de trabajadores de servicios de campo siempre encuentra condiciones de red celular deficiente en un determinado lugar. Defina una configuración de medios específica para esa ubicación y asigne esa configuración a la política del cliente del grupo de servicios de campo.

Tabla 15-6 Política del cliente, mejores prácticas

Configuración	Valor	Descripción	Mejores prácticas/consejos
Bandwidth Control (Control de ancho de banda)			
Bandwidth Control (Control de ancho de banda)	<input type="checkbox"/> Deshabilitada*	Cuando está deshabilitada, permite al administrador establecer la tasa máxima de bits de video permitida para las configuraciones de medios en un endpoint.	
Maximum Video Bit Rate (Kbps) [Tasa máxima de bits de video (Kbps)]	2500*	Establece la tasa máxima de bits de video permitida. (8 a 6000)	
Default MTU Size (bytes) (Tamaño de MTU predeterminado (bytes))	1200	De forma predeterminada, la Unidad Máxima de Transmisión (MTU) se define en 1200 bytes. Los clientes pueden ajustar esta configuración en entornos difíciles para mejorar la calidad del video.	
Bandwidth Adaptive Streaming (BAS) (Transmisión Adaptable al Ancho de Banda (BAS))	Redes celulares*	Habilita la BAS (Transmisión Adaptable al Ancho de Banda) para los usuarios de teléfonos inteligentes. La BAS eliminará dinámicamente las imágenes para mantener la conexión en redes con ancho de banda bajo, dando preferencia a los paquetes de audio.	Se recomienda el uso de la BAS para garantizar la conectividad de las llamadas en redes poco confiables, como las redes celulares. El audio tiene prioridad en una llamada para mantener la comunicación durante una llamada Onsite. Los usuarios pueden ajustar la configuración de medios a resoluciones más bajas y compartir imágenes fijas de alta resolución en condiciones de ancho de banda bajo.
Media configuration on connection (Configuración de medios en la conexión)	Nula	Establece la configuración de medios predeterminada que se utiliza cuando se conectan las llamadas.	Esto se debe establecer en una configuración de medios de ancho de banda más bajo, ya que las llamadas se pueden hacer en condiciones de red desconocidas. Se pueden seleccionar configuraciones de medios de mayor resolución/ancho de banda durante la llamada. Los usuarios generalmente ejecutarían una prueba de ancho de banda para determinar el ancho de banda máximo disponible durante la llamada.
Pause Video While Transferring Image (Pausar el video mientras transfiere la imagen)	<input checked="" type="checkbox"/> Habilitada*	Esta configuración pausa el video mientras se produce una transferencia de imágenes. El endpoint que es la fuente de video activa indicará si el video está en pausa en función de esta configuración.	

Tabla 15-6 Política del cliente, mejores prácticas

Configuración	Valor	Descripción	Mejores prácticas/consejos
Preferred Voice Codec (Códec de voz preferido)	Predeterminada*	Determina el ancho de banda de audio que se utiliza para el audio de voz en una llamada.	El códec de audio Opus utilizará 24 Kbps como velocidad de bits de destino cuando se establezca en predeterminada, utilizará 10 Kbps cuando se establezca en "Velocidad baja de bits". Esto no incluye la sobrecarga de paquetes asociada con los paquetes de audio.
Preferred Subject Audio Codec (Códec de audio de sujeto preferido)	Predeterminada*	Determina el ancho de banda de audio para el audio asociado al video, también conocido como audio de sujeto. La mayoría de los usuarios no necesitarán que se active el audio de sujeto.	El códec de audio Opus utilizará 24 Kbps como velocidad de bits de destino cuando se establezca en predeterminada, utilizará 10 Kbps cuando se establezca en "Velocidad baja de bits". Esto no incluye la sobrecarga de paquetes asociada con los paquetes de audio. El audio del sujeto se debe utilizar cuando el aislamiento de audio es obligatorio como parte de la resolución de problemas. Por ejemplo, ruido del motor. Por lo general, se utiliza un micrófono externo con un hub de Onsite Collaboration con el adaptador multipuerto 5000HD.
Audio Efficiency (Eficiencia de audio)	Latencia más baja*	Se utiliza para determinar cómo se transmiten los paquetes de audio de voz en una llamada. La latencia más baja enviará los paquetes de audio a medida que se generen. El ancho de banda más bajo agrupará los paquetes de audio para reducir la sobrecarga de red asociada al envío de paquetes individualmente.	Para redes de ancho de banda alto: > 1 Mbps elija LATENCIA MÁS BAJA para redes de ancho de banda medio: 500 Kbps a 1 Mbps elija LATENCIA MEDIA/ANCHO DE BANDA para redes de ancho de banda medio: < 500 Kbps elija ANCHO DE BANDA MÁS BAJO para las redes satelitales: < 500 Kbps con latencia alta elija LATENCIA ALTA
Calls (Llamadas)			
Allow New Contacts (Permitir contacto nuevo)	<input type="checkbox"/> Deshabilitada*	Deshabilitada de forma predeterminada, esta configuración permite a los clientes agregar contactos fuera de su organización al utilizar una dirección SIP. Cuando está habilitada los usuarios solo pueden acceder al directorio global de su organización y el signo más (+) no aparece en la ventana Contacts.	Utilice la configuración predeterminada, a menos que el cliente tenga problemas de privacidad y quiera que se habilite esta capacidad para restringir las llamadas solo a su directorio global y a los miembros del grupo.
Allow Cellular/Mobile Data Usage (Permitir el uso de datos celulares/móviles)	<input type="checkbox"/> Deshabilitada*	Es necesario para los usuarios de teléfonos inteligentes sin acceso a Wi-Fi.	Los usuarios de datos celulares deben tenerla habilitada. Por ejemplo, los usuarios de servicios de campo que no tienen acceso a redes inalámbricas 802.11.

Tabla 15-6 Política del cliente, mejores prácticas

Configuración	Valor	Descripción	Mejores prácticas/consejos
Prompt to Enable Cellular/Mobile Data Usage (Solicitud para habilitar el uso de datos móviles/celulares)	Nunca *	Se establece cuándo solicita permiso al usuario para utilizar los datos celulares.	
Start remote/non-Onsight video on connection (Iniciar video remoto/no Onsight en la conexión)	<input type="checkbox"/> Deshabilitada *	Al llamar a los endpoint no Onsight, el flujo de vídeo se iniciará automáticamente.	Esto evita confusiones al llamar a salas de videoconferencia o de reuniones de terceros. Los usuarios a veces se olvidan de iniciar el flujo de vídeo.
Fill/Fit video in viewfinder when streaming (Rellenar/ajustar video en el visor al transmitir)	Rellenar *	Fill, rellena la pantalla horizontalmente. La parte superior e inferior se pueden recortar para ajustarse. Fit, rellena la pantalla verticalmente. Es posible que aparezca un borde negro en los lados del espectador. Actual Size: muestra el video en su resolución original. El video puede aparecer con un borde negro alrededor.	
Maximum Number of Connections (Cantidad máxima de conexiones)	4	La PC con Windows puede funcionar como anfitrión de la conferencia y agregar varios participantes a una llamada. El hardware del PC y el ancho de banda de la red disponible para el PC con Windows pueden afectar a la calidad de la llamada.	
Auto Answer (Respuesta Automática)	<input type="checkbox"/> Deshabilitada *	Habilita la capacidad de respuesta automática a una llamada entrante.	Útil para los endpoint sin supervisión, como las cámaras inteligentes robustas de Onsight.
Auto answer delay (seconds) [Retardo de respuesta automática (segundos)]	5	Establece el retardo antes de que una llamada entrante se responda de forma automática.	
Push Notifications (Notificaciones push)	<input checked="" type="checkbox"/> Habilitada *	Determina si los clientes de Android utilizan las notificaciones push cuando la aplicación está en segundo plano o no se está ejecutando. Los dispositivos iOS siempre utilizan las notificaciones push según la política de Apple.	Al habilitar las notificaciones push permite que Onsight Connect sea optimizado por la batería de un dispositivo Android, si las notificaciones push están deshabilitadas, Onsight Connect se debe ignorar por la optimización de la batería para que pueda acceder a la red mientras un dispositivo está en modo de espera o reposo.

Tabla 15-6 Política del cliente, mejores prácticas


Configuración	Valor	Descripción	Mejores prácticas/consejos
Prompt to Ignore Battery Optimizations (Solicitud para ignorar las optimizaciones de la batería)	<input checked="" type="checkbox"/> Habilitada*	Hay dos opciones: Siempre que las notificaciones push estén deshabilitadas. Solo cuando el usuario desactiva las notificaciones push.	Ignorar las optimizaciones de la batería permite que una aplicación acceda a la red cuando el dispositivo está en modo de espera o reposo. Para dispositivos Android: Cuando un usuario deshabilita las notificaciones push, se activa una ventana emergente que solicita al usuario habilitar Ignore Battery Optimizations. Esto los llevará a la configuración externa de la optimización de la batería de Android, donde deben seleccionar Onsite para eliminarla de la lista de aplicaciones de optimización para la batería del dispositivo.  Nota: Si un usuario decide no habilitar la opción de Ignore Battery Optimizations, no recibirá notificaciones cuando el dispositivo esté en modo de reposo. Y no se les solicitará que vuelvan a habilitar la opción de Ignore Battery Optimizations a menos que vuelvan a habilitar y a deshabilitar las notificaciones push.
Encryption Mode (Modo de cifrado)	Automático*	El valor predeterminado debería ser Automático, esto asegura que todas las conexiones de Onsite tendrán el cifrado habilitado durante la llamada. Automático también da la flexibilidad de llamar a los sistemas de videoconferencia que no tienen el cifrado establecido.	Si no se desea llamar a sistemas que no tienen el cifrado establecido, establezca el cifrado en On. Cualquier endpoint que no admite el cifrado no se aceptará como una conexión válida.
Prompt to Share Images After Capture (Solicitud para compartir imágenes después de la captura)	<input checked="" type="checkbox"/> Habilitada*	Se solicitará al usuario que comparta después de una captura de imagen.	Habilitar para usuarios principiantes e invitados.
Allow recording video/audio and saving images for ALL participants (Privacy Mode) [Permitir la grabación de video/audio y guardar las imágenes para TODOS los participantes (Modo de privacidad)]	<input type="checkbox"/> Deshabilitada*	Deshabilita las grabaciones e instantáneas de todos los participantes en una llamada.	Se podría usar para invitados externos o grupos específicos en función de los requisitos de privacidad.
Local Privacy Mode (Modo de privacidad local)	Permitir grabaciones y guardar instantáneas*	Permite flexibilidad en cuanto a los medios que pueden almacenar los usuarios.	Se podría usar para invitados externos o grupos específicos en función de los requisitos de privacidad.

Tabla 15-6 Política del cliente, mejores prácticas

Configuración	Valor	Descripción	Mejores prácticas/consejos
Software Acoustic Echo Cancellation (AEC) (Software de cancelación del eco acústico (AEC))	<input checked="" type="checkbox"/> Habilitada	Predeterminada activada o desactivada	A DETERMINAR
Software Acoustic Echo Cancellation (AEC) [Software de cancelación del eco acústico (AEC)]	A DETERMINAR	Predeterminada activada o desactivada	A DETERMINAR
Noise Suppression (Supresión del ruido)	<input checked="" type="checkbox"/> Habilitada	Predeterminada activada o desactivada	
Save Call Transcript (Guardar la transcripción de la llamada)	<input checked="" type="checkbox"/> Habilitada	Habilitada predeterminada	Permite que todas las llamadas se transcriban en el idioma (predeterminado).
Require consent for remote video sharing requests (Requerir consentimiento para solicitudes remotas de uso compartido de videos)	<input type="checkbox"/> Deshabilitada*	La predeterminada está deshabilitada. Cuando se habilita, se debe conceder el consentimiento antes de iniciar una transmisión de video con un participante.	Se podría usar para invitados externos o grupos específicos en función de los requisitos de privacidad. Esta configuración ofrece a los clientes un mayor control sobre el uso compartido de videos durante una llamada de Onsite. La privacidad de los videos se mejora en ubicaciones sensibles al requerir que los usuarios den su consentimiento antes de compartir videos.
Networking (Redes)			
Diffserv DSCP (Voice) (Voz)	Mejor esfuerzo *	Mejor esfuerzo: 0, carga controlada: 24, audio/video/garantizado: 40, voz: 56	
Diffserv DSCP (Video)	Mejor esfuerzo *		
Diffserv DSCP (Subject Audio) (audio de sujeto)	Mejor esfuerzo *		
Diffserv DSCP (Data Stream) (flujo de datos)	Mejor esfuerzo *		
TeamLink			
Enable (Habilitar) TeamLink	<input checked="" type="checkbox"/> Habilitada *	Cuando está habilitada, TeamLink determinará si firewall permite el registro directo del SIP o si debe utilizar HTTPS para proxy de los mensajes de SIP a través de los servidores de TeamLink.	
Allow HTTP registration (Permitir registro HTTP)	<input checked="" type="checkbox"/> Habilitada *	Se utiliza para la resolución de problemas.	HTTPS se utiliza de forma predeterminada y es el transporte preferido para TeamLink, HTTP solo se utiliza si HTTPS no está disponible.

Tabla 15-6 Política del cliente, mejores prácticas


Configuración	Valor	Descripción	Mejores prácticas/consejos
Do not allow direct SIP registration (Use for troubleshooting only) [No permitir el registro directo del SIP (utilizar solo para la resolución de problemas)]	<input type="checkbox"/> Deshabilitada*	Cuando se habilita, TeamLink dirigirá todo el tráfico a través de HTTPS.	Esto solo se recomienda para la resolución de problemas. Forzar TeamLink podría provocar su uso cuando no es necesario.
Firewall Detect (Detección de firewall)			
SIP Detection Method (Método de detección de SIP)	TeamLink*	Se utiliza para determinar qué servidores son el objetivo de TeamLink para la prueba de detección de firewall. La prueba de detección de firewall determinará el mejor método a utilizar para pasar el firewall.	Esta configuración no se debe cambiar a menos que se consulte con el soporte de Librestream.
Workspace			
Access (Acceso)	<input checked="" type="checkbox"/> Habilitada*	Autoriza el acceso a Onsight Workspace de los miembros del grupo.	Habilite Onsight Workspace solo cuando los usuarios necesiten cargar, ver y editar archivos al utilizar Onsight Connect.
Upload Path (Ruta de carga)	~/onsight	Establece la estructura de directorios de nivel superior en Workspace. Todos los archivos cargados se colocarán en la ruta de carga en una carpeta de Llamadas.	Todos los miembros del grupo tendrán sus carpetas de llamadas colocadas en la ruta de carga. Utilice una ruta de carga diferente para los distintos grupos.
Auto Upload Media (Carga automática de medios)	<input type="checkbox"/> Deshabilitada*	Cuando está habilitada, cualquier archivo capturado durante una llamada Onsight se cargará automáticamente en Workspace una vez que la llamada termina.	Los usuarios no tendrán control sobre los archivos que se cargaron.
Maximum Upload Bit Rate (Kbps) [Velocidad máxima de bits de carga (Kbps)]	0*	Si se establece en 0, la carga de archivos avanzará sin ninguna restricción de ancho de banda controlada por la aplicación. Cuando se establece un límite, la carga de archivos no superará el valor máximo en Kbps.	 Nota: La tasa de bits de carga estará sujeta a las limitaciones de la red en el ancho de banda.

Tabla 15-6 Política del cliente, mejores prácticas




Configuración	Valor	Descripción	Mejores prácticas/consejos
Restrict Upload Folder Access to Owner (Restringir el acceso a la carpeta de carga al propietario)	<input type="checkbox"/> Deshabilitada*	De forma predeterminada, todos los usuarios de Workspace pueden ver todas las carpetas. Cuando está habilitada, los usuarios solo pueden acceder a las carpetas de carga que poseen. Los permisos de las carpetas en Workspace tendrán que ser editados manualmente para cambiar esta configuración.	Los permisos de archivos y carpetas se pueden editar por un administrador al iniciar sesión en Onsite Workspace. Tenga cuidado al habilitar esta configuración, cancelar los permisos para permitir compartir puede ser tedioso para múltiples directorios.  Nota: Que incluso aún si todos los usuarios tienen acceso completo a todas las carpetas de Workspace, los archivos originales siempre estén protegidos de la edición. Las ediciones solo se pueden realizar en las copias de las versiones de los archivos originales.
Allow cellular/mobile data usage (Permitir el uso de datos celulares/móviles)	<input checked="" type="checkbox"/> Habilitada*	Cuando está habilitada, los archivos se cargarán utilizando los datos del celular/móvil si no hay una conexión inalámbrica disponible. Si está deshabilitada, los archivos no se cargarán hasta que haya una conexión de red inalámbrica disponible.	Se dará prioridad a la carga de archivos a través de una red inalámbrica. Los datos del celular/móvil solo se utilizarán en ausencia de una red inalámbrica.
Artificial Intelligence (Inteligencia artificial)			
AI Setting (Configuración de IA)	Ninguno	Establece el perfil de IA predeterminado.	 Nota: Solo se puede aplicar un perfil de configuración de IA a una política del cliente. Se recomienda combinar todas las configuraciones de IA en un solo perfil.
CV Document Link URL (URL de enlace del documento de CV)	Ninguno	Establece la URL de enlace del documento de visión por computadora	Ingrese la URL en el campo CV Document Link URL . Esto le permitirá administrar todos los enlaces de sus documentos desde una sola ubicación.  Nota: Los enlaces personalizados (de documentos) no funcionarán si el Local Privacy Mode está activado para su dominio, grupo o cuenta de usuario.

Tabla 15-6 Política del cliente, mejores prácticas

Configuración	Valor	Descripción	Mejores prácticas/consejos
Auto Tag Images (Etiquetado automático de imágenes)	<input type="checkbox"/> Deshabilitada*		
Transcription Language (Lenguaje de transcripción)		Establece el idioma predeterminado para las transcripciones.	
Custom Messages (Mensajes personalizados)			
Login (Iniciar sesión)		Establece el mensaje personalizado para iniciar sesión cuando un usuario se conecta.	A DETERMINAR
Recording (Grabación)		Establece un mensaje de grabación personalizado que se muestra a todos los participantes cuando una llamada comienza a grabarse.	A DETERMINAR

15.2.6. Permisos de cliente, mejores prácticas

Tabla 15-7 Permisos de cliente, mejores prácticas

Configuración	Acción					Mejores prácticas/consejos
	Dominio predeterminado	Administrador del cliente	Usuarios estándar	External Guest Users (Usuarios invitados externos)	Grupo de licencias de dominio	
General						
Enable GPS in Video and Images (Permitir el GPS en los videos e imágenes)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	No utilice Inherit como acción para el grupo de Usuarios invitados externos sin tener en cuenta el acceso que tendrá el invitado a la configuración de los ajustes. Por ejemplo, si estableció el modo de Privacidad local para desactivar las grabaciones y guardar instantáneas para el grupo de Usuarios invitados externos, pero concedió permisos para editar la configuración, entonces permitió de hecho que el usuario invitado tenga acceso a guardar grabaciones e instantáneas, si editan la configuración localmente en endpoint.
Show GPS Overlay (Mostrar superposición de GPS)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Show Date/Time Overlay (Mostrar superposición de fecha y hora)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	

* Todos los valores predeterminados están marcados con un asterisco.

Tabla 15-7 Permisos de cliente, mejores prácticas

Configuración	Acción					Mejores prácticas/consejos
	Dominio predeterminado	Administrador del cliente	Usuarios estándar	External Guest Users (Usuarios invitados externos)	Grupo de licencias de dominio	
Text Location of Overlay (Ubicación del texto de la superposición)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Text Size of Overlay (Tamaño del texto de la superposición)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Image Capture Resolution (Resolución de captura de imagen)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Permite al usuario definir la resolución de captura de la imagen.
Encoder Hardware Acceleration (Aceleración del hardware del codificador)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Solo se aplica a los PC con Windows.
Media Path (Ruta de medios)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Copy Captured Image to Gallery / Camera Roll (Copie la imagen capturada en la galería y carrete de la cámara)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Allow Illumination (Permitir la iluminación)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Se aplica a cualquier cliente que admite la iluminación.
Allow Flash (Permitir el flash)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Se aplica a cualquier cliente que admite el flash.
Allow Laser (Permitir el láser)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Se aplica solo a Cube.
Login (Iniciar sesión)						
Auto Login (Inicio de sesión automático)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	No se recomienda para los usuarios que comparten un dispositivo.
Run at Windows startup (Ejecutar al inicio de Windows)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
SIP						
SIP messaging (Mensajes de SIP)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Support SIP UPDATE method (Admite el método de ACTUALIZACIÓN de SIP)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	

Tabla 15-7 Permisos de cliente, mejores prácticas

Configuración	Acción					Mejores prácticas/consejos
	Dominio predeterminado	Administrador del cliente	Usuarios estándar	External Guest Users (Usuarios invitados externos)	Grupo de licencias de dominio	
Verify SIP TLS Server (Verificar el servidor de TLS de SIP)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
Enable WebEx CMR Compatibility (Habilitar compatibilidad con CMR de WebEx)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
Force Media Relay (Forzar relé de medios)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
IP Calls (Llamadas IP)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Media Configurations (Configuraciones de medios)						
Low Profile (Perfil bajo)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Medium Profile (Perfil medio)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
High Profile (Perfil alto)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
HD (720p) Profile [Perfil HD (720p)]	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Full HD (1080p) Profile [Perfil Full HD (1080p)]	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Custom Profiles (Perfiles personalizados)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Bandwidth Control (Control de ancho de banda)						
Enable Bandwidth Control (Habilitar el control del ancho de banda)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Maximum Video Bit Rate (Tasa máxima de bits de vídeo)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Enable BAS (Habilitar BAS)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Es posible que quiera dar a los usuarios la capacidad de editar BAS, ya que podría no ser obligatorio en redes celulares no congestionadas. BAS puede restringir la velocidad de imagen de forma innecesaria si la red experimenta una caída temporal del ancho de banda.

Tabla 15-7 Permisos de cliente, mejores prácticas

Configuración	Acción					Mejores prácticas/consejos
	Dominio predeterminado	Administrador del cliente	Usuarios estándar	External Guest Users (Usuarios invitados externos)	Grupo de licencias de dominio	
Media MTU (Medios MTU)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	Un usuario normal nunca debería necesitar ajustar la MTU. El personal de TI puede encontrar esto útil cuando se trata de solucionar problemas de la red.
Media configuration on connection (Configuración de medios en la conexión)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Esto se debe establecer en una configuración de medios de ancho de banda más bajo, ya que las llamadas se pueden hacer en condiciones de red desconocidas. Se pueden seleccionar configuraciones de medios de mayor resolución/ancho de banda durante la llamada. Los usuarios generalmente ejecutarían una prueba de ancho de banda para determinar el ancho de banda máximo disponible durante la llamada.
Pause Video while transferring image (Pausar el video mientras transfiere la imagen)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	En las redes deficientes, la transmisión de video mientras se transfiere una imagen puede afectar a la calidad de la llamada, por lo que puede permitir a los usuarios establecer "Pause video while transferring".
Preferred Voice Codec (Código de voz preferido)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Se puede utilizar G.7.11 cuando el ancho de banda de la red es bueno (> 300 Kbps), el GSM debe utilizarse en condiciones de ancho de banda bajo. En condiciones de red deficientes puede ser una ventaja cambiar al código de ancho de banda más bajo (GSM). Sin embargo, la mejor práctica es controlar los códecs de audio a través de la política del cliente.
Preferred Subject Audio Codec (Código de audio de sujeto preferido)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	El audio del sujeto se debe utilizar cuando el aislamiento de audio es obligatorio como parte de la resolución de problemas. Por ejemplo, ruido del motor. Por lo general, se utiliza un micrófono externo con un hub de Onsite Collaboration con el adaptador multipuerto 5000HD. Si un usuario necesita el audio del sujeto ocasionalmente, esto se debe establecer en "Allow".
Audio Efficiency (Eficiencia de audio)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Este ajuste puede ser útil para los usuarios que transmiten por satélite de BGAN. Sin embargo, los usuarios de BGAN deben tener la eficiencia de audio establecida en "Lower Bandwidth" a través de la política del cliente.
Calls (Llamadas)						
Allow Cellular/Mobile Data Usage (Permitir el uso de datos celulares/móviles)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	

Tabla 15-7 Permisos de cliente, mejores prácticas

Configuración	Acción					Mejores prácticas/consejos
	Dominio predeterminado	Administrador del cliente	Usuarios estándar	External Guest Users (Usuarios invitados externos)	Grupo de licencias de dominio	
Start remote/non-Onsight video on connection (Iniciar video remoto/no Onsight en la conexión)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Maximum Number of Connections (Cantidad máxima de conexiones)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
Enable auto answer (Habilitar respuesta automática)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Es obligatorio para la compatibilidad con algunos sistemas de videoconferencia de terceros.
Auto answer delay (seconds) [Retardo de respuesta automática (segundos)]	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Push Notifications (Notificaciones push)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Solo para clientes de Android.
Encryption Mode (Modo de cifrado)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Prompt to Share Images After Capture (Solicitud para compartir imágenes después de la captura)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Disable recordings and saving snapshots for all participants (Desactivar las grabaciones y guardar instantáneas para todos los participantes)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Local Privacy Mode (Modo de privacidad local)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
Require consent for remote video sharing requests (Requerir consentimiento para solicitudes remotas de uso compartido de videos)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	

Tabla 15-7 Permisos de cliente, mejores prácticas

Configuración	Acción					Mejores prácticas/consejos
	Dominio predeterminado	Administrador del cliente	Usuarios estándar	External Guest Users (Usuarios invitados externos)	Grupo de licencias de dominio	
Networking (Redes)						
Diffserv DSCP (QoS)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
TeamLink						
Enable/Disable TeamLink (Habilitar/deshabilitar TeamLink)	Allow	Allow	Inherit*	Inherit*	Inherit*	
Change TeamLink Settings (Cambiar la configuración de TeamLink)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
Firewall Detect (Detección de firewall)						
SIP Detection Method (Método de detección de SIP)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
Workspace						
Maximum Upload Bit Rate (Kbps) [Velocidad máxima de bits de carga (Kbps)]	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Permitir a los usuarios editar la velocidad de bits de carga puede ser útil para cargar archivos grandes.
Allow cellular/mobile data usage (Permitir el uso de datos celulares/móviles)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Permitir que los usuarios editen el uso de datos del celular/móvil puede afectar los planes de datos.
Software Updates (Actualizaciones de software)						
Install Software Updates (Instalar actualizaciones de software)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Permite a los usuarios instalar actualizaciones de software desde OPM (PC, Cube, 5000HD y Hub).
Update Server (Actualizar el servidor)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Permite al usuario introducir una URL de actualización de SW en una red local que dirige a un paquete de actualización de Onsight.
Check for updates automatically (Comprobar las actualizaciones automáticamente)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Permite las alertas automáticas de actualización de SW cuando el usuario se conecta a un cliente.

Información relacionada

[Política y permisos del cliente \(en la página 78\)](#)

Índice

Caracteres Especiales

- Última actividad 91
- Última modificación 34
- Última versión publicada 77, 77

Números

- 10/100 Ethernet 9
- 443 9
- 5000HD 77, 77
- 802.11 a/b/g/n 9

A

- Acceso 74
- Acceso a Workspace 19
- Acceso al contenido 51
- Acceso de lectura/escritura 86
- Acceso de superadministrador 52
- Acceso público a Internet 54
- Acción 78
- Acciones comunes 13, 25, 27, 29, 32, 34, 35, 52, 52, 53
- Activador 105
- Actividad del cliente 91, 98
- Activo 75, 91
- Activos 19
- Activos del Workspace 75
- Actualizaciones 77
- Actualizaciones automáticas 77
- Actualizaciones de software 77, 77
- Actualizaciones del cliente de OnSight móvil 77
- Actualizaciones del Hub de OnSight Collaboration 54
- Actualizar 93
- Actualizar los registros existentes 40, 46
- Acuerdo de licencia de usuario final (EULA) 109
- Administración de clave de API 54, 54
- Administración de configuración de privacidad 81
- Administración de grupo de licencia y política 21
- Administración de grupo de licencias 22
- Administración de licencia de dominio 21
- Administración de los administradores de grupo 32
- Administración de usuario 31
- Administración del conocimiento 73
- Administración del sitio 70
- Administrador 13, 16, 23, 25, 31, 51
- Administrador de grupo 25, 31, 32, 32
- Administrador de OnSight 43
- Administrador de OPM 53, 78
- Administrador del cliente 25
- Administrador del servidor SIP 72
- Administrador principal 13
- Administrador temporal 16
- Administradores 13, 62
- Administradores adicionales 31
- Administradores de grupo 34, 34, 35
- Administrar 19
- Administrar contactos externos 47
- Administrar datos 73
- Administrar grabaciones 73
- Administrar imágenes 73
- Administrar licencias de usuario 21
- Administrar usuarios 23, 34, 34, 35
- Advertencia 96
- Agregar a contactos 14
- Agregar a la lista 48
- Agregar manualmente un contacto externo 45
- Agregar manualmente un grupo 23
- Agregar miembros 34
- Agregar miembros seleccionados 34
- Agregar usuarios 25
- Agregar/eliminar contactos externos de las listas 48
- Agregar/eliminar miembros del grupo 34
- Alemán 103
- Algoritmo de firma 63, 64
- Algoritmo de resumen 63, 64
- Altitud de llamada 93
- Amarillo 79
- Ambos 100, 101
- Android 28, 77
- Android Google Play Store 28
- Anfitriones de conferencias 54
- Anonimización 56
- Anonimización de datos 56, 56, 98
- Anonimización de datos PII 56
- Anonimización programada 56
- Anonimizar datos de los usuarios activos 56
- Anonimizar usuarios previamente eliminados de su dominio 56
- Anular la contraseña de los usuarios existentes 40
- Anular, 78
- Apellido 16, 25, 39, 43, 67
- API 53
- API de dispositivo IoT 88
- API de llamada en OnSight 54
- API de medición de IoT 88
- API de OCR 88
- API de procesamiento natural del idioma 88
- API de SCIM 54
- API de SMS 85
- API de usuarios invitados 54
- API de visión de la computadora 88
- API del Workspace 54, 73
- Aplicación de hoja de cálculo 40
- Aplicar filtro 91, 93, 96, 96, 101
- Archivo CSV 40
- Archivo de importación 39
- Archivo de metadatos de IdP 63
- Archivo de valores separados por comas (CSV) 39
- Archivo para importar 40, 40
- Arquitectura de plataforma de realidad aumentada OnSight 7
- Arquitectura segura 73
- Aserción SAML 65
- Aserciones firmadas requeridas 63
- Asignación automática de autorregistro 71
- Asignación de administradores de grupo 35
- Asignación de correo electrónico 65
- Asignación de ID de SSO federado 65, 66
- Asignación de identidad 40, 65
- Asignación de identidad de usuario 66
- ASIGNACIÓN DE IDENTIDAD DE USUARIO 66
- Asignación de nombre de usuario 65
- Asignación de un administrador a un grupo 32
- Asignación de usuarios a un grupo 32
- Asignación del correo electrónico 66
- Asignación del nombre de usuario 65
- Asignación manual de cuentas SIP 73

Asignar automáticamente cuentas SIP a usuarios autorregistrados 71, 72
Asignar automáticamente cuentas SIP a usuarios nuevos 39, 40
Asignar automáticamente una cuenta SIP a este usuario 16, 25, 73
Asignar licencias 39
Asignar/restablecer una cuenta SIP 73
Asignar/Restaurar cuenta de Workspace 74
Asignar/Restaurar cuenta SIP 25
Atributo 65, 66, 66, 67
Atributo de IdP asignado 40, 65, 65, 66, 66
Atributo SSO 29
Audio de video 93
Auditoría de contenido 73
Autenticación 57
Autenticación básica HTTP 75
Autenticado 51
Autenticado localmente durante 30 días en el cliente 51
Autoetiquetado de imágenes/videos 56
Automatizar el proceso para iniciar sesión 28
Autorizado 51
Autorregistro 25, 59, 61, 71
Autorregistro de SSO 67
Ayuda para mensajes personalizados 86

B

Bloquear 87
Borrar 78
Borrar grupo 34
Borrar miembros 34
Buscar actualizaciones 77
Búsqueda 14
Búsqueda y recuperación rápida 73

C

Cámara inteligente de Onsite 83
Cambiar contraseña 13
Cambiar contraseñas 31
Cambiar la configuración 31
Cambiar propietario de cuenta 52, 53
Cambiar tipo de cuenta 32
Cambié la contraseña del usuario (texto, SMS) 103
Campo de cuenta Onsite 65, 65, 66
Campos de cuenta Onsite 65
Campos personalizados 57, 59, 80, 98, 98, 99
Cantidad máxima de intentos incorrectos de inicio de sesión 61
Cantidad mínima de caracteres no alfabéticos 60
Cantidad mínima de letras mayúsculas 60
Cantidades de llamadas o de inicios de sesión 100
Capacidades de auditoría 73
Captura de imágenes fijas 54
Capturar contenido 19
Características clave de Workspace 73
Características de la licencia 53
Carga automática 73
Carga automática de medios 74
Carga de archivo 40
Carga manual 73
Cargar 40, 46, 63
Cargar certificado IdP 63, 63
Cargar contenido 19
Cargar datos 73, 73
Cargar grabaciones 73
Cargar imágenes 73
Carpeta de carga 19
Casos especiales 39
Certificado de proveedor de servicio local SHA1 70
Certificado de SP 63

Certificado IdP 63, 63
Certificado público IdP 63
Chino (Simplificado) 103
Cifrado 93
Cifrado de clave 70
Cifrado SAML 70
Cisco VCS Expressway 71
Clave 61
Clave de API 96
Clave de autorregistro 43
Clave de registro 61
Clave generada por API 87
CLAVES DE API 86
Claves de interfaz de programación de aplicaciones 86
Cliente creado 52
Cliente de Onsite 58
Cliente Onsite Connect 7, 13
Clientes de Enterprise 62, 63
Código de video 93
Código de voz 93
Código Challenge 43
Colaborador 19
Colaborar 19
Compartir audio 7
Compartir contenido 19
Compartir datos 73
Compartir grabaciones 73
Compartir imágenes 7, 73
Compartir pantalla 54
Compartir video 7
Compatibilidad con CMR de WebEx 85
Complemento con licencia 63
Completo 86
Comportamiento del usuario invitado 79
Comuníquese con el código QR de soporte 111
Conceder acceso 61
Condiciones de uso 105
Configuración 29, 51, 52, 52
Configuración a nivel de grupo 31
Configuración de IA 88
Configuración de IIS 9
Configuración de inteligencia artificial (IA) 88
Configuración de privacidad 84
Configuración de proveedor de servicio local 64
Configuración de seguridad y SSO 29
Configuración de sus ajustes de IdP 63
Configuración del certificado SSO 70
Configuración del cliente 16, 25, 31
Configuración del cliente de usuarios 25
Configuración del dominio 31
Configuración del lenguaje de marcado de aserción de seguridad 63
Configuración del nivel de dominio 79
Configuración del proveedor de identificación de socio 63
Configuración del proveedor de servicio de socio 63
Configuración del servidor 70
Configuración global de los invitados externos 57
Configuración personal 13, 13, 14
Configuración SAML 62, 63, 63, 64, 64, 65
Configuración SIP 40, 72
Configuración SIP pública 71
Configuración SSO 40
Configuración Webhook 75
Configuraciones de medios 54
Configuraciones de medios personalizadas 55
Configurar la política del cliente 81

- Configurar los permisos de cliente 82
- Configure manualmente sus ajustes IdP 64
- Confirmación 79
- Confirmación de cambio de contraseña 86
- Confirmación de participante externo 86
- Confirmación de usuario invitado (texto) 103
- Confirmar los cambios 51
- Conjunto de uso de clave extendido 70
- Connect Enterprise 19, 19, 25, 40, 53, 93
- Connect Enterprise con Workspace Contributor) 19
- Connect Enterprise con Workspace Enterprise 19
- Consentimiento 84
- Consumo de datos móviles 73
- Contacto de soporte 111
- Contacto externo 45
- Contacto nuevo 45
- Contactos 14, 14
- Contactos externos 39, 40, 45, 47, 48, 58
- Contactos predeterminados 39
- Contacts.csv 40
- Contacts.xml file 40
- Contenido 19, 73
- Contraseña 9, 13, 28, 72, 75, 79
- Contraseña de autenticación 72, 72, 72
- Contraseña inicial 43
- Contraseñas 39
- Control automático de versiones 73
- Control de ancho de banda 54
- Control de dominio 21
- Controles de permiso 73
- Controles de permiso detallados 73
- Coreano 103
- Correo electrónico 16, 25, 43, 66
- Correo electrónico de bienvenida 9, 16, 27
- Correo electrónico de bienvenida a Onsite 43
- Correo electrónico de confirmación de la aprobación 43
- Correo electrónico de invitación 62
- Correo electrónico del administrador 75
- Correo electrónico local de bienvenida 28
- Correo electrónico obligatorio 61
- Correo electrónico personalizado 55
- Correos electrónicos de bienvenida 77
- Correos electrónicos de notificación 29
- Correos electrónicos procedentes de OPM 103
- Crear lista nueva de contactos 47
- Crear manualmente un usuario nuevo 25
- Crear un duplicado 46
- Crear un usuario nuevo 25
- Crear una lista de contactos externos 47
- Crear usuario nuevo 25, 25, 39
- Crear usuarios 22
- Crear y borrar usuarios 31
- Credenciales de la cuenta Onsite 62
- Credenciales de Onsite 62
- Credenciales SSO 67
- CSV 43, 45, 65, 91, 93, 96, 98, 99, 101
- Cualquiera 99
- Cuántas llamadas 98
- Cube 7, 20
- Cuenta 52
- Cuenta compartida 71, 71, 72, 72, 72
- Cuenta creada 86
- Cuenta de usuario 57
- Cuenta de usuario de Onsite 71
- Cuenta de usuario expira 25, 25, 25
- Cuenta de Workspace 56

- Cuenta eliminada 86
- Cuenta principal SIP 71
- Cuenta registrada 86
- Cuenta registrada (HTML, texto) 103
- Cuenta SIP 71, 72
- Cuentas de Onsite 43
- Cuentas de usuario de Onsite, 40
- Cuentas SIP 72
- CUENTAS SIP 70
- Cuentas SIP comodín 72
- Cumplimiento de la privacidad de los datos 56

D

- Datos anónimos 56
- Datos de autenticación 63
- Datos de autorización 63
- Datos de la marca temporal 57
- Datos personales activos 56
- Departamento 16, 25
- Derecho a ser olvidados (RTBF) 56
- Desactivar la cuenta de usuario invitado cuando se elimine de la lista de contactos 80
- Descarga del cliente en Windows 68
- Descargar 27, 29
- Descargar certificado de SP 63, 70
- Descargar para iOS 28
- Descargar para Windows 28
- Descargar plantilla de importación 40, 46
- Descripción 23, 34, 75, 82, 86, 87, 88, 96
- Desde dirección de correo electrónico 80
- Deshabilitada 84
- Deshabilitar el acceso al directorio global 79
- Destinatario de llamada 100, 101
- Detalles 96
- Detalles de llamada 93
- Detalles del grupo 34
- Devoluciones de llamada HTTP 75
- Dirección 45
- Dirección (SIP) 93
- Dirección de correo electrónico 56, 65, 66
- Dirección de servidor 72, 72
- Dirección de servidor SIP 72
- Dirección IP 91, 100
- Dirección SIP 14, 71
- Direcciones de correo electrónico 29
- Directorio de contactos globales 79
- Directorio global 14, 34, 38, 38, 45, 45, 57, 58, 79
- Disponibilidad de directorio global 38
- Disponible para su uso 105
- Dispositivo habilitado con SIP 45
- Dispositivo móvil 20
- Dispositivos Android 54
- Distribución de Software 77
- DNT 93
- Dominio 21, 22, 43
- Dominio de cuenta Onsite 53
- Dominio de Onsite 62
- Dominio de SIP 72
- Dominio de SIP URI 71, 72, 72, 72
- Dominio de SSO 63
- Dominio del cliente 13, 52
- Dominios de correo electrónico permitidos 61
- Duración 91, 93, 93, 93
- Duración de llamada 99
- Duración del bloqueo de la cuenta 61
- Duración total 93, 98

E

- Editar 19, 87
- Editar grupo 32, 34, 36
- Editar política del cliente 78
- Editar política y permisos del cliente 36
- El acceso a la red no está disponible 62
- El administrador debe aprobar el registro de las cuentas usando la página de autorregistro 61
- El modo de captura ya no está disponible 20
- Elegir configuración 36, 74, 81
- Elemento creado 75
- Elemento eliminado 75
- Elemento modificado 75
- Eliminar contacto de la lista 28
- EmailAddress 39
- Encabezados de columnas 39
- Encabezados HTTP 75
- Endpoint 54, 88
- Endpoint de Onsite 45, 78
- Endpoints de API REST 87
- Endpoints de Onsite 51
- Endpoints de SIP de video de terceros 45
- Endpoints de video externos o de terceros 58
- Endpoints remotos 9
- Enlace del cliente móvil 68
- Enlace SSO 63
- Enlaces de aprovisionamiento de usuario 68
- Entrada de firewall 100
- Entre 99
- Enviar correo electrónico de bienvenida 16
- Enviar correo electrónico de bienvenida a los usuarios nuevos 40
- Enviar correo electrónico de bienvenida si cambia la dirección de correo electrónico 40
- Enviar instrucciones 62, 69
- Enviar una notificación al usuario si cambia la contraseña 40
- Equipos autorizados 73
- Error 96
- Español 103
- Espectador de Onsite Connect 20
- Esquema y host de OPM 28
- Establecimiento de llamada 93
- Estadísticas 93
- Estadísticas de llamadas 55
- Estadísticas de uso 43, 98
- Estadísticas y eventos 93
- Estado 91
- Estado de acceso de superadministrador 52
- Estado de invitación de participante 79
- Estándar abierto 63
- Estilos de botón 105
- Etiquetado de contenido 73
- Etiquetas definidas por el cliente 86
- Europa 56
- Evento 75
- Eventos 56, 75, 96
- Expertos 54
- Expiración 80
- Expiración de cuenta 25, 25
- Expiración de la clave de API 86
- Expiración de la contraseña 59
- Expiración del usuario 53
- Exportar 40, 45, 91, 93, 96, 99, 101
- Exportar contactos externos 45
- Exportar metadatos de SP 63
- Exportar usuarios 43
- ExternalContacts.CSV 46

F

- Fatal 96
- Fecha de creación 34
- Fecha de expiración 25, 86
- Fecha de expiración del cliente 52
- Fecha de finalización 91, 93, 101
- Fecha de inicio 91, 93, 101
- Federación de identidad de usuario 65
- Federación de identidad del usuario 62, 64, 66, 67, 68
- Federación de identidad del USUARIO 65
- FEDERACIÓN DE IDENTIDAD DEL USUARIO 66
- Filtrado 38
- Filtro de directorio global 38, 39
- Filtros de disponibilidad de directorio global 38
- Firewall 54, 71
- Firma digital 70
- Firmar solicitudes de autenticación 63, 64
- Formato SIP URI 45, 45
- Formatos de archivo compatibles 45
- Francés 103
- Frecuencia de lote 75
- Funcionalidad del cliente 53, 54
- Funciones alojadas 53, 55
- Funciones para atravesar el firewall de TeamLink 54
- Fusionar grupos 40

G

- Generación de informes avanzados 55
- General 70
- Generar automáticamente el nombre de usuario 67
- Generar clave 86
- Generar contraseña temporal 16
- Generar un informe 99
- Grabación 106
- Grabación de control 54
- Grabaciones 19, 105
- Grabaciones capturadas 20
- GroupMembership 39
- Grupo 39, 81, 82
- Grupo de asignación automática 71
- Grupo de licencia única 21
- Grupo de licencias 22, 23, 40
- Grupo de licencias de dominio 16, 25
- Grupo de licencias para usuarios nuevos 40
- Grupo de licencias predeterminada 21
- Grupo de política 23, 25, 25, 25, 31, 78
- Grupo de política de dominio 16
- Grupo de política del administrador del cliente 25
- Grupo de políticas del cliente 25
- Grupo de todos los usuarios 21
- Grupo nuevo 23
- Grupo SIP 72, 72
- Grupo SIP de asignación automática 25
- Grupos 98, 99
- Grupos de licencia 25, 31, 53
- Grupos de licencia personalizados 22
- Grupos de política 25
- Guardar 51
- Guía de Webhooks de Onsite Workspace 75
- Guías de API de Onsite 87

H

- Habilitada 79, 84
- Habilitar el acceso a Workspace 74
- Habilitar el autorregistro 61
- Hacer llamadas 19
- Hardware 93

- Heredar 36, 78, 82, 83
- Historial de llamadas 98
- Hora 96
- Hora de inicio 93, 93
- Hora de inicio de sesión 91
- Hora reportada 93
- Hora universal coordinada (UTC) 57
- Host y ruta de acceso de OPM 28
- HTTPS 9, 9, 57
- Hub 7, 20
- Hub de Collaboration 77, 77
- Hub de Onsite Collaboration 77
- Huella digital SHA1 70

I

- ID de sesión SIP 93
- ID de SSO federado 16, 40, 65, 65, 66
- ID del nombre del sujeto 65
- Identificación de la entidad 63, 63, 64
- Idioma 16, 25
- Idioma predeterminado 57
- Imágenes 19
- Imágenes capturadas 20
- Implementar certificados del servidor 70
- Implementar paquetes de actualización 77
- Importación de metadatos 63
- Importar 40, 45, 46, 46
- Importar desde archivo 46
- Importar metadatos IdP 63
- Importar plantilla 40, 40
- Importar resultados 40, 46
- Importar una plantilla de importación de usuarios 40
- Importar usuarios 40, 46
- Importar usuarios desde un archivo 25
- Imprimir 101
- Incluir la opción para que el invitado llame al anfitrión inmediatamente 80
- Incluir registros anónimos 99
- Información 96
- Información de la cuenta SIP 72
- Información de la cuenta SIP Enterprise 72
- Información Personal Identificable (PII) 56
- Informe de actividad del cliente 91
- Informe de ejecución 99
- Informe de eventos 96
- Informe del mapa térmico 101
- Informe del usuario exportado 59
- Informes 98, 99
- Informes avanzados 73
- Informes de llamadas 98
- Informes de OPM y estadísticas de llamadas 56
- Inglés 103
- Inglés únicamente 103
- Iniciar sesión 14, 20, 29, 51, 101, 105, 106
- Iniciar sesión en administración de OPM 9
- Iniciar sesión en Onsite Connect 28, 28
- Iniciar sesión por primera vez 9
- Inicio de sesión del cliente SSO 68
- Inicio de sesión sin conexión 62
- Inicio de sesión único 62, 62
- Inicio de sesión único (SSO) 16
- Inicio de transmisión 93
- Insertar plantilla predeterminada 86
- Instalar 27, 29
- Instrucciones de importación de CSV 45
- Instrucciones habilitadas para SSO 86
- Inteligencia artificial (IA) 55

- Interfaces de programación de aplicaciones (API) 54
- Interfaz de red 93
- Interfaz del servicio web 9
- Internet de las cosas (IoT) 56
- Internet público 100
- Interno 71
- Invitación de invitado externo 86
- Invitación de usuario participante (HTML, texto, SMS) 103
- Invitaciones de participante externos 77
- Invitaciones de participantes por SMS 85
- Invitados 59
- Invitados externos 31
- Invitar a un participante externo 51
- iOS 77, 83
- iOS App Store 28
- iPhone 7
- Italiano 103

J

- Japonés 103

L

- Latitud de llamada 93
- Lectura 86
- Lenguaje de marcado de aserción de seguridad (SAML) 62
- Licencia Contributor 73
- Licencia Enterprise 73
- Licencia individual 19
- Licencia maestra 31
- Licencia múltiple 19
- Licencia Workspace Enterprise 73
- Licencias 13, 51, 52, 53, 54, 54, 61
- Licencias de Connect Enterprise 16
- Licencias de Onsite Connect Endpoint 13
- Licencias de usuario 19
- Licencias disponibles 22
- Licencias disponibles de Connect Enterprise 11
- Licencias disponibles de Workspace Enterprise 11
- Licencias totales de Connect Enterprise 11
- Licencias totales de Workspace Contributor 11
- Licencias totales de Workspace Enterprise 11
- Licencias totales y disponibles 11
- Líderes potenciales 98
- Límite 93
- Límite de 160 caracteres 79
- Lista de contactos 58
- Lista de contactos externos 45, 46, 48
- Lista de usuarios importados 65
- Lista de valores separados por comas 61
- Lista nueva 45, 47
- Listas de contactos 21, 45
- Llamada 101
- Llamada en Onsite 20
- Llamadas 93
- Llamadas multiusuario 54
- Local 9, 9, 11, 52, 54, 70, 75, 77
- Local: guía de instalación 70
- Longitud máxima de mensaje SMS a usuario 79
- Longitud mínima 60
- Los contactos externos son públicos de forma predeterminada 58
- Los datos anónimos no son reversibles 56

M

- Manejo de duplicado 46
- Manuales y guías de OPM 83
- Mapa térmico 100
- Mapa térmico para 101

Marco 93
Mayor o igual 99
Mecanismo de notificaciones por Webhooks 75
Medios 54
Mejorar los datos de los informes 59
Membresía de grupo 78
Membresía de grupo de licencias 25, 25
Membresía de grupo de política 25, 40
Menor o igual 99
Mensaje 105
Mensaje de bienvenida 28
Mensaje SMS 79
Mensajes personalizados 55, 105, 105, 106
Metadatos IdP 63, 63
Método de activación de la cuenta 61
Mi perfil 13
Microsoft Excel 40
Miembro de 40
Miembros individuales 39
Modificar grupo 34, 35, 36, 74
Modificar usuarios 31
Modo campo 54, 80
Modo de captura 20
Modo de cifrado 80
Modo experto 54, 80
Modo importar 40
Modo usuario (experto/campo) 54
Motivo de terminación 93, 93

N

Negar 36, 82, 83
Negar acceso de superadministrador 52
Ninguno 86
No mostrar de nuevo 105
Nombre 16, 23, 25, 34, 39, 43, 45, 47, 67, 75, 86, 87, 88, 93
Nombre de autenticación 72, 72
Nombre de autenticación único 72
Nombre de dominio Onsign 63
Nombre de host 91
Nombre de identificación 65
Nombre de informe 99
Nombre de la empresa 22
Nombre de usuario 9, 16, 28, 32, 39, 43, 56, 65, 65, 67, 93
Nombre de usuario de autenticación 72
Nombre de usuario/ 75
Nombre del atributo 66, 66, 67
Nombre del campo personalizado 59
Notificación 11, 61, 67
Notificaciones de liberación nueva 77
Notificaciones del sistema 39
Notificar a los administradores por correo electrónico cuando se registre una cuenta 67
Notificar a los usuarios existentes 69, 69
Número de licencias por tipo 53
Número de resultados 99

O

OamClientWebService 28, 28
Obligatorio 62
Olvidó la contraseña 103
Omitir duplicados 46
Omitir duplicados (mantener registros existentes) 40
Onsight 5000HD 77
Onsight Connect 43, 62
Onsight Connect para Windows 103
Onsight Cube 77, 77
Onsight Platform Manager: guía de instalación 77
Onsight Workspace 73

Opcional 29, 62
Opciones de licencia 19
Opciones de mensaje 105
Opciones para configurar el servidor SIP 71
OpenOffice Calc 40
OPM.com\user@domain 28

P

Página autorregistro 43
Página Autorregistro 29
Página de actualizaciones de software 77
Página de confirmación de la verificación del correo electrónico 43
Página de contactos externos 46
Página web de autorregistro 25
País 16, 25, 25, 98, 99
Pantalla de control 11, 13, 13, 19
Parámetros 88
Parámetros del filtro 91, 91, 93, 96, 96, 98, 99, 100
Participante al que se llama 93
Participante que llama 93
PC con Windows 7, 20, 54, 83
Pérdida de conectividad a la red 51
Perfil 16, 25, 29, 59
Perfil de configuración de IA 88, 88
Perfiles de configuración de IA 88
Período de retención de datos (DRP) 56, 98
Permisos de administrador de grupo 31
Permisos de grupo 31
Permisos de los usuarios invitados externos 51
Permisos de usuario estándar 31
Permisos del cliente 21, 23, 31, 34, 36, 55, 78, 82, 83, 83, 84
Permisos del cliente de grupo 83
Permitir 36, 82, 83, 84
Permitir a los usuarios invitar a participantes 31
Permitir a los usuarios que inviten a participantes externos 79
Permitir configurar el Modo de usuario al invitar al invitado 80
Permitir contacto nuevo 25
Permitir el uso de datos celulares/móviles 74
Permitir invitaciones de participante por mensaje de texto 79
Persona que llama 100, 101
Personalización 55, 86
Personalización de correo electrónico 86
Personalización de SMS 86
Personas 73
Plantilla de importación de usuarios 40
Política de contraseña 59, 60
Política de inicio de sesión 59, 61
Política de seguridad de Enterprise 9
Política del cliente 21, 21, 22, 23, 25, 31, 31, 34, 36, 51, 54, 54, 55, 58, 60, 74, 78, 80, 81, 82, 83, 84, 85, 105, 106
POLÍTICA DEL CLIENTE 81
Política del cliente de grupo 74, 83
Política del cliente de usuario 78, 78, 78
Portal del cliente 70
Portugués (Portugal y Brasil) 103
Precedencia 78
Precedencia de políticas 80
Predeterminada 79
Privacidad de contenido 54, 54
Privacidad de video 84
Privacidad de video remoto 84
Privado 38, 47, 71, 72
Private SIP Server settings 39
Privilegios de administración 31
Privilegios de administrador de Onsight Platform Manager 53
Procesamiento natural del idioma (NLP) 55

Promedio de duración 98
Promoción de un usuario estándar 32
Propietario de cuenta 13, 13, 29, 52, 53, 53, 62
Protocolo de inicio de sesión (SIP) 7, 14, 70
Protocolo de red HTTPS 9
Proveedor celular 93
Proveedor de identidad (IdP) 62, 63
Proveedor de identificación de SSO 63, 63
Proveedor de identificación SSO (IdP) 63
Proveedor de servicio (SP) 63, 63
Proveedor de servicio de socio 63
Proveedor de servicio local 63
Proxy web 9
Público 38, 47, 71, 72
Puertos SIP 54

R

Rechazar 84
Recopilación de datos de Workspace 73
Recordarme 28
Recuento de conexiones del cliente 100
Red cableada 9
Red inalámbrica 9
Reenviar el correo electrónico de bienvenida 29
Reenviar el mensaje de bienvenida 27
Región 16, 25
Registrar una cuenta 43, 103
Registro de evento 96, 96
Registro de TeamLink 54
Reglamento General de Protección de Datos (RGPD) 56
Requerimiento de correo electrónico 29
Requerimientos de red 9
Requerir aserciones cifradas 63, 64
Requerir aserciones firmadas 64
Requerir dirección de correo electrónico para cuentas autorregistradas 29, 61, 67
Requerir respuestas firmadas 63
Requerir respuestas firmadas. 64
Requisitos de pista de auditoría 73
Resolución 93
Resolución de problemas 52
Restablecer contraseña 103
Restablecer los cambios 51
Restringir el acceso a la carpeta de carga al propietario 74
Resultados 98
Resumen de invitación de participante 99
Resumen de licencia y uso general 98
Resumen de uso de licencia 99
Resumen de uso general 99
Rojo 79
Ruso 103
Ruta de carga 74

S

Salas de reuniones de WebEx 85
Salas de videoconferencias 45
SampleUserImport.csv 40
Sección de categoría 81
Sección de usuarios de Onsight 53
Seguridad 51, 59, 60, 61, 71
Seleccionar todas las filas 69
Servicio de mensaje de texto 85
Servicio de SIP alojado 72
Servicio en línea 51
servicio por suscripción 7
Servicios de IoT 56, 88
Servicios de llamada 51
Servicios de llamada en Onsight 19

Servidor de Workspace 73
Servidor privado 71, 72
Servidor público 71, 72, 72
Servidor SIP 71, 72, 72
Servidor SIP de Enterprise 71, 72, 72
Severidad 96
Si se configura un correo electrónico válido 29
Siguiendo actualización 73
Siguiendo inicio de sesión 73
SIP 25, 51, 54, 85
SIP URI 14, 72
SIP URI único 72
Sistema operativo 93, 93
Sistemas de gestión interna 73
SMS 55, 55, 62, 85
Sobrescribir grupos 40
Software 51
Solicitar 29
Solicitar en el primer inicio de sesión 67
Solicitud de restablecimiento de contraseña 86
Solicitud de restablecimiento de contraseña (texto, SMS) 103
Solicitudes remotas de uso compartido de video 84
Solo el host de OPM 28
Soporte de Librestream 52
Soporte de llamadas de Librestream 52
SSO 39, 40, 55, 62, 62, 64, 65, 65, 66, 66, 67, 68, 69, 103
Sueco 103
Superadministradores 52

T

Tabletas 103
Tasa de bits de video 93
Tasa máxima de bits de video 54
TCP 9, 71, 72, 72, 72
TeamLink 54, 93
Teléfono inteligente Android 83
Teléfonos inteligentes 103
Telestración 7
Tendencias históricas 98
Tiendas de aplicaciones 77, 77
Tipo de autenticación predeterminada 72
Tipo de cuenta 25, 31
Tipo de dispositivo 93
Tipo de enlace de inicio de sesión 64
Tipo de grupo 23
Tipo de grupo de asignación 72
Tipo de grupo de cuenta 72
Tipo de licencia 25
Tipo de membresía 34
Tipo de participante 101
Tipo de transporte predeterminado 72
Tipos de cuenta y permisos de usuario 31
Tipos de licencia 21, 40
Tipos de licencia de Workspace 19
Título 105
TLS 71, 72, 72, 72
Todo 38, 91
Todos los contactos 47, 47
Todos los países 99
Todos los usuarios 78, 80, 99, 99
Torres de telefonía móvil 100
Totales de licencia 34
Traductor Onsight 55
Transmisión de datos HTTPS 54
Tutorías/Capacitación 98

U

Ubicación y cantidad de llamadas/inicios de sesión 101

Un URI absoluto 28
URI 72
URI del consumidor 75
URL 9, 61
URL de ACS 63
URL de autorregistro 61
URL de inicio de sesión único 64
URL de Onsite Platform Manager 28
URL SSO 63
user@domain.com 9
user@sipdomain.com 14
Uso compartido de video 84
Uso máximo 99, 99, 99
Uso máximo o mínimo 98
Uso mínimo 99, 99, 99
Usuario 91, 96
Usuario al que se llama 93
Usuario Enterprise 19
Usuario estándar 25, 31, 31, 32
Usuario nuevo 16, 25, 25
Usuario que llama 93
Usuario y grupos 73
Usuarios 11, 16, 23, 25, 25, 43, 57
USUARIOS 32
Usuarios activos 11
Usuarios anónimos 91, 93
Usuarios de API 96
Usuarios de Enterprise 40
Usuarios de Onsite 53
Usuarios de SSO 29
Usuarios de Windows 77
Usuarios en espera de aprobación de un administrador 11
Usuarios estándar 62, 91, 93, 96, 99
Usuarios expirados 11
Usuarios invitados 29
Usuarios invitados externos 11, 51, 53, 57, 58, 62, 79, 81, 86,
91, 96, 99
Usuarios Invitados externos 93
Usuarios totales 11
Usuarios y grupos 58
Utilizar siempre TeamLink 54

V

Valor 36
Valor del campo personalizado 59
Valores predeterminados de invitación de invitado externo 80
Varias cuentas 71, 71, 72, 72, 72
Varias cuentas de administrador 13
Varias cuentas SIP 72
Varios grupos 78
Varios participantes 54
Velocidad máxima de bits de carga (Kbps) 74
Ver datos 73
Ver grabaciones 73
Ver imágenes 73
Verde 79
Verifique su dirección de correo electrónico 43
Versión 91
Versión específica 77
Video de terceros Endpoint 7
Visión de la computadora (CV) 55
Visualización 56
Visualización de los instrumentos 56
Visualizar informe 46
Volver a autenticarse 51

W

Windows 77, 77, 77, 103

Workspace 20, 86
Workspace Contributor 19, 25, 40, 53
Workspace Contributor) 19
Workspace Enterprise 19, 19, 25, 40, 53
Workspace Webhooks 75

Z

Zona horaria predeterminada 57