



# Onsight Platform Manager

## Guia do administrador

# Copyright

## Guia do Onsight Platform Manager

**Doc nº: 400199-24 Rev: F**

Fevereiro de 2022 (v11.4.7)

As informações neste documento estão sujeitas a alterações sem aviso prévio. A reprodução de qualquer forma sem a permissão por escrito da Librestream é estritamente proibida.

### **Aviso de direitos autorais:**

Copyright 2004-2022 Librestream Technologies Incorporated. Todos os direitos reservados.

### **Aviso de patentes:**

Patente dos Estados Unidos nº 7.221.386, juntamente com patentes adicionais pendentes no Canadá, nos Estados Unidos e em outros países, todas em nome da Librestream Technologies Inc.

### **Aviso de marca registrada:**

Librestream, o logotipo Librestream, Onsight, o logotipo Onsight, Onsight Connect, Onsight Flow, Onsight Workspace, Onsight Cube, Onsight Collaboration Hub, Onsight Smartcam, Onsight Platform Manager e Onsight Teamlink são marcas registradas ou marcas comerciais da Librestream Technologies Incorporated no Canadá, nos Estados Unidos, na União Europeia e/ou em outros países. Todas as outras marcas registradas são de propriedade de seus respectivos proprietários.

# Índice

Copyright.....	ii
<b>1. VISÃO GERAL.....</b>	<b>7</b>
1.1. Arquitetura da plataforma de realidade aumentada do Onsite.....	7
<b>2. REQUISITOS DE REDE.....</b>	<b>9</b>
2.1. Configuração de firewall.....	9
2.2. No local.....	9
2.3. Primeiro logon no OPM.....	9
<b>3. PAINEL.....</b>	<b>11</b>
<b>4. CONFIGURAÇÕES DO ADMINISTRADOR.....</b>	<b>13</b>
4.1. Alteração da senha do administrador.....	13
4.2. Alteração dos contatos pessoais do administrador.....	14
4.3. Adição de administradores ao OPM.....	16
<b>5. LICENÇAS DE USUÁRIO.....</b>	<b>19</b>
5.1. Opções de licença.....	19
5.2. Modo de captura.....	20
<b>6. GERENCIAR USUÁRIOS E GRUPOS.....</b>	<b>21</b>
6.1. Gerenciamento de licenças e políticas de domínio.....	21
6.2. Gerenciamento de grupos de licenças.....	22
6.3. Gerenciamento de usuários e grupos de licenças/políticas.....	22
6.4. Adição de um grupo.....	23
<b>7. USUÁRIOS E GRUPOS.....</b>	<b>25</b>
7.1. Criar novo usuário.....	25
7.1.1. Criação de um novo usuário.....	25
7.2. E-mail de boas-vindas.....	27
7.2.1. E-mail de boas-vindas no local.....	28
7.2.2. Formatos de URL no local.....	28
7.3. Requisito de e-mail do usuário.....	29
7.4. Tipos e permissões de conta de usuário.....	31
7.5. Promoção de usuários e atribuição de um administrador de grupo.....	31
7.6. Editar grupos.....	34
7.6.1. Adicionar/Remover membros do grupo.....	34
7.6.2. Atribuição de administradores de grupo.....	35
7.6.3. Editar a política do cliente e as permissões.....	36
7.6.4. Diretório global.....	38
7.7. Importar/exportar usuários.....	39
7.7.1. Criação de um modelo de importação de usuários.....	40
7.7.2. Importação de usuários.....	40
7.8. Exportar usuários.....	43
7.9. Autorregistro de usuários.....	43
<b>8. CONTATOS EXTERNOS.....</b>	<b>45</b>
8.1. Adição manual de um contato externo ao diretório global.....	45
8.2. Importação de uma lista de contatos externos.....	46
8.3. Adicionar uma lista de contatos externos.....	47
8.4. Adicionar/Remover contatos externos de listas.....	48

<b>9. CONFIGURAÇÕES.....</b>	<b>51</b>
9.1. Tempo limite de autenticação.....	51
9.2. Conta.....	52
9.2.1. Acesso de superadministrador.....	52
9.2.2. Alterar proprietário da conta.....	53
9.2.3. Licenças.....	53
9.2.4. Anonimização de dados.....	56
9.2.5. Anonimização programada.....	56
9.3. Usuários.....	57
9.3.1. Contas de usuário.....	57
9.3.2. Usuários convidados externos.....	58
9.3.3. Diretório global.....	58
9.3.4. Campos personalizados.....	59
9.4. Segurança.....	59
9.4.1. Política de senhas.....	60
9.4.2. Expiração de senha.....	60
9.4.3. Política de logon.....	60
9.4.4. Autorregistro.....	60
9.5. Logon único.....	61
9.5.1. Logon único.....	61
9.5.2. Configuração do Security Assertion Markup Language.....	62
9.5.3. Federação da identidade do usuário.....	64
9.5.4. Autorregistro de SSO.....	67
9.5.5. Links de provisionamento de usuários.....	68
9.5.6. Notificar usuários existentes.....	69
9.5.7. No local — Configuração do certificado SSO.....	69
9.6. Protocolo de início de sessão.....	70
9.6.1. Configurações de SIP.....	70
9.6.2. Conta SIP.....	71
9.7. Onsite Workspace.....	73
9.7.1. Habilitação do acesso dos usuários ao Workspace.....	73
9.8. Webhooks do Workspace.....	75
9.8.1. Criação e modificação da configuração de um Webhook.....	75
9.9. Atualizações de software.....	76
9.9.1. Onsite Connect para Windows.....	77
9.9.2. Notificações de novos lançamentos.....	77
9.9.3. Atualizações no Onsite Cube, Collaboration Hub e 5000HD.....	77
9.9.4. Atualizações de software no local.....	77
9.10. Política do cliente e Permissões.....	77
9.10.1. Usuários convidados externos.....	78
9.10.2. Padrões de convite para convidados externos.....	79
9.10.3. Precedência da política.....	80
9.10.4. Política e permissões de cliente do grupo.....	83
9.10.5. Privacidade de vídeo remoto.....	84
9.10.6. Compatibilidade com WebEx CMR.....	85
9.11. Serviço de mensagens curtas.....	85
9.12. Personalização.....	86

9.13. Chaves de interface de programação de aplicativos.....	86
9.13.1. Chave gerada pela API.....	87
9.14. Configurações de inteligência artificial.....	87
<b>10. ESTATÍSTICAS E EVENTOS.....</b>	<b>89</b>
10.1. Atividade do cliente.....	89
10.1.1. Geração de um relatório de atividades do cliente.....	89
10.2. Estatísticas.....	91
10.2.1. Geração de um relatório estatístico.....	91
10.3. Eventos.....	94
10.3.1. Geração de um relatório de eventos.....	94
10.4. Relatórios.....	96
10.4.1. Geração de um relatório.....	96
10.5. Mapas de calor.....	98
10.5.1. Geração de um relatório de mapa de calor.....	98
<b>11. SUPORTE A IDIOMAS.....</b>	<b>101</b>
<b>12. MENSAGENS PERSONALIZADAS.....</b>	<b>103</b>
12.1. Criação de uma mensagem personalizada (formulário).....	103
12.2. Mensagens personalizadas e política do cliente.....	104
12.2.1. Modificação da política do cliente para suporte a mensagens personalizadas.....	104
<b>13. CONTRATO DE LICENÇA DE USUÁRIO FINAL.....</b>	<b>105</b>
<b>14. CONTATO COM O SUPORTE.....</b>	<b>107</b>
<b>APPENDICES.....</b>	<b>109</b>
Precedência de prioridade e política do cliente.....	109
Práticas recomendadas.....	114
15.2.1. Conta — Práticas recomendadas.....	114
15.2.2. Usuários — Práticas Recomendadas.....	116
15.2.3. Segurança — Práticas recomendadas.....	117
15.2.4. Software — Práticas recomendadas.....	119
15.2.5. Política do cliente — Práticas recomendadas.....	120
15.2.6. Permissões do cliente — Práticas recomendadas.....	133
Índice Remissivo.....	a



# 1. VISÃO GERAL

O Onsight Platform Manager (OPM) é uma ferramenta on-line segura para gerenciamento centralizado de usuários. Os administradores do sistema podem gerenciar licenças de usuário do Onsight, listas de contatos e grupos, além de configurar políticas e permissões de grupos de usuários. Usando o OPM, os administradores podem gerenciar e manter grupos de usuários Onsight de forma eficiente.

O OPM fornece ferramentas para:

1. **Criar e gerenciar contas de usuário** — os administradores do OPM podem criar usuários, grupos de políticas, grupos de licenças e políticas, além de permissões de clientes.
2. **Gerenciamento de licenças** — os administradores do OPM podem visualizar e gerenciar o status de seus pools de licenças, incluindo:
  - **Connect Enterprise** — fornece serviços de chamada do Onsight Connect. Nas versões anteriores do OPM (v9 e anteriores), isso era referido como licença de usuário do Onsight. **Connect Enterprise** é equivalente à licença de usuário do Onsight.
  - **Workspace Enterprise** — fornece ao usuário acesso ao Workspace com base em permissões atribuídas pelo administrador. Fazer upload, exibir, compartilhar e analisar dados, imagens e gravações entre equipes internas. Nas versões anteriores do OPM (v9 e anteriores), essa era uma configuração de domínio que foi habilitada para fornecer acesso ao Workspace a todos os usuários. Agora é gerenciada por atribuições de licença de usuário.
  - **Workspace Contributor** — fornece ao usuário acesso pelo **Workspace** à sua pasta de upload; o acesso a outros ativos não pode ser concedido. Centraliza com segurança o conteúdo de clientes, fornecedores e colaboradores terceirizados para análise.
3. **Configurar políticas e permissões do cliente** — as **Client Policies** e **Permissions** são aplicadas a um ponto de extremidade do Onsight quando o usuário faz logon.
4. **Gerar relatórios avançados** — a revisão regular das estatísticas de uso, inclusive quem fez logon no software, quantas chamadas uma pessoa fez e recebeu, além da duração total e média das chamadas, indicará o nível de adoção da tecnologia.

As tarefas descritas são tarefas de nível de administração e não são destinadas aos usuários finais do Onsight Connect. Muitas das tarefas que envolvem a configuração de **Client Policy** e **Permissions** afetam a capacidade de funcionamento do ponto de extremidade.

## 1.1. Arquitetura da plataforma de realidade aumentada do Onsight

A plataforma de realidade aumentada do Onsight é um serviço baseado em assinatura gerenciado centralmente. Um usuário autorizado pode fazer logon em um cliente Onsight Connect em um PC Windows, iPhone, iPad e conectar-se a dispositivos Onsight, como Cube ou Hub.

Uma vez conectado, um usuário do Onsight Connect pode visualizar e compartilhar com segurança vídeos, imagens, áudios e telestrações com outro usuário do Onsight. Ele também pode compartilhar áudio e vídeo com um ponto de extremidade de vídeo de terceiros que aceita o protocolo de início de sessão (SIP). Para obter mais informações sobre os recursos completos do Onsight Connect, analise a documentação on-line em [www.librestream.com/support/](http://www.librestream.com/support/).



## 2. REQUISITOS DE REDE

O software Onsight requer o protocolo de rede HTTPS para se comunicar com o Onsight Platform Manager.

**Tabela 2-1 Requisitos de rede**

<b>HTTPS:</b>	443
<b>Web Proxy:</b>	Conforme definido pela política de segurança da sua empresa
<b>Wireless Network:</b>	802.11 a/b/g/n
<b>Wired Network:</b>	Recomenda-se uma porta Ethernet 10/100 com fio.

### 2.1. Configuração de firewall

Se o Windows Firewall ou outro software de firewall de terceiros estiver sendo executado na rede onde você está tentando acessar o Onsight Platform Manager, pode ser necessário adicionar exceções de firewall para as portas listadas na Tabela 1.

**Tabela 2-2 Configuração de firewall**

Nome	Protocolo	Porta	Descrição
HTTPS	TCP	443	Obrigatório se os pontos de extremidade remotos acessarem o servidor de pacote ou a interface do serviço Web por HTTPS. Se a configuração de IIS usar uma porta diferente de 443, certifique-se de que você tenha dado permissão a essa porta.

### 2.2. No local

Ao longo deste documento, as informações que se aplicam apenas às instalações locais estão contidas nas seções No local.

### 2.3. Primeiro logon no OPM

Você receberá suas informações de logon de administração do OPM da Librestream em um e-mail de boas-vindas.

Para fazer logon no OPM, abra um navegador e navegue até: <https://onsight.librestream.com>. Digite o nome de usuário e a senha recebidos no e-mail de boas-vindas:

**Tabela 2-3 Nome de usuário e senha**

<b>User Name:</b>	user@domain.com
<b>Password:</b>	Senha

Para evitar acesso não autorizado ao software, você deve alterar essa senha imediatamente após o primeiro logon, conforme descrito em [Alteração da senha do administrador \(na página 13\)](#).

Depois de fazer logon, você será levado para o painel.

 **Nota:** no local — a URL do seu servidor OPM vai depender da URL do servidor atribuída durante a instalação. Consulte o guia de instalação no local.



## 3. PAINEL

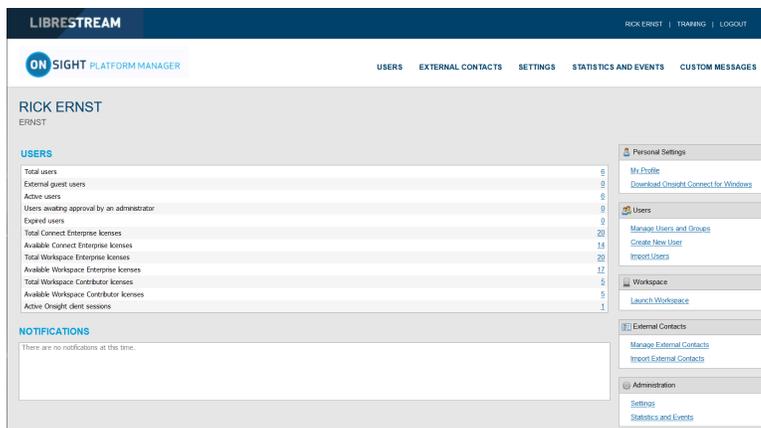


Figura 3-1 Painel

A página de painel inclui uma seção **USERS** e **NOTIFICATION**, além de uma lista de links.

### USUÁRIOS

A seção USERS contém uma tabela que exibe tipos de usuários, licenças e informações relacionadas:

#### Total Users

O número total de todos os usuários (ativos e expirados) no domínio.

#### External Guest Users

O número total de contas de convidados externos ativos.

#### On Premises

Os usuários convidados externos não são aceitos pelas instalações no local.

#### Active Users

O número total de usuários ativos no domínio.

#### Users Awaiting Approval by an administrator

O número total de usuários autorregistrados aguardando aprovação do administrador. (Consulte Autorregistro para obter detalhes.)

#### Expired Users

O número total de contas de usuários expirados.

#### Total and Available Licenses

Na lista, aparecem as licenças totais e as disponíveis para cada tipo:

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



# 4. CONFIGURAÇÕES DO ADMINISTRADOR

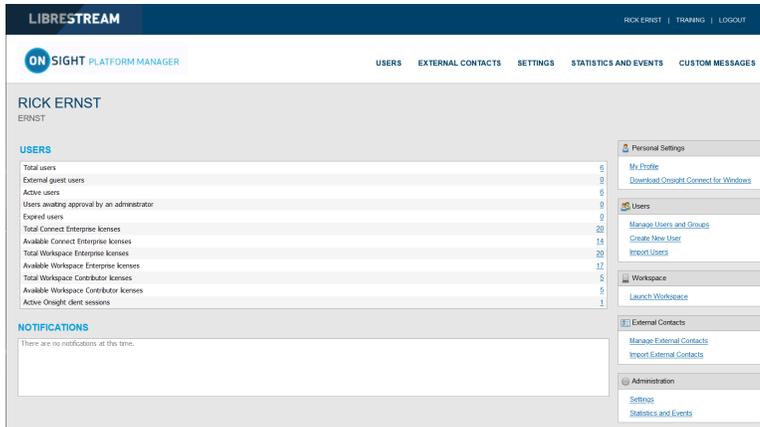


Figura 4-1 Painel

O proprietário da conta é o administrador principal. O administrador não consome nenhuma licença de ponto de extremidade do OnSight Connect; portanto, para fazer logon em um cliente OnSight Connect como usuário, você deve atribuir uma licença de cliente ao seu proprietário da conta.

Quando estiver conectado ao OPM, localize  **Personal Settings** para acessar **My Profile**. Meu perfil permite que o administrador defina suas configurações pessoais como qualquer outra conta de usuário, incluindo a atribuição de licenças. Uma vez que as licenças são atribuídas à conta, o administrador também pode fazer logon em um cliente OnSight Connect e usar os recursos fornecidos pelo tipo de licença.

Os administradores não precisam ter licenças atribuídas para gerenciar seu domínio de cliente do OPM. Você pode criar várias contas de administrador.

## 4.1. Alteração da senha do administrador

1. Faça logon no OPM e acesse seu painel.

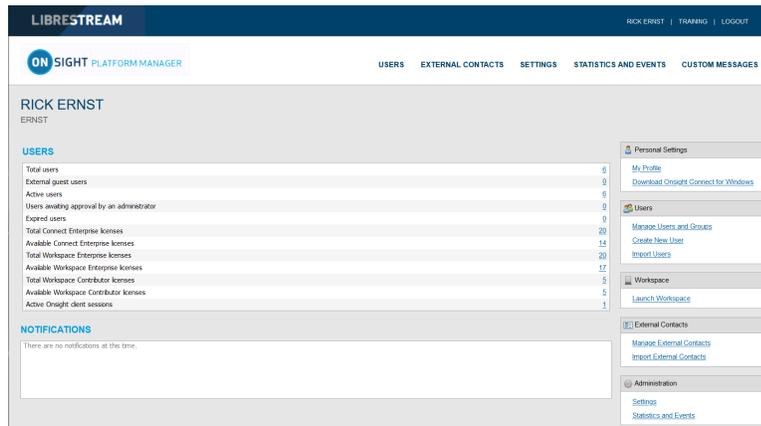
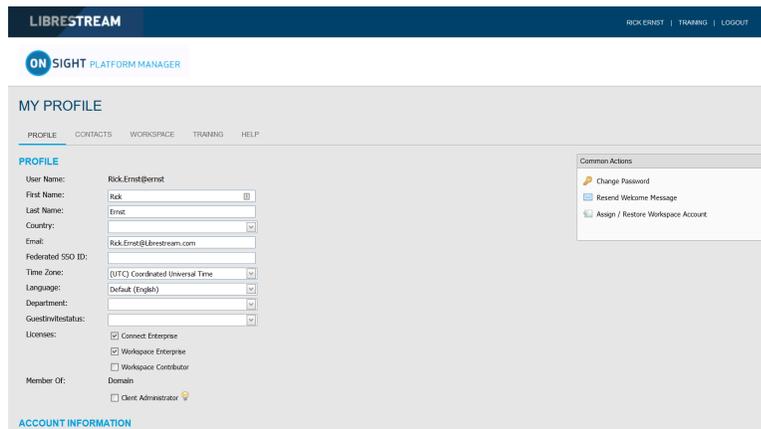


Figura 4-2 Painel

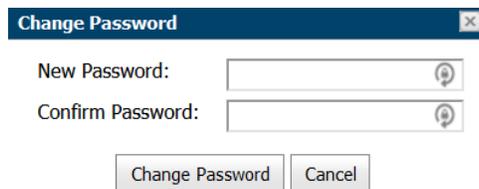
2. Localize  **Personal Settings** à direita e selecione **My Profile**. Isso irá levá-lo para a página de configuração **My Profile**.



**Figura 4-3 Meu perfil**

3. Localize **Common Actions** à direita e selecione  **Change Password**. Informe a nova senha em ambos os campos fornecidos.

 **Nota:** a sua senha deve ser diferente da atual.



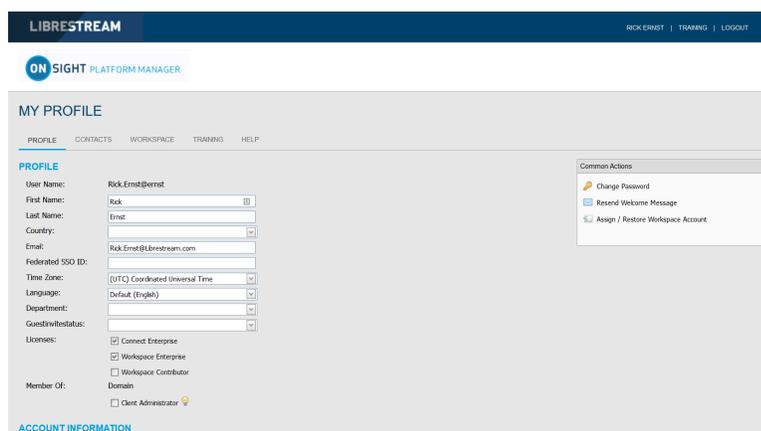
**Figura 4-4 Alterar senha**

4. Clique no botão **Change Password** para salvar suas alterações. Isso conclui o procedimento.

## 4.2. Alteração dos contatos pessoais do administrador

Faça login no OPM.

1. Localize  **Personal Settings** e selecione **My Profile**.



**Figura 4-5 Meu perfil**

2. Selecione a guia **CONTACTS**.

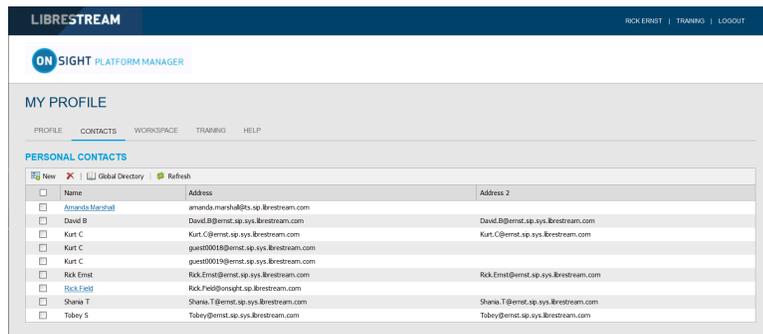


Figura 4-6 Meus contatos

- Clique no ícone **Global Directory** para procurar um contato a ser adicionado à sua lista **Contacts**.

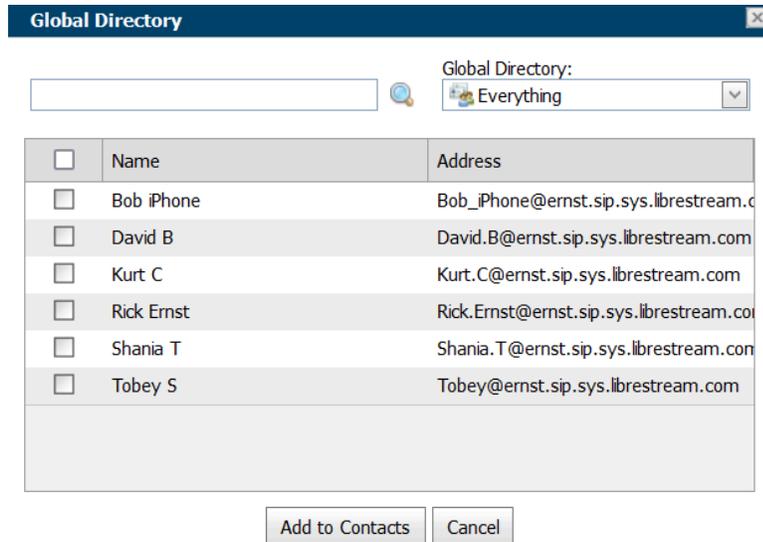


Figura 4-7 Diretório global

- Informe um nome para pesquisar e pressione o ícone **Search** para ver uma lista de todos os usuários.
- Ative a caixa de seleção ao lado do nome da pessoa e clique em **Add to Contacts**.
- Para criar um contato manualmente, clique no ícone **New Contact**. Isso só será necessário se você precisar adicionar um contato terceirizado.

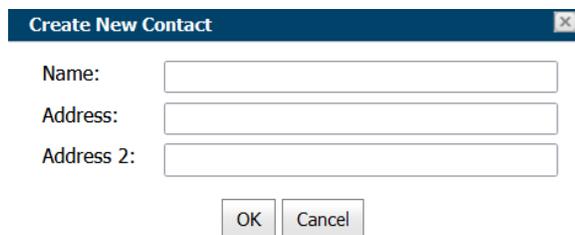


Figura 4-8 Criar novo contato

- Informe **Name** e o protocolo de início de sessão (SIP) no campo **Address** do contato. Você também pode informar um **Address 2** opcional.

**Nota:** o endereço deve estar no formato SIP URI, por exemplo, **user@sipdomain.com**.

- Clique em **OK** para salvar. Isso conclui o procedimento.

## 4.3. Adição de administradores ao OPM

Você deve fazer logon no OPM.

Para adicionar usuários, você precisará:

1. Selecionar **USERS** no menu principal. A página USERS é exibida.

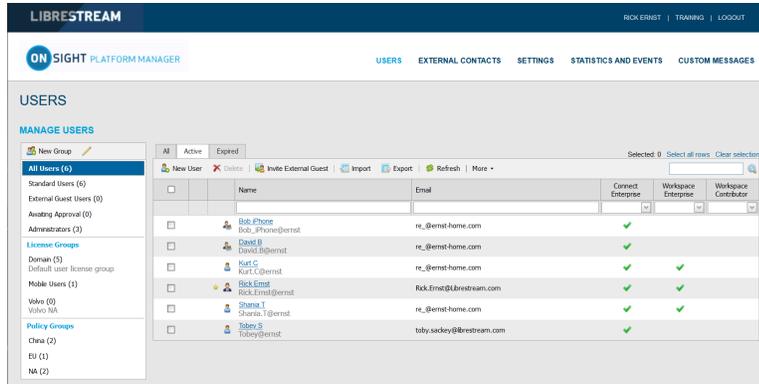


Figura 4-9 USUÁRIOS

2. Clique no ícone  **New User**. A página CREATE NEW USER é exibida.

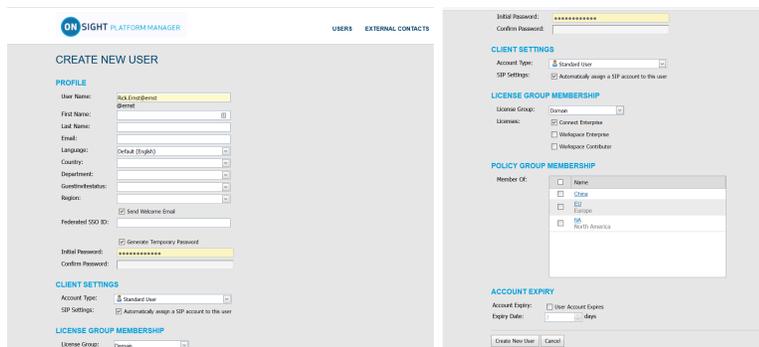


Figura 4-10 Criar novo usuário

3. Apresente as informações de **PROFILE** que incluem:

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



**Nota:** **Send Welcome Email** e **Generate Temporary Password** estão selecionados por padrão. Se você escolher não enviar o e-mail de boas-vindas, é recomendável também desabilitar **Generate Temporary Password**. Você precisará notificar os novos administradores sobre seus nomes de usuário e senhas.

- e. Defina **Language**, **Country**, **Department** e **Region** usando os menus suspensos, conforme necessário.

- f. Se **Single Sign On** estiver habilitado, informe o **Federated SSO ID** (se necessário). Consulte a seção **SSO** para obter detalhes.

4. Em **CLIENT SETTINGS**, selecione **Administrator** para **Account Type**.

5. Verifique se a opção **Automatically assign a SIP account to this user** está habilitada por padrão.



**Nota:** isso é obrigatório se você está atribuindo uma licença Connect Enterprise e quer que seus administradores consigam fazer logon localmente em um cliente Onsight e fazer chamadas.

6. Por padrão, o **Administrator** vai pertencer ao grupo de **licenças de domínio**. Você não precisa atribuir o administrador a um grupo de licenças diferente.
7. Por padrão, o **Administrator** pertence ao **grupo de políticas de domínio**. Você não precisa atribuir o administrador a um grupo de políticas do cliente diferente.
8. É recomendável não definir a expiração da conta para **Administradores**, a menos que seja obrigatório. Por exemplo, um administrador temporário foi atribuído enquanto alguém está de férias.  
Isso conclui o procedimento.



# 5. LICENÇAS DE USUÁRIO

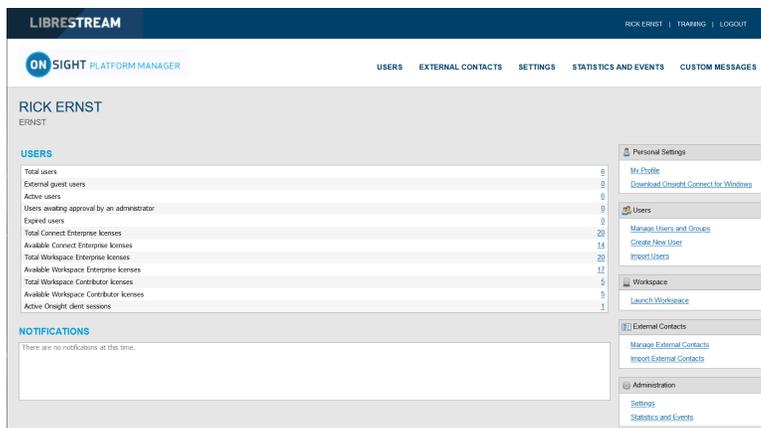


Figura 5-1 Painel

O OnSight Platform Manager dá suporte a três opções de licença de usuário:

- **Connect Enterprise** — fornece serviços de chamada OnSight (as definições do SIP devem ser configuradas no domínio).
- **Workspace Enterprise** — fornece ao usuário corporativo acesso ao Workspace com base em permissões atribuídas pelo administrador.
- **Workspace Contributor** — fornece ao usuário colaborador acesso pelo Workspace à sua pasta de upload e para editar seu conteúdo; o acesso a outros ativos não pode ser concedido ao colaborador.

 **Nota:** os tipos de licença do Workspace são mutuamente exclusivos. Um usuário não pode ser atribuído a ambos os tipos de licença do Workspace. Cada licença permite recursos para o usuário dentro do aplicativo OnSight Connect. Os usuários podem ter licenças únicas ou múltiplas atribuídas à sua conta. Todas as licenças permitem a captura de conteúdo localmente (imagens e gravações).

## 5.1. Opções de licença

A tabela a seguir descreve as combinações válidas de atribuição de tipos de licença:

Tabela 5-1 Opções de licença

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

### Usuário A (Connect Enterprise):

Usuários **Connect Enterprise** podem fazer logon no **Onsight Connect**, fazer chamadas, capturar conteúdo e compartilhar conteúdo com outros usuários Connect Enterprise.

### Usuário B (Workspace Enterprise):

Usuários **Workspace Enterprise** podem fazer logon no **Onsight Connect**, capturar conteúdo, fazer upload de conteúdo para o **Workspace** e fazer logon no Workspace para editar, gerenciar e colaborar com conteúdo. Isso inclui todos os ativos aos quais receberam permissões de acesso.

### Usuário C (Workspace Contributor):

Usuários **Workspace Contributor** podem fazer logon no **Onsight Connect**, capturar conteúdo, fazer upload de conteúdo para o **Workspace** e fazer logon no Workspace para acessar o conteúdo da pasta de upload. Esse usuário não pode ter acesso ao conteúdo fora de sua pasta de upload.

### Usuário D (Connect Enterprise com Workspace Enterprise):

Usuários **Connect Enterprise** podem fazer logon no **Onsight Connect**, fazer chamadas, capturar conteúdo e compartilhar conteúdo com outros usuários **Connect Enterprise**. Além disso, com os usuários **Workspace Enterprise**, eles podem fazer upload de conteúdo para o **Workspace**. Esse usuário também pode fazer logon no Workspace para editar, gerenciar e colaborar com conteúdo. Ele pode receber permissões para acessar outro conteúdo dentro do Workspace fora de sua pasta de upload.

### Usuário E (Connect Enterprise com Workspace Contributor):

Usuários **Connect Enterprise** podem fazer logon no **Onsight Connect**, fazer chamadas, capturar conteúdo e compartilhar conteúdo com outros usuários Connect Enterprise. Além disso, com os usuários **Workspace Contributor**, eles podem fazer upload de conteúdo para o **Workspace**. Esse usuário também pode fazer logon no **Workspace** para acessar o conteúdo da pasta de upload. Esse usuário não pode ter acesso ao conteúdo fora de sua pasta de upload.

## 5.2. Modo de captura

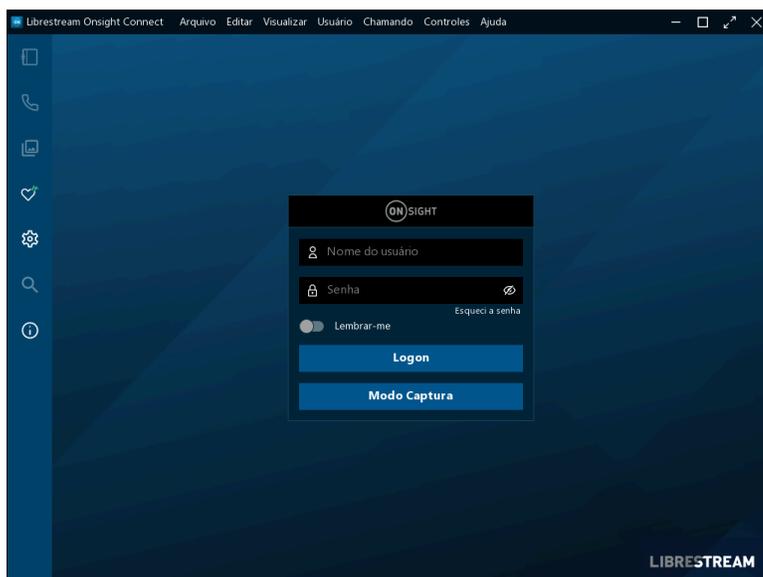


Figura 5-2 Modo de captura

O **Capture Mode** fornece o uso off-line do Onsight Connect sem precisar de logon. Na janela de logon do Onsight Connect, os usuários podem pressionar o botão **Capture Mode** para inserir o **Onsight Connect Viewer**. Isso permite o acesso a fontes de vídeo de câmeras de dispositivos móveis, bem como dispositivos Onsight, como o **Cube** e o **Hub**, sem exigir logon do usuário Onsight.

Os usuários que não receberam uma conta do Onsight podem baixar o **Onsight Connect** e capturar conteúdo imediatamente. Todo o conteúdo é salvo localmente em seu dispositivo móvel ou PC Windows. Depois que uma conta lhes é atribuída, eles podem fazer logon e acessar as imagens e gravações capturadas anteriormente, que podem ser compartilhadas em uma chamada do Onsight ou enviadas para o Workspace.

Depois que um usuário faz logon no aplicativo Onsight Connect com um logon de usuário do Onsight, o **Capture mode** não fica mais disponível na janela de logon. Um logon do Onsight deve ser usado para ter acesso ao aplicativo a partir desse ponto.

# 6. GERENCIAR USUÁRIOS E GRUPOS

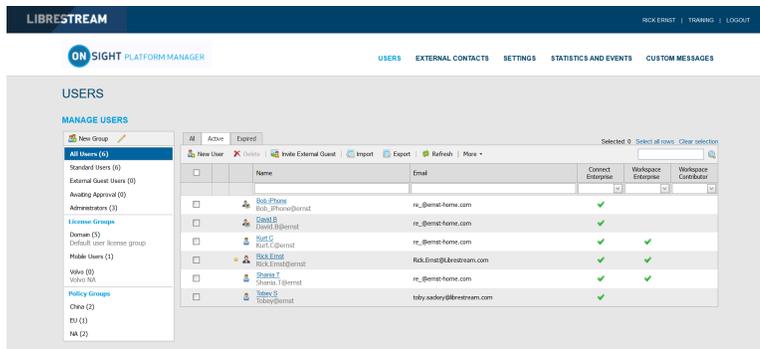


Figura 6-1 Gerenciar grupos e usuários

Os administradores do OnSight usam o OPM para gerenciar centralmente licenças de usuário, listas de contatos, políticas e permissões. Existem duas abordagens principais para gerenciar licenças no OnSight Platform Manager. **Select Users** no menu principal para permitir que você gerencie:

- Gerenciamento de licenças de domínio
- Gerenciamento de grupos de licenças e políticas

## 6.1. Gerenciamento de licenças e políticas de domínio

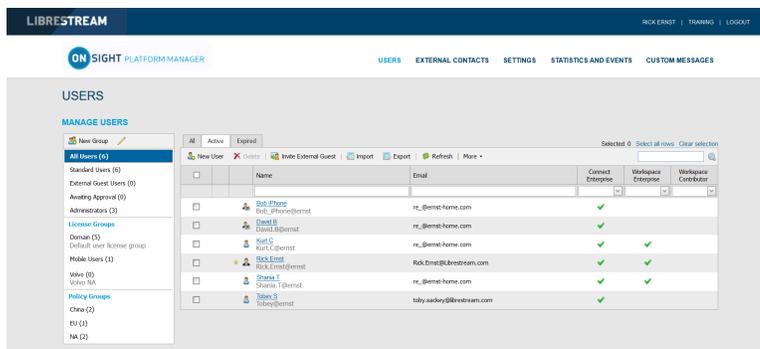


Figura 6-2 Grupo Todos os usuários/licença de domínio

O domínio é o grupo de licenças padrão. Todas as licenças estão sob o controle do domínio, é um pool único de licenças a partir do qual todas as licenças são atribuídas aos usuários. Os tipos de licença adicionados ao domínio podem ser atribuídos por um administrador a qualquer usuário do domínio.

**Client Policy** pode ser definida para todos os usuários editando o grupo **All Users**.

### Referências relacionadas

[Política do cliente — Práticas recomendadas \(na página 120\)](#)

## 6.2. Gerenciamento de grupos de licenças

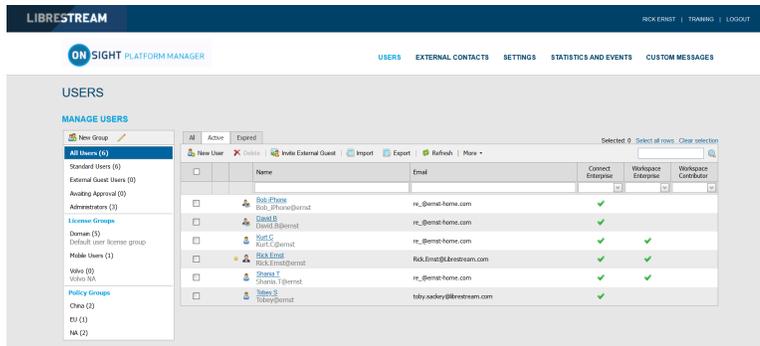


Figura 6-3 Grupos de licenças

O gerenciamento de grupos de licenças é um método opcional para gerenciar licenças. É habilitado apenas mediante solicitação. Ele permite que um administrador do OnSight crie grupos de licenças e atribua licenças do domínio aos grupos de licenças. Os membros do grupo são adicionados a cada grupo de licenças e recebem licenças sob o controle dos grupos de licenças.

Quando os grupos de licenças são habilitados, o domínio padrão ainda está ativo e atua como um grupo de licenças independente. As licenças são transferidas do domínio padrão para grupos de licenças personalizados. Uma vez que uma licença é transferida, ela fica sob o controle do grupo de licenças.

Administradores e administradores de grupos podem criar usuários dentro de um grupo de licenças, desde que tenham licenças disponíveis no grupo. Os usuários podem ser criados sem licenças, mas devem receber uma licença antes de se tornarem ativos.

A **Client Policy** pode ser definida independentemente para cada grupo de licenças.

### Referências relacionadas

[Política do cliente — Práticas recomendadas \(na página 120\)](#)

## 6.3. Gerenciamento de usuários e grupos de licenças/políticas

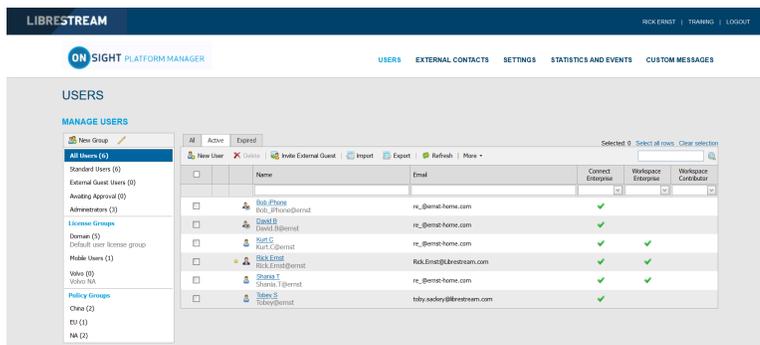


Figura 6-4 Grupos de políticas e licenças

O administrador do OPM pode criar dois tipos de grupos: **License** e **Policy**.

### Grupos de licenças

Os **License Groups** são opcionais e podem ser habilitados mediante solicitação. Eles são usados para aplicar a **Client Policy** e atribuir licenças aos membros do grupo. O administrador pode atribuir licenças a diferentes grupos de licenças. Os administradores podem ser atribuídos a um grupo (administrador de grupo). Por exemplo, um administrador do OPM atribuiu 10 licenças Connect Enterprise a um **License Group**. Um administrador de grupo pode ser designado para gerenciar e conceder no máximo 10 licenças **Connect Enterprise** a um máximo de 10 membros do grupo. Se um usuário **Connect Enterprise** for excluído do grupo, a licença fica disponível para uso e pode ser atribuída a um novo usuário. O administrador do OPM pode reatribuir licenças de volta para o domínio ou outro grupo de licenças.

Os grupos padrão não podem ser excluídos.

## Grupos de políticas

Os **Policy Groups** são usados para aplicar a política do cliente aos membros do grupo. Os grupos de políticas não têm recursos de gerenciamento de licenças. Ao usar grupos de políticas, licenças são atribuídas aos usuários do pool de licenças de domínio.

## Substituição do administrador

Um administrador pode substituir a política de grupo de um usuário específico editando a página **Client Policy** do usuário. As configurações da política de cliente do usuário terão precedência sobre qualquer configuração de política de cliente do grupo.

## Grupos de licenças e uso

O uso de **License Groups** é opcional e deve ser habilitado para o seu domínio.

- Você pode deixar todas as licenças atribuídas ao seu domínio padrão. Se você não tiver necessidade de gerenciamento de licenças para grupos personalizados, o gerenciamento de licenças do pool de domínios é recomendado.
- Você pode gerenciar a **Client Policy** usando grupos de políticas personalizados. Se você não precisar gerenciar a política do cliente para grupos personalizados, poderá definir **Client Policy** para todos os usuários editando a política **Standard Users**.
- Se a opção **External Guests** estiver habilitada, você poderá gerenciar a política do cliente para eles editando a política **External Guest Users**.
- As licenças de domínio podem ser atribuídas por administradores e administradores de grupos que foram atribuídos a grupos.
- Se os grupos de licenças não estiverem habilitados para o seu domínio, não haverá restrições no número de usuários que um administrador pode adicionar ao seu grupo, desde que haja licenças disponíveis no domínio.

## Gerenciamento de usuários

As opções padrão contidas no painel **MANAGE USERS** incluem:

- **All Users** inclui todos no domínio: Administradores, usuários não administrativos e usuários convidados externos. Inclui a configuração da política do cliente. Quando um novo usuário é adicionado, ele é automaticamente um membro do grupo Todos os usuários.
- **Standard Users**, por padrão, inclui usuários não administrativos e administradores (os usuários convidados externos não estão incluídos). Inclui a configuração da política do cliente.
- **External Guest Users** (opcional) inclui todos os usuários convidados externos e permite a configuração da política do cliente.
- **Awaiting Approval** indica o número de usuários autorregistrados aguardando aprovação do administrador. A política do cliente não é aplicável.
- **Administrators** indica o número de contas de administrador. A política do cliente não está incluída.
- **License Groups** (opcional) inclui grupos de licenças personalizados e o domínio padrão. A política do cliente está incluída.
- **Policy Groups** inclui grupos de políticas personalizados. O gerenciamento de licenças não está incluído.



**Nota:** os grupos padrão não podem ser excluídos.

### Referências relacionadas

[Política do cliente — Práticas recomendadas \(na página 120\)](#)

## 6.4. Adição de um grupo

Faça logon no OPM.

Para adicionar um grupo manualmente:

1. Selecione **USERS** no menu principal. A página Users é exibida.

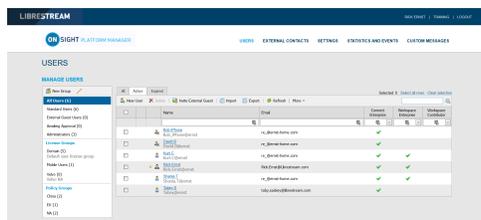


Figura 6-5 USUÁRIOS

2. Para adicionar um grupo personalizado, clique no ícone  **New Group** no painel **MANAGE USERS**. A janela Create New Group é exibida.

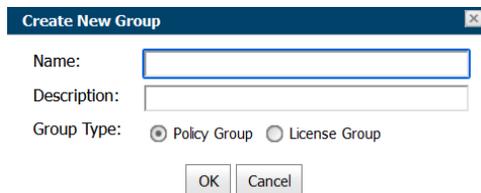


Figura 6-6 Criar novo grupo

3. Especifique as informações dentro dos campos **Name** e **Description**.

4. Defina **Group Type** como:

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

5. Clique em **OK**.



**Nota:** os grupos de licenças devem ter um número definido de licenças que tenham sido atribuídas a eles pelo administrador. Os usuários só podem ser adicionados ao grupo de licenças se houver licenças disponíveis. Tanto os grupos de políticas quanto os grupos de licenças têm uma política do cliente e permissões incluídas.

Isso conclui o procedimento.

Para obter mais informações, consulte a seção [Política do cliente e Permissões \(na página 77\)](#).

#### Referências relacionadas

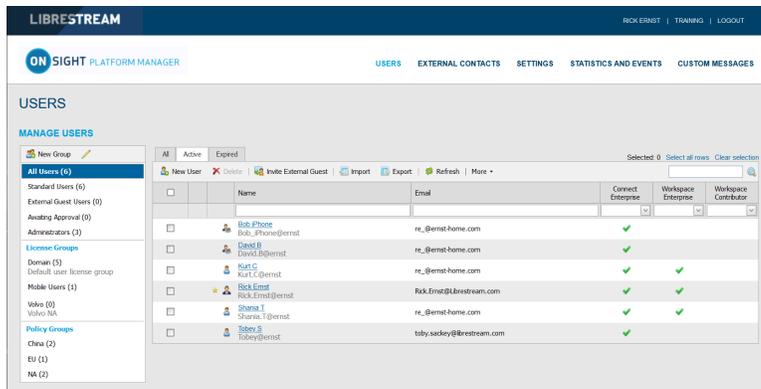
[Política do cliente — Práticas recomendadas \(na página 120\)](#)

[Permissões do cliente — Práticas recomendadas \(na página 133\)](#)

#### Informações relacionadas

[Política do cliente e Permissões \(na página 77\)](#)

# 7. USUÁRIOS E GRUPOS



Existem três métodos para um administrador adicionar usuários:

1. Criar um novo usuário manualmente.
2. Importar usuários de um arquivo (por exemplo, SampleUserImport.csv).
3. Autorregistro através da página Web de autorregistro do OPM.

## 7.1. Criar novo usuário

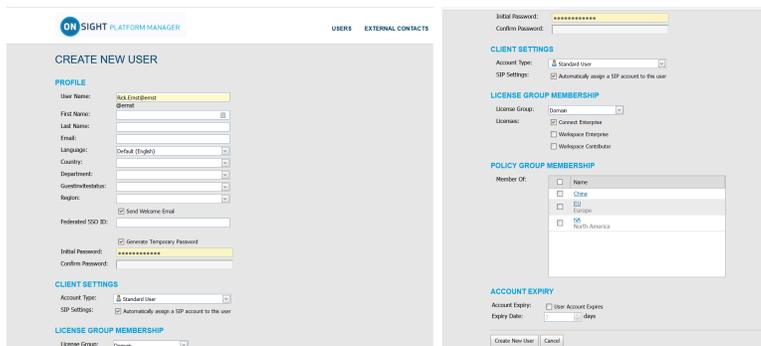


Figura 7-2 Criar um novo usuário

Selecione **USERS** no menu principal e clique no ícone  **New User** para acessar a janela **CREATE NEW USER**. Para criar um novo usuário, você precisará fornecer detalhes de:

- **PROFILE** — forneça detalhes de informações do usuário que incluem **User Name**, **First Name**, **Last Name**, **Email** e use menus suspensos para indicar: **Language**, **Country**, **Department** e **Region** etc.
- **CLIENT SETTINGS** — defina o **Account Type** usando o menu suspenso como **Administrator**, **Group Administrator** ou **Standard User**.
- **LICENSE GROUP MEMBERSHIP** — atribua o novo usuário a um grupo de licenças conforme necessário e habilite a caixa de seleção para indicar o tipo de licença (**Connect Enterprise**, **Workspace Enterprise** ou **Workspace Contributor**).
- **POLICY GROUP MEMBERSHIP** — atribua o novo usuário a um **Policy Group** conforme necessário.
- **ACCOUNT EXPIRY** — habilite a opção de **User Account Expires** e forneça uma **Expiry Date** conforme necessário.

Clique no botão **Create New User**.

### 7.1.1. Criação de um novo usuário

Faça login no OPM.

Para criar manualmente uma nova conta de usuário:

1. Selecione **USERS** no menu principal. A página USERS é exibida.

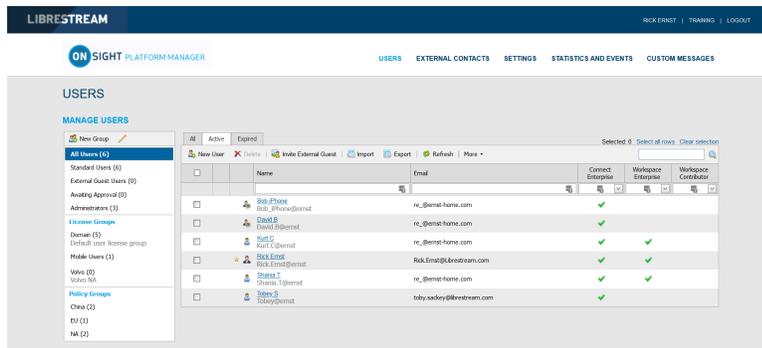


Figura 7-3 Página de usuários

2. Clique no ícone  **New User**. Você verá a janela **CREATE NEW USER**.

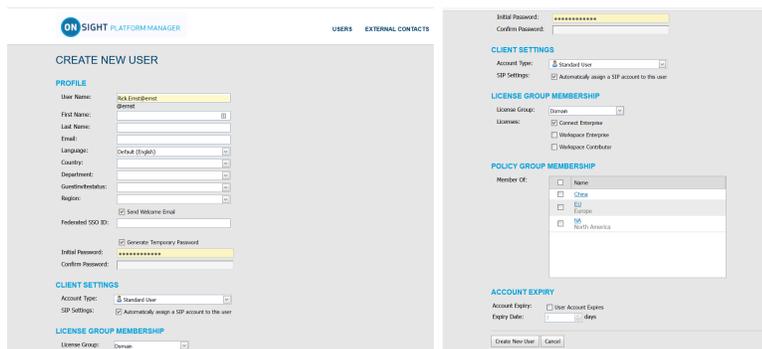


Figura 7-4 Criação de um novo usuário



**Nota:** se o ícone  **New User** estiver ausente, você não poderá adicionar novos usuários. Revise as configurações da sua **Client Policy** para **Allow New Contacts**, conforme necessário.

3. Especifique as informações do **PROFILE** para o novo usuário. Por padrão, as opções **Send Welcome Email** e **Generate Temporary Password** estão selecionadas.
4. Em **CLIENT SETTINGS**, selecione o tipo de conta:  **Standard User**,  **Administrator** ou  **Group Administrator**.
5. A opção **Automatically assign a SIP account to this user** está selecionada por padrão. Consulte **SETTINGS > SIP** para obter detalhes sobre a configuração do **Auto-Assignment SIP Pool**.



**Nota:** os usuários existentes podem ter as suas configurações do SIP atribuídas ou atualizadas no pool de atribuição automática, acessando a página **Users Client Settings** e pressionando **Assign / Restore SIP Account** na seção **Common Actions**.

6. Selecione **LICENSE GROUP MEMBERSHIP** para o usuário. Por padrão, todos os usuários pertencem ao **Domain license group**. Se você tiver criado grupos de licenças, selecione o grupo e o(s) tipo(s) de licença ao(s) qual(is) está atribuindo o usuário. Você também pode atribuir o usuário a um **Client policy group** marcando a caixa de seleção **Member Of** para indicar a que grupo ele pertence.



**Nota:** tanto **License groups** quanto **Policy groups** têm as configurações **Client policy** e **Permission** associadas a eles. Se você tiver definido uma **Client Policy** no **License group**, não precisará atribuir um **Policy group** ao usuário.



- **Opcional:** Você poderá definir a caixa de seleção **User Account Expires** e **Expiry date** para o usuário.
- Para aplicar as suas alterações, clique no botão  **New User** na parte inferior da janela.
- Para definir um usuário como **Client Administrator**, clique no nome do usuário na lista da página **USERS**. Marque a caixa de seleção **Client Administrator**. Agora, o usuário consegue editar todas as configurações de um ponto de extremidade.

7. Clique no botão **Create New User**.  
Isso conclui o procedimento.

 **Nota:** \*a configuração do administrador do cliente para contas de usuário foi descontinuada. Recomenda-se que os usuários sejam adicionados a grupos de políticas para controlar as permissões dos clientes. Contudo, os usuários que atualmente têm o administrador do cliente habilitado para sua conta de usuário podem ser gerenciados através da política de grupo de administradores do cliente. Além disso, se você estiver fazendo a transição de OMS para OPM, a configuração de administradores do cliente é o único método para conceder direitos de administrador a um usuário.

## 7.2. E-mail de boas-vindas

The screenshot shows the 'CREATE NEW USER' form in the OnSight Platform Manager. The form is titled 'CREATE NEW USER' and is divided into three main sections: PROFILE, CLIENT SETTINGS, and LICENSE GROUP MEMBERSHIP. The PROFILE section includes fields for User Name, First Name, Last Name, Email, Language, Country, Department, Guestinviestatus, and Region. There are checkboxes for 'Send Welcome Email' and 'Generate Temporary Password'. The CLIENT SETTINGS section includes 'Account Type' (Standard User) and 'SIP Settings' (Automatically assign a SIP account to this user). The LICENSE GROUP MEMBERSHIP section includes 'License Group' (Domain).

**Figura 7-5** Opção de e-mail de boas-vindas

O e-mail de boas-vindas notifica novos usuários de sua conta OnSight Connect, além de fornecer links para **Download and install OnSight Connect** e **Login**. O e-mail de boas-vindas pode ser ativado como uma caixa de seleção dentro da seção **PROFILE** quando você cria um novo usuário. Depois disso, a mensagem de boas-vindas pode ser reenviada, se necessário. Clique em **USERS** no menu principal e selecione um usuário na lista. Localize **Common Actions** e selecione **Resend Welcome Message**.

## 7.2.1. E-mail de boas-vindas no local

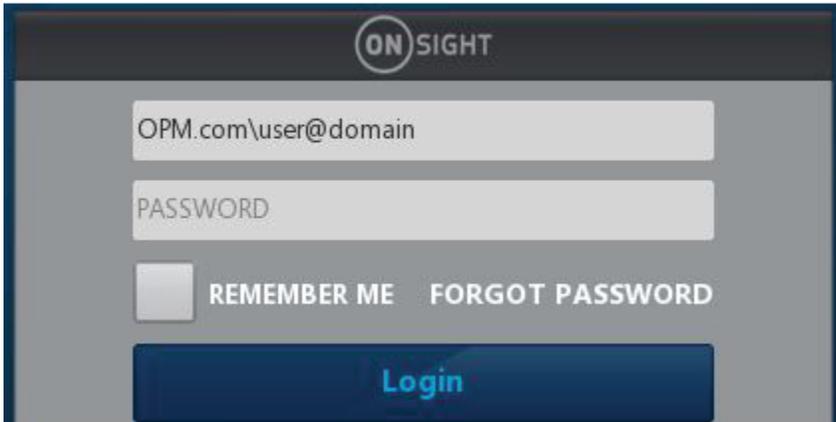


Figura 7-6 URL no local

Os e-mails de boas-vindas **On-premises** conterão um link **Login to Onsight Connect**, que iniciará o Onsight Connect e o direcionará para a URL do seu Onsight Platform Manager. A URL no link deve corresponder à URL configurada durante a instalação do seu servidor no local.

O formato deve ser `OPM.com\user@domain`, em que `OPM.com` é o nome de domínio do seu servidor.

Se uma porta diferente da 443 for usada para a instalação do OPM-OP, o formato deverá ser `OPM.com:port\user@domain`, em que `OPM.com:port` é o nome de domínio do servidor e o número da porta que está sendo usada. Por exemplo, `OPM.com:8083\user@domain`.

Depois de conectados, eles deverão confirmar se querem usar este serviço de conta Onsight a partir de agora. O usuário deve clicar em **Yes** para aceitar as alterações. Daí em diante, ele precisará apenas inserir seu **User Name** e **PASSWORD** para fazer logon ou habilitar a opção **REMEMBER ME** para automatizar o processo de logon.

## 7.2.2. Formatos de URL no local

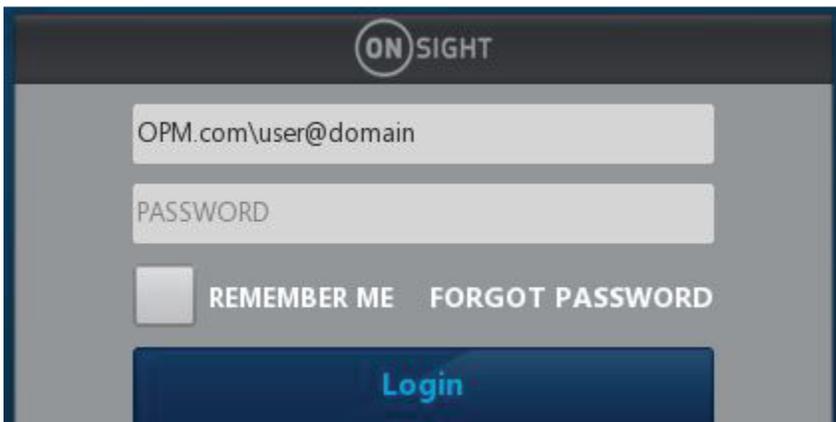


Figura 7-7 URL no local

Ao especificar o caminho do OPM no campo de nome de usuário no logon, formatos abreviados são aceitos. Padrões típicos codificados são usados no caso em que elementos do caminho estão ausentes.

O campo de nome de usuário deve conter um caminho do OPM se o texto inserido contiver uma barra invertida "\": `[OPM URI]\user@domain`

A parte "OPM URI" será analisada como um URI, de modo que somente URIs relativos ou absolutos serão aceitos (por exemplo, sem espaços no nome do host). Os formatos aceitáveis incluem:

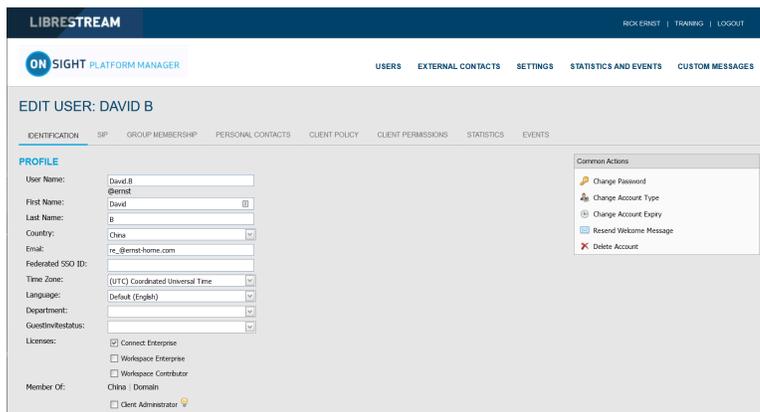
- Um URI absoluto: `https://[authority]/[path]\user@domain`.
- Somente host OPM: `[host]\user@domain`. O esquema será definido como `https`, o caminho será definido como `"OamClientWebService"`.
- Host e caminho do OPM: `[host]/[path]\user@domain`. O esquema será definido como `https`. Host e caminho são usados no estado em que se encontram.
- Esquema e host do OPM: `https://[host]\user@domain`. O caminho será definido como **OamClientWebService**. Esquema e host são usados no estado em que se encontram.
- Apenas esquemas `https` são aceitos.

Além disso, na mensagem de boas-vindas estão links para baixar o Onsign Connect do seu Onsign Platform Manager e links de download para a **loja de aplicativos do iOS** e a **Android Google Play Store**. O usuário pode clicar em **Download for Windows** ou **Download for iOS** ou **Android**.

Depois que o usuário instalou o Onsign Connect, ele deve clicar no botão **Login to Onsign Connect** para configurar corretamente o software para fazer login na sua instalação do OPM.

Os usuários de dispositivos móveis devem instalar o Onsign Connect na **Apple Store** ou **Google Play Store**.

## 7.3. Requisito de e-mail do usuário



**Figura 7-8** Requisito de e-mail do usuário

Os endereços de e-mail são opcionais no OPM. **No entanto, se um usuário não tiver um endereço de e-mail configurado, ele não receberá e-mails de notificação (e-mails de boas-vindas, e-mails de redefinição de senha etc.).** Se ele solicitar uma redefinição de senha, a página dirá "Se um e-mail válido estiver configurado...", mas não confirmará se um e-mail está configurado para sua conta. Na página **PROFILE** do usuário, na seção **Common Actions**, a opção **Resend Welcome Email** estará oculta se o usuário não tiver endereço de e-mail. E-mails de boas-vindas notificam os usuários como fazer **download, install e login** no Onsign Connect.

Os e-mails são necessários nas seguintes condições:

- Os usuários convidados exigem um endereço de e-mail válido ou número de telefone para receber um convite.
- O usuário **Account Owner** deve ter um endereço de e-mail válido.

## Requisitos de e-mail para configurações de segurança e SSO

The image shows two screenshots of the Settings page. The left screenshot is the 'SECURITY' tab, and the right is the 'SSO' tab. Both show the 'SELF REGISTRATION' section with the checkbox 'Require Email Address for Self-Registered Accounts' checked. Blue arrows point to this checkbox in both screenshots.

Figura 7-9 Configurações de segurança e SSO

O requisito de e-mail para usuários autorregistrados (seja pela página de autorregistro ou provisionado pelo SSO) é configurável nas páginas **SETTINGS > SECURITY** e **SETTINGS > SSO**.

Se definido como **Required** — os usuários que se registrarem por meio da página de autorregistro devem inserir um e-mail.

**SSO Users** — se o e-mail fornecido como atributo estiver em branco, o provisionamento falhará. Se o e-mail for definido como **Prompt on First Login**, o usuário deverá inserir um e-mail.

 **Nota: Require Email Address for Self-Registered Accounts** não pode ser desmarcado.

Se definido como **Optional** — os usuários que se inscreverem por meio da página de autorregistro poderão informar um e-mail opcionalmente. Se não for fornecido, o e-mail estará em branco e eles não receberão um e-mail de boas-vindas.

**SSO Users** — se o e-mail fornecido como atributo estiver em branco, o provisionamento prosseguirá com um e-mail em branco. Se o e-mail for definido como **Prompt**, o usuário poderá informar um e-mail opcionalmente.

 **Nota: Require Email Address for Self-registered Accounts** pode ser desmarcado.

E-mails fornecidos por um atributo de SSO não requerem verificação.

 **Nota:** qualquer e-mail fornecido por um usuário durante o autorregistro requer verificação antes que a conta possa ser usada. E-mails fornecidos por um atributo de SSO não requerem verificação.

## 7.4. Tipos e permissões de conta de usuário

Initial Password: [masked]  
Confirm Password: [ ]

**CLIENT SETTINGS**

Account Type: Standard User  
SIP Settings:  Automatically assign a SIP account to this user

**LICENSE GROUP MEMBERSHIP**

License Group: Domain  
Licenses:  Connect Enterprise  
 Workspace Enterprise  
 Workspace Contributor

**POLICY GROUP MEMBERSHIP**

Member Of:

<input type="checkbox"/>	Name
<input type="checkbox"/>	China
<input type="checkbox"/>	EU Europe
<input type="checkbox"/>	NA North America

**ACCOUNT EXPIRY**

Account Expiry:  User Account Expires  
Expiry Date: 7 days

Create New User Cancel

Figura 7-10 Tipo de conta de usuário

Em **CLIENT SETTINGS**, o menu suspenso **Account Type** indica o nível de acesso que o usuário tem ao OnSight Platform Manager. As licenças atribuídas ao usuário determinam os recursos a que o usuário tem acesso no OnSight Connect e no Workspace. A política e as permissões do cliente ditam o acesso dos usuários às configurações nos aplicativos do cliente. As opções **Account Type** incluem **Administrator**, **Group Administrator** e **Standard User**.

**Administrator:** acesso total ao OPM e às configurações de domínio, inclusive gerenciamento do usuário.

 **Nota:** apenas um administrador pode atribuir licenças a grupos de licenças. Quando um domínio é criado pela primeira vez para um cliente, o proprietário da conta é o único administrador. O proprietário da conta deve criar administradores adicionais.

**Standard User Permissions:** um **Standard User** não tem privilégios de administração. Ele está sujeito à política do grupo e às permissões atribuídas a ele com a associação ao grupo pelo administrador do OPM. Ele pode convidar convidados externos se a opção **Allow users to invite guests** estiver habilitada no domínio (requer a licença master de convidados externos para o domínio).

**Group Administrator Permissions:** um administrador de grupo tem acesso às configurações de nível de grupo a que foi atribuído, inclusive:

- Modificar usuários que estão em seu grupo (alterar configurações, senhas etc.).
- Criar e excluir usuários dentro de seu grupo.
- Definir **Client Policy** para o grupo.

Para **License Groups**, os administradores do grupo poderão adicionar usuários com base no número de licenças atribuídas ao grupo pelo administrador do OPM.

## 7.5. Promoção de usuários e atribuição de um administrador de grupo

Faça logon no OPM.

O gerenciamento de administradores de grupos é um processo de duas etapas. Você deve alterar um usuário padrão para um administrador de grupo e, em seguida, atribuí-lo a um grupo.

## Promoção de um usuário padrão a um administrador

1. Para promover um usuário a **Group Administrator**, você precisará fazer login no OPM e selecionar **USERS** no menu principal. A página USERS é exibida.

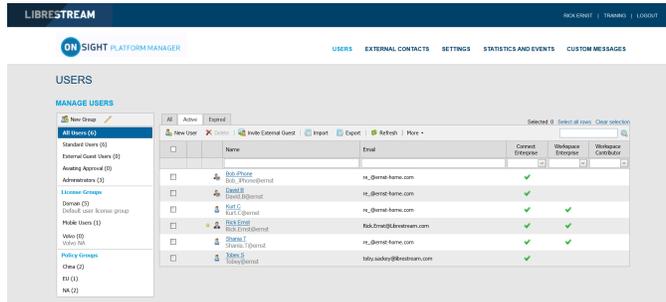


Figura 7-11 Página de usuários

2. Clique para selecionar um nome de usuário na tabela Usuários.

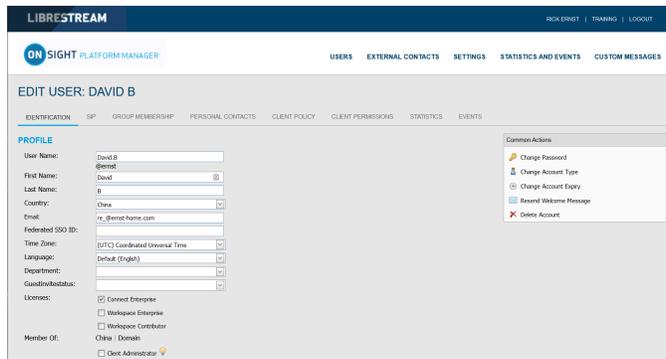


Figura 7-12 Página Editar usuário

- a. Localize a área **Common Actions** e selecione **Change Account Type**.
- b. Selecione **Administrador de grupo** em **Account Type** e selecione **Change Account Type** para aplicar a alteração. Uma mensagem é exibida indicando que o tipo de conta foi alterado com sucesso.

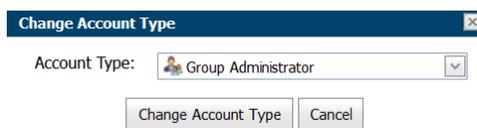


Figura 7-13 Alterar tipo de conta

- c. Clique em **OK**.

## Atribuição de um administrador a um grupo

3. Para designar um administrador a um grupo:

a. Selecione **Users** no menu principal e selecionar o grupo para atribuir um administrador.

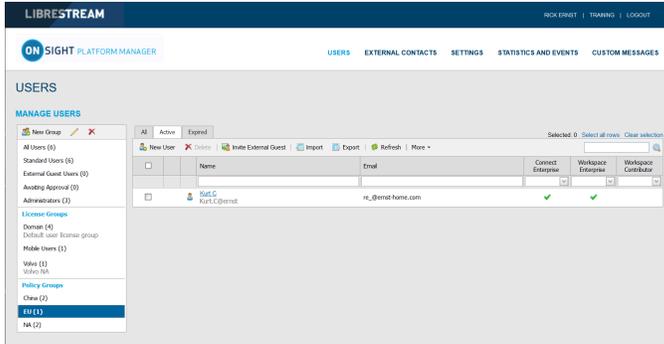


Figura 7-14 Seleção de um grupo

b. Clique no ícone  **Modify Group** para editar. A página EDIT GROUP é exibida.

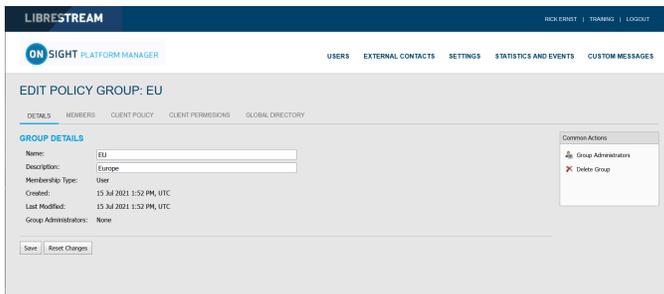


Figura 7-15 Editar grupo de políticas

c. Na seção **Common Actions**, clique em  **New Group**.

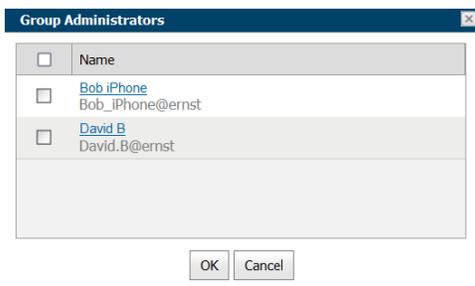


Figura 7-16 Administradores de grupo

d. Habilite a caixa de seleção ao lado de um ou mais administradores de grupo da lista e clique em **OK**. A seção Administradores de grupo é atualizada de acordo.

e. Clique em **Save**.

## 7.6. Editar grupos

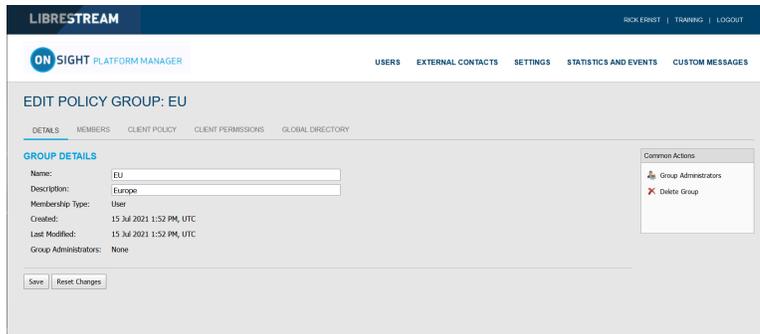


Figura 7-17 Editar um grupo

Para editar um grupo, selecione **USERS** no menu principal e selecione um grupo no painel **MANAGE USERS**. Clique no ícone  **Modify Group** (lápiz) para abrir a página **GROUP DETAILS**. A página **GROUP DETAILS** inclui:

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

Há guias adicionais disponíveis para editar o grupo, que incluem **MEMBERS**, **CLIENT POLICY**, **CLIENT PERMISSIONS** e **GLOBAL DIRECTORY**.

A seção **Common Actions** permite modificar  **Group Administrator** e  **Delete Groups**.

### Referências relacionadas

[Política do cliente — Práticas recomendadas \(na página 120\)](#)

[Permissões do cliente — Práticas recomendadas \(na página 133\)](#)

### 7.6.1. Adicionar/Remover membros do grupo

Faça login no OPM, selecione **USERS** no menu principal, selecione um grupo no painel **MANAGE USERS** e clique no ícone  **Modify Group** (lápiz) para abrir a página **EDIT GROUP**.

Para atribuir membros a um grupo:

1. Selecione a guia **Members** e clique no ícone  **Add Members** para adicionar usuários ao grupo.

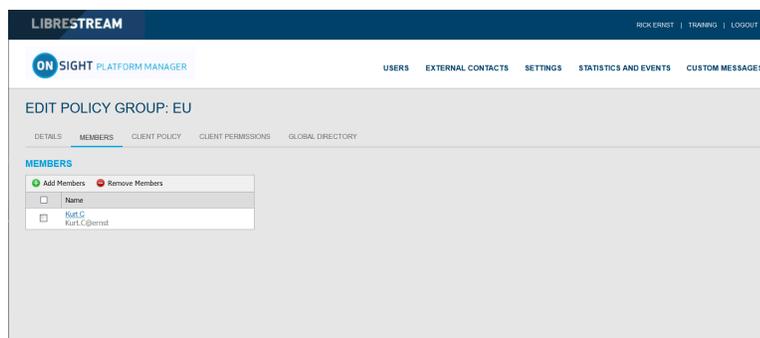


Figura 7-18 Editar grupo de iniciadores

2. Habilite as caixas de seleção para os usuários que você quer adicionar e pressione o botão **Add Selected Members**.

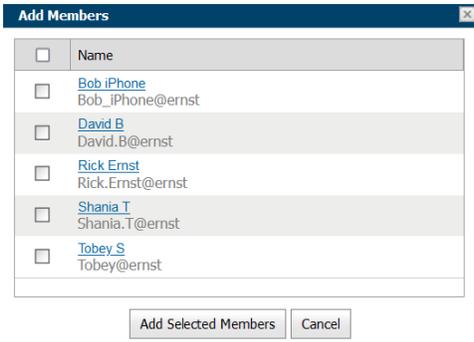


Figura 7-19 Adicionar membros

3. Para remover membros, habilite a caixa de seleção ao lado da lista de nomes do usuário e pressione o ícone  **Remove Members**. Isso conclui o procedimento.

## 7.6.2. Atribuição de administradores de grupo

Selecione **USERS** no menu principal e selecione um grupo no painel **MANAGE USERS** e clique no ícone  **Modify Group** (lápis) para abrir a página **EDIT GROUP**.

Para designar um administrador de grupo:

1. Selecione **USERS** no menu principal e selecione um grupo.
2. Clique no ícone  **Modify Group** (lápis) para editar o grupo dentro da página DETAILS.

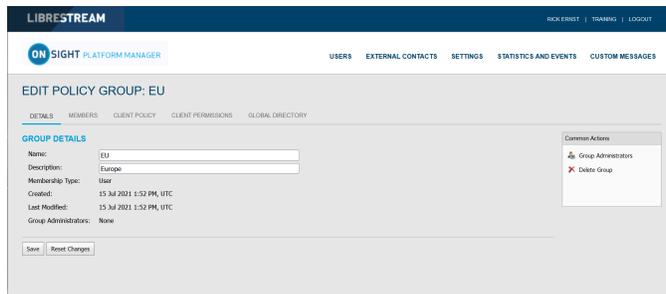


Figura 7-20 Detalhes do grupo

3. Localize a seção **Common Actions** e clique em  **New Group**. Uma lista de usuários com privilégios de administrador de grupo é exibida.

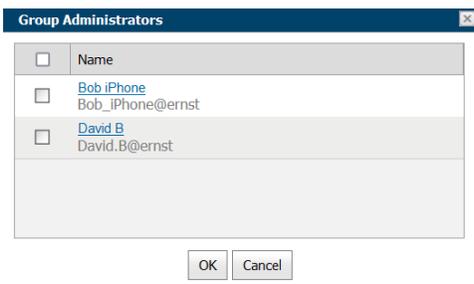


Figura 7-21 Administradores de grupo

4. Habilite a caixa de seleção ao lado de um ou mais administradores de grupo da lista e clique em **OK**.
5. Clique em **Save** para finalizar suas alterações. Isso conclui o procedimento.

### 7.6.3. Editar a política do cliente e as permissões

Faça logon no OPM, selecione **USERS** no menu principal, selecione um grupo no painel **MANAGE USERS** e clique no ícone  **Modify Group** (lápiz) para abrir a página **EDIT GROUP**.

Para modificar a política do cliente e as permissões de um grupo:

1. Selecione a guia **CLIENT POLICY** para configurar as definições do ponto de extremidade.

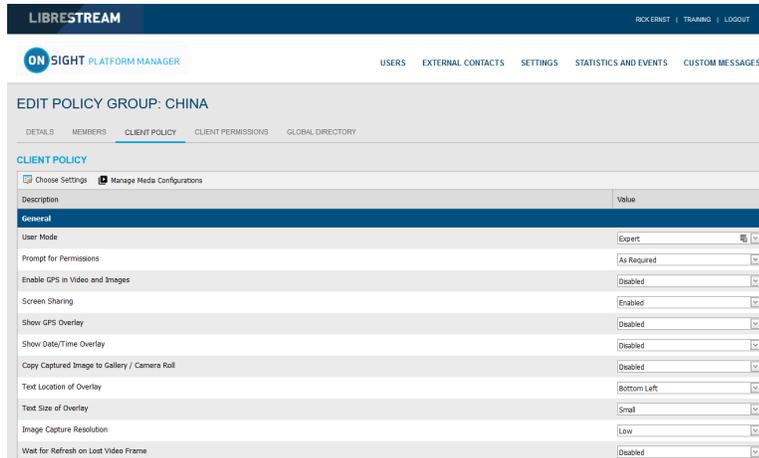


Figura 7-22 Editar grupo de políticas

2. Clique em  **Choose Settings** para adicionar as configurações que deseja controlar. Habilite as categorias e clique em **OK**.

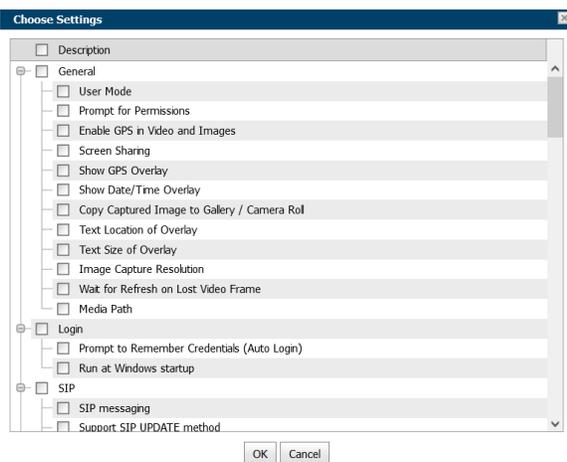


Figura 7-23 Escolher configurações

3. Defina **Value** para cada categoria e pressione **Save**.

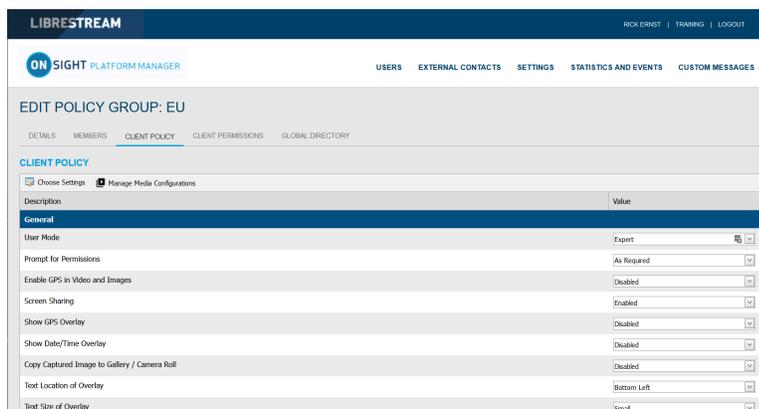
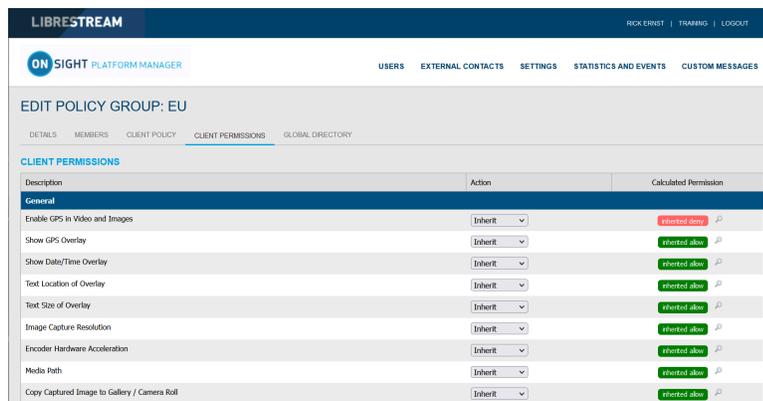


Figura 7-24 Política do cliente

#### 4. Selecione a guia **CLIENT PERMISSIONS**.



Description	Action	Calculated Permission
<b>General</b>		
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** Permissões do cliente

#### 5. Defina a ação como **Inherit**, **Allow** ou **Deny** para cada configuração.



**Nota:** Inherit (Herdar) é a permissão padrão, o cliente herdará configurações de qualquer grupo do qual o usuário é membro se a configuração não estiver incluída na política atual. Deny (Negar) não permitirá ao usuário editar as configurações no aplicativo OnSight Connect. Allow (Permitir) permitirá ao usuário editar as configurações no aplicativo OnSight Connect.

Isso conclui o procedimento.

Consulte [Política do cliente e Permissões \(na página 77\)](#) para obter uma descrição mais detalhada das ações.

O **Onsight Platform Management Settings Template** (modelo de configurações de gerenciamento da plataforma OnSight) descreve e fornece as melhores práticas para cada política de configuração e permissão disponíveis.

#### Referências relacionadas

[Política do cliente — Práticas recomendadas \(na página 120\)](#)

[Permissões do cliente — Práticas recomendadas \(na página 133\)](#)

#### Informações relacionadas

[Política do cliente e Permissões \(na página 77\)](#)

## 7.6.4. Diretório global

### 7.6.4.1. Disponibilidade do Diretório global

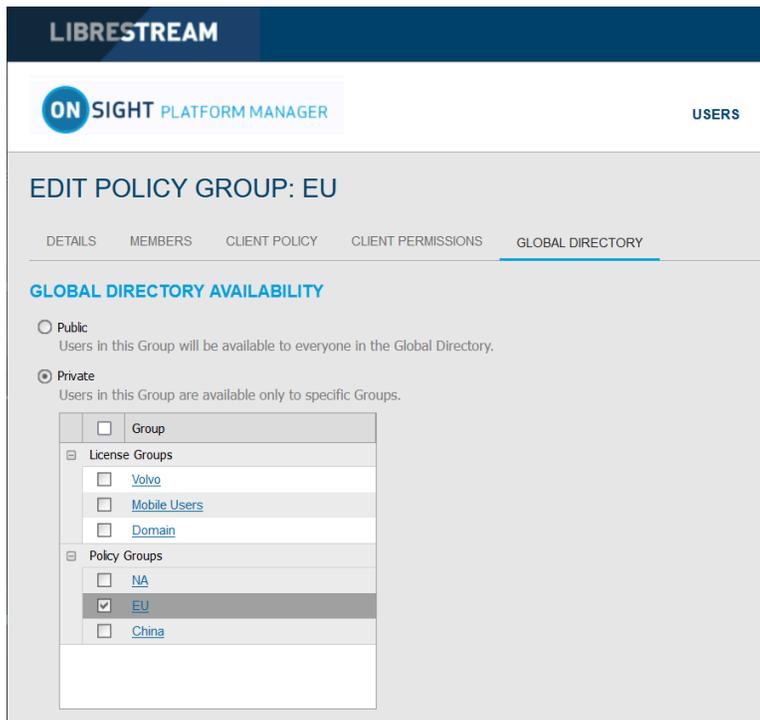


Figura 7-26 Editar grupo de políticas

Para editar o Diretório global, selecione **USERS** no menu principal e selecione um grupo no painel **MANAGE USERS**. Clique no ícone  **Modify Group** (lápis) e selecione a guia **GLOBAL DIRECTORY**. Os filtros **GLOBAL DIRECTORY AVAILABILITY** controlam se o grupo atual está visível no Diretório global.

- Selecione **Public** para tornar os membros do grupo visíveis para todos os grupos do Diretório global.
- Selecione **Private** para tornar esse grupo visível a fim de selecionar grupos no Diretório global. Selecione os grupos para os quais você quer ficar visível. Por exemplo, talvez você queira que só o grupo Serviço de campo fique visível para os membros do grupo Repositório de correções.

 **Dica:** pense nisso como "quem pode me procurar?".

### 7.6.4.2. Filtro do Diretório global

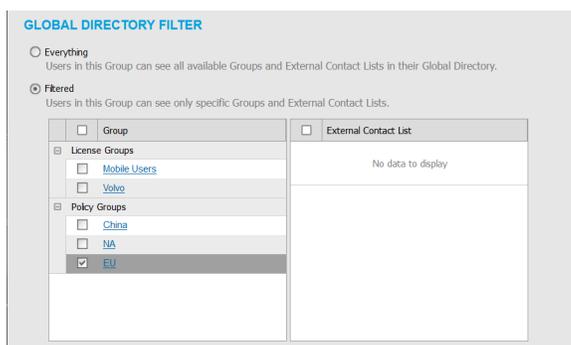


Figura 7-27 FILTRO DO DIRETÓRIO GLOBAL

O filtro do Diretório global controla quem fica visível para o grupo atual no **Global Directory**.

1. Habilite a caixa de seleção **Everything** se quiser que o grupo possa visualizar todos os grupos e contatos no Diretório global.
2. Habilite a opção **Filtered** para limitar a visibilidade da pesquisa ao grupo atual. Habilite as caixas de seleção para grupos e listas de contatos que deseja disponibilizar ao grupo atual. Por exemplo, talvez você queira que só o grupo **Serviço de campo** possa procurar os membros do grupo **Repositório de correções**.

### 7.6.4.3. Contatos padrão

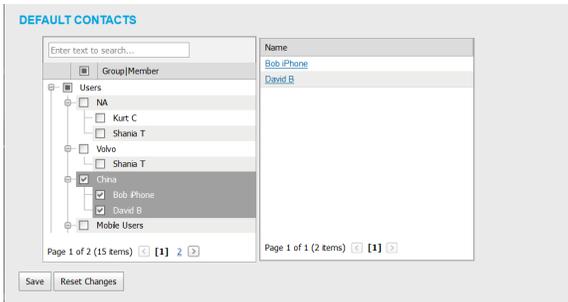


Figura 7-28 Contatos padrão

**DEFAULT CONTACTS** controlam quais contatos são incluídos automaticamente na lista de contatos de um membro do grupo quando ele faz login no aplicativo OnSight Connect.

1. Habilite a caixa de seleção para o grupo ou membros individuais do grupo que deseja adicionar à lista de contatos padrão do grupo atual. Desmarque e salve para remover contatos.
2. Pressione **Save** para manter as suas alterações.

 **Nota:** as listas de contatos externos devem ser criadas na guia **EXTERNAL CONTACTS** e atribuídas a grupos antes de estarem disponíveis no **Global Directory Filter** para seleção.

## 7.7. Importar/exportar usuários

Um administrador do OPM pode importar usuários usando um arquivo de valores separados por vírgula (CSV) criado a partir do modelo de importação. Esse é o método recomendado ao criar novos usuários e atribuir licenças.

### Práticas recomendadas para importar contatos

Na maioria dos casos, incluindo a primeira vez que você importar usuários, você precisará incluir os seguintes cabeçalhos de coluna em seu arquivo de importação:

- **UserName**
- **FirstName**
- **LastName**
- **EmailAddress** (Opcional, mas é necessário quando você quer usar notificações e recursos do sistema, como mudança de senha.)
- **GroupMembership** (Opcional)

Importar usuários com essas informações mínimas é o suficiente para ter todos os usuários configurados corretamente com as definições padrão em seu domínio.

As configurações do SIP podem ser definidas automaticamente selecionando **Automatically assign SIP accounts to new users** durante a etapa de importação. Essa é a melhor maneira de garantir que suas contas SIP sejam configuradas corretamente para cada usuário.

Casos especiais em que você precisa incluir mais do que as informações básicas do usuário incluem:

- **Single Sign On (SSO)**
- **Private SIP Server settings**
- **Passwords** (Use quando não depender do sistema para gerar senhas temporárias para os usuários.)

## 7.7.1. Criação de um modelo de importação de usuários

Faça login no OPM e selecione **USERS** no menu principal.

Para criar um modelo de importação de usuários manualmente:

1. Clique no ícone  **Import**.

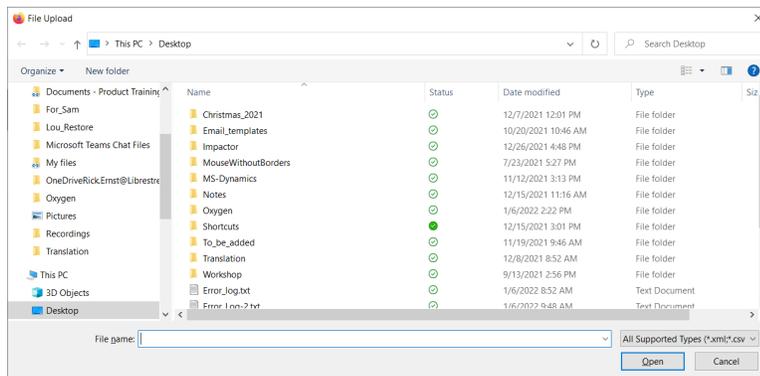


**Figura 7-29 Importação a partir de um arquivo**

2. Clique no link **Download Import Template**.
3. Depois de baixado, abra o `SampleUserImport.csv` em seu aplicativo de planilhas. Por exemplo, Microsoft Excel, OpenOffice Calc etc.
4. Siga as convenções de formatação descritas nas **CSV Import Instructions** e insira informações conforme necessário.

### Importação de um modelo de importação de usuários

5. Localize o campo **File to Import** e clique no botão **Browse....** Uma janela **File Upload** é exibida.



**Figura 7-30 Upload de arquivo**

6. Navegue e selecione o seu modelo de importação de usuários, depois clique em **Open**.
7. Clique em **Upload**.  
Isso conclui o procedimento.

## 7.7.2. Importação de usuários

Faça login no OPM e selecione **USERS** no menu principal. Você deve ter baixado e modificado previamente um modelo de importação como arquivo CSV. Consulte Criação de um modelo de importação de usuários.

Para importar usuários usando um modelo:

1. Clique no ícone  **Import**.
2. Selecione **Users** no menu suspenso **Import Mode**.

**Dica:** a definição de contatos externos como modo de importação vai importar os contatos externos listados em um arquivo `contacts.csv` ou `contacts.xml`. Consulte as **CSV Import Instructions** para obter detalhes sobre o formato de **CONTATOS EXTERNOS**. O arquivo de contatos externos deve ser um arquivo separado do arquivo de importação de usuários.

**Nota:** na página **EXTERNAL CONTACTS**, você pode selecionar a opção **More > Export** para baixar um modelo de arquivo do contato.

3. Localize o campo **File to Import** e clique no botão **Browse....** Uma janela **File Upload** é exibida.

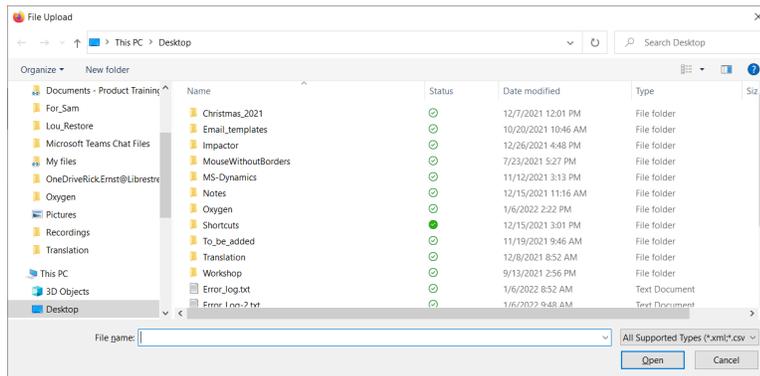


Figura 7-31 Fazer upload de arquivo

4. Navegue e selecione o seu modelo de importação de usuários, depois clique em **Open**.

5. Clique em **Upload**. A janela **Import Users** é exibida.

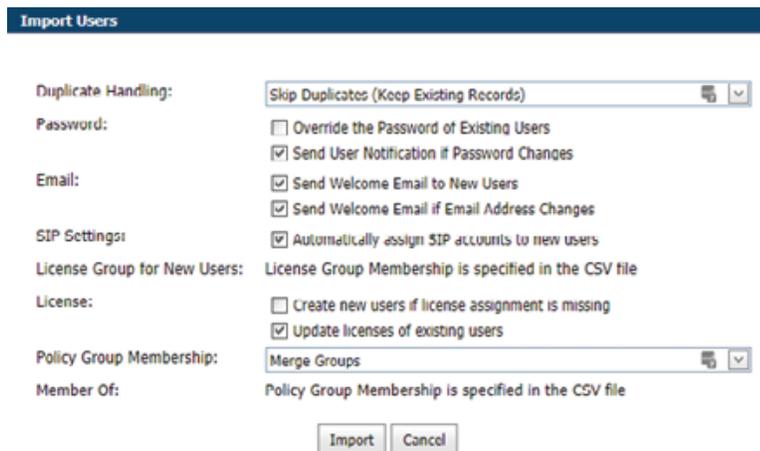


Figura 7-32 Importar usuários

6. Determine como quer lidar com as duplicatas:

- **Skip Duplicates** (manter registros existentes) ou
- **Update existing records**.

7. Na seção **Password**, determine como quer importar senhas:

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

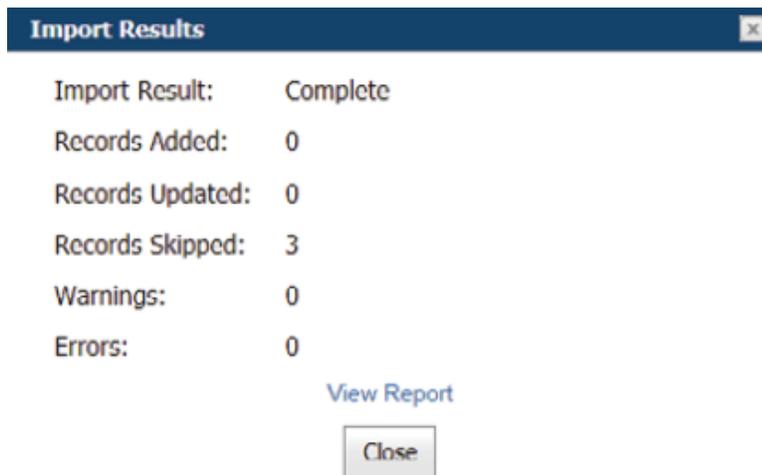
8. Na seção **Email**, selecione as opções relevantes:

- **Send Welcome Email to New Users.**
  - **Send Welcome Email if Email Address Changes.**
9. **SIP Settings** — habilite a caixa de seleção **Automatically assign SIP accounts to new users**. Essa é uma etapa importante na configuração das contas dos usuários para garantir que eles estão prontos para fazer chamadas do Onsite.
  10. O grupo de licenças para novos usuários é especificado no arquivo CSV.
  11. Licenças — habilite as opções apropriadas:
    - a. **Create new users if license assignment is missing.**
    - b. Atualize as licenças dos usuários existentes como:
      - i. **Connect Enterprise**
      - ii. **Workspace Enterprise**
      - iii. **Workspace Contributor**



**Nota:** os tipos de licença que você está atribuindo a cada usuário devem estar disponíveis no grupo de licenças escolhido.

12. Na seção de **Policy Group Membership**, determine como quer atribuir a associação ao grupo aos usuários existentes. Nesse caso, você está importando um arquivo do usuário do Onsite para reconfigurar as contas de usuários existentes. Selecione entre:
  - a. **Merge Groups** — permite que os usuários sejam membros de vários grupos.
  - b. **Overwrite Groups** — modifica os grupos atribuídos.
13. Na seção **Member Of**, é informado que a associação ao grupo de políticas é especificada no arquivo CSV.
14. Selecione **Import** para continuar. A janela **Import Results** é exibida.



**Figura 7-33 Resultados da importação**

Isso conclui o procedimento.

**Nota:** você deve usar o campo **License Group for New Users** para atribuir membros do grupo de licenças ao importar usuários e atribuir licenças. Isso significa que apenas os membros do mesmo grupo de licenças podem ser importados pelo arquivo de usuário especificado. O campo GroupMembership do arquivo SampleUserImport.csv não pode ser utilizado para especificar a associação ao grupo de licenças.

Ao importar usuários para um grupo de licenças, deve haver licenças suficientes disponíveis para cada tipo que está sendo atribuído a cada usuário.

 **SSO** — se você estiver usando SSO e **Federated SSO ID** para fornecer o mapeamento de identidade entre os usuários da sua empresa e as contas de usuários do Onsight, deverá preencher o campo de ID de SSO federado para cada usuário no arquivo UserImport.csv. O ID de SSO federado deve corresponder ao atributo de IdP mapeado que você configurou na página SSO Settings.

## 7.8. Exportar usuários



**Figura 7-34 Exportar usuários**

Clique em **USERS** no menu principal e clique em **Export** para baixar um arquivo CSV contendo uma lista de todos os usuários no domínio. Você pode optar por incluir **Usage Statistics** no relatório, conforme necessário.

## 7.9. Autorregistro de usuários

O administrador do Onsight pode habilitar o autorregistro para contas Onsight. O administrador distribui o link para a página de autorregistro com instruções para os candidatos à conta Onsight.

Os usuários que forem direcionados para o autorregistro serão solicitados a fornecer as seguintes informações na página **REGISTER FOR AN ACCOUNT**.

- **User Name**
- **Initial Password**
- **First Name**
- **Last Name**
- **Email**
- **Self-Registration Key** (se necessário)
- **Challenge code** (CAPTCHA)

Dependendo de como o administrador configurou o autorregistro, o usuário receberá um e-mail para **Verify your Email Address**. Ele será direcionado para a página de confirmação de verificação de e-mail. Depois que o e-mail for verificado e a conta for aprovada, o usuário receberá um e-mail de confirmação de aprovação e poderá começar a usar o Onsight Connect.

Se não houver exigência de aprovação das contas pelo administrador, o novo usuário receberá um e-mail **Welcome to Onsight** imediatamente após o registro.

### Referências relacionadas

[Segurança — Práticas recomendadas \(na página 117\)](#)



## 8. CONTATOS EXTERNOS

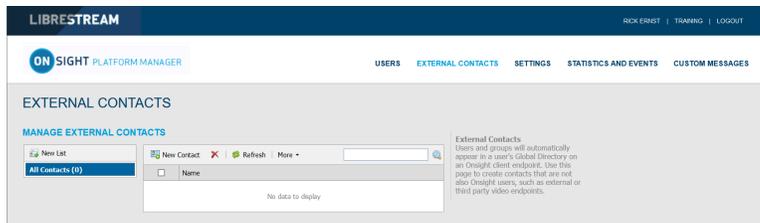


Figura 8-1 Contatos externos

Clique em **EXTERNAL CONTACTS** no menu principal para visualizar todos os contatos externos. Os contatos externos são pontos de extremidade de SIP para vídeo de terceiros, como salas de videoconferência ou qualquer outro dispositivo compatível com SIP que não seja um usuário do OnSight Connect em seu domínio do OnSight.

Por padrão, qualquer usuário adicionado ao OPM é automaticamente adicionado ao **Global Directory**.

### Lista de contatos externos

Você também pode usar o ícone  **New List** para criar uma nova lista de contatos externos que pode ser compartilhada em seus grupos de domínio, licença e política.

### Exportar contatos externos

Você pode exportar seus contatos externos como um arquivo de modelo CSV que pode ser modificado para incluir os contatos da sua organização e, em seguida, pode ser reimportado para o OnSight Platform Manager. Para exportar uma lista de contatos externos, clique em **More > Export** para baixar um modelo `ExportContacts.csv`.



**Nota:** os endereços que você informar devem estar no formato URI do SIP, por exemplo, `videoroom@sipdomain.com`.

O arquivo CSV pode ser modificado, desde que você siga as convenções de nomes de colunas e preencha todos os campos necessários.



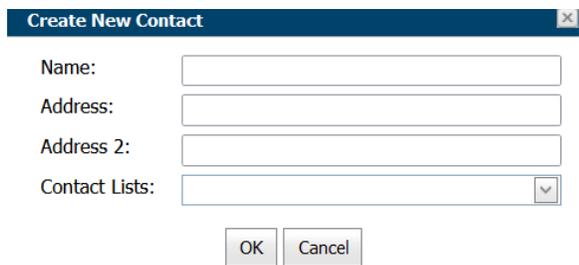
**Dica:** clique em **More > Import** para acessar o link **CSV Import instructions** na seção **Supported file formats** conforme necessário.

## 8.1. Adição manual de um contato externo ao diretório global

Faça login no OPM e selecione **EXTERNAL CONTACTS** no menu principal.

Para adicionar um contato externo manualmente ao Diretório Global:

1. Clique no ícone  **New Contact**.



The image shows a 'Create New Contact' dialog box with the following fields: Name, Address, Address 2, and Contact Lists (a dropdown menu). At the bottom, there are 'OK' and 'Cancel' buttons.

**Figura 8-3 Criar novo contato**

2. Informe o **Name** e **Address** (Endereço 2, se necessário).

 **Nota:** os endereços que você informar devem estar no formato URI do SIP, por exemplo, videoroom@sipdomain.com.

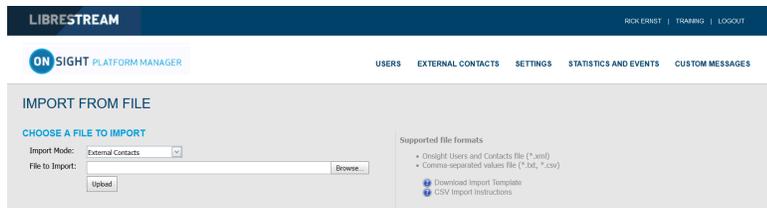
3. Selecione o menu suspenso **Contacts Lists** ao qual adicionar o contato externo.
4. Clique em **OK**. Agora você poderá ver o contato externo ao pesquisar no Diretório Global de um ponto de extremidade Onsign. Isso conclui o procedimento.

## 8.2. Importação de uma lista de contatos externos

Faça login no OPM e selecione **EXTERNAL CONTACTS** no menu principal. Você deve ter criado e modificado previamente um arquivo `ExternalContacts.csv` usando a operação **More > Import > Download Import Template**.

Para importar uma lista de contatos externos revisada como arquivo:

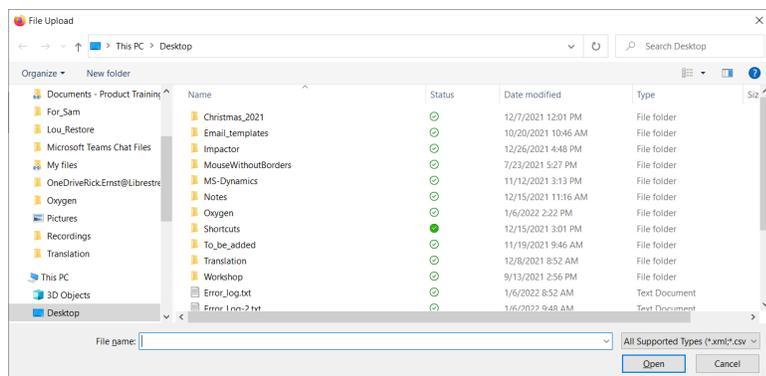
1. Clique em **More > Import**. A janela **IMPORT FROM FILE** é exibida.



The image shows the 'IMPORT FROM FILE' dialog box in the OnSight Platform Manager. It includes a 'CHOOSE A FILE TO IMPORT' section with an 'Import Mode' dropdown set to 'External Contacts' and a 'File to Import' field with a 'Browse...' button. To the right, there are 'Supported file formats' listed: Onsign Users and Contacts file (\*.xml), Comma-separated values file (\*.csv), Download Import Template, and CSV Import Instructions.

**Figura 8-4 Importação a partir de um arquivo**

2. Navegue e selecione o `ExternalContacts.csv` a ser importado clicando no botão **Browse**.



**Figura 8-5 Fazer upload de arquivo**

3. Clique em **Open**.
4. Pressione **Upload**. A janela **Import Users** será exibida.

**Figura 8-6 Janela Importar usuários**

5. Selecione a opção **Duplicate Handling**, que é ideal para a sua situação:
  - **Skip Duplicates** (manter registros existentes)
  - **Update Existing Records**
  - **Create a Duplicate**
6. Clique em **Import**.  
Quando a importação estiver concluída, a janela **Import Results** será exibida.
7. Clique em **View Report** para revisar os detalhes.
8. Pressione **Close**.
9. Volte à página **EXTERNAL CONTACTS** para ver os contatos importados.  
Isso conclui o procedimento.

## 8.3. Adicionar uma lista de contatos externos

Faça login no OPM e selecione **EXTERNAL CONTACTS** no menu principal.

Para criar uma lista de contatos externos manualmente:

1. Localize e selecione o ícone  **New List** abaixo do título MANAGE EXTERNAL CONTACTS.



**Figura 8-7 Gerenciar contatos externos**

2. A janela **Create New Contact List** é exibida.

**Create New Contact List**

Name:

Description:

Global Directory Availability:  Public  
Contacts in this Contact List will be available to everyone in the Global Directory.

Private  
Contacts in this Contact List are available only to specific Groups.

<input type="checkbox"/>	Group
<input type="checkbox"/>	China
<input type="checkbox"/>	Domain
<input type="checkbox"/>	EU
<input type="checkbox"/>	Mobile Users
<input type="checkbox"/>	NA
<input type="checkbox"/>	Volvo

OK Cancel

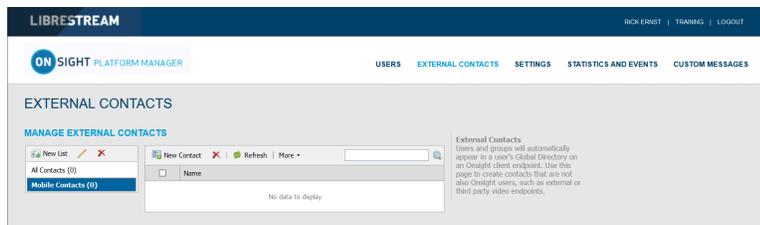
**Figura 8-8 Criar nova lista de contatos**

- Dê um **Name** para a lista e uma descrição.
- Selecione **Public** ou **Private** para definir o nível de acessibilidade para a lista.



**Nota:** se selecionar Private, selecione os grupos que terão acesso à lista.

- A nova lista é exibida abaixo de **All Contacts** em **MANAGE EXTERNAL CONTACTS**.



**Figura 8-9 A nova lista é exibida**

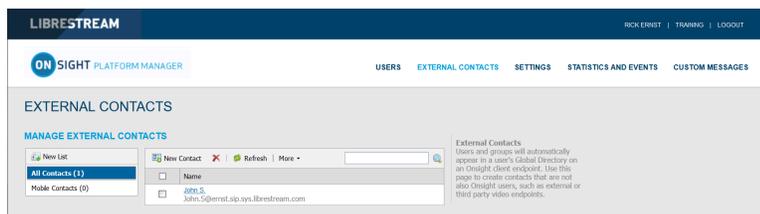
Isso conclui o procedimento.

## 8.4. Adicionar/Remover contatos externos de listas

Faça logon no OPM.

Para modificar os contatos dentro da sua lista de contatos externos:

- Selecione os **EXTERNAL CONTACTS** no menu principal.



**Figura 8-10 Gerenciar contatos externos**

- Selecione a lista à qual pretende que os contatos sejam adicionados.
- Ative a caixa de verificação junto ao(s) contato(s) externo(s) que pretende adicionar à lista.
- Clique em **More > Add to List**.
- Selecione a lista onde os contatos serão adicionados.

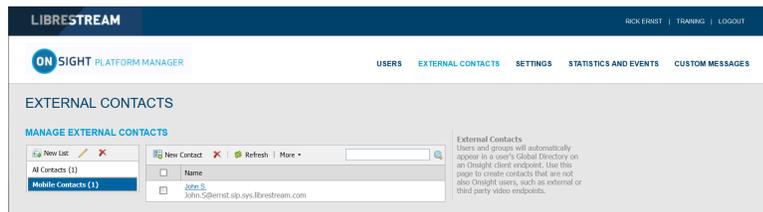


Figura 8-11 O nome de contato é exibido na lista

6. Verifique se o nome do contato aparece na lista.

**i Dica:** é possível remover o nome de um contato de uma lista selecionando a lista, ativando a caixa de seleção ao lado do(s) nome(s) do(s) contato(s) e clicando em **More > Remove from List**.

Isso conclui o procedimento.



# 9. CONFIGURAÇÕES

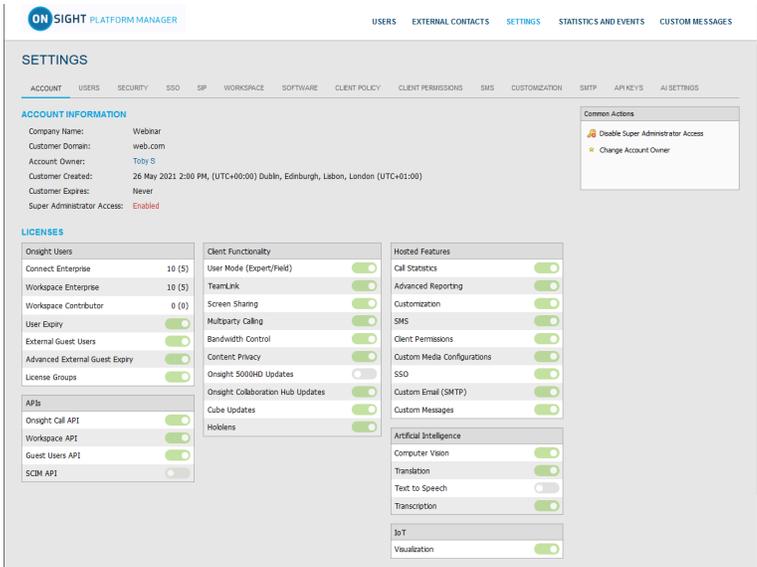


Figura 9-1 Configurações

Clique em **SETTINGS** no menu principal para definir as configurações para cada ponto de extremidade do OnSight para cumprir suas políticas. As configurações são aplicadas ao ponto de extremidade quando um usuário faz logon no OnSight Connect. **External Guest Users** podem ser habilitados em **LICENSES** para que qualquer usuário ativo do OnSight Connect possa convidar um convidado externo por um período definido pelo administrador. As permissões de usuários convidados externos podem ser restritas, mas têm acesso total à experiência de colaboração do OnSight.

Guias adicionais estão acessíveis em **SETTINGS**, que incluem:

- As configurações **SIP** são atribuídas no pool de atribuição automática.
- As configurações de **Software** controlam quais configurações da versão do OnSight Connect podem ser selecionadas e instaladas para sistemas operacionais Windows.
- As configurações de **Client Policy** são selecionadas para cada ponto de extremidade, por exemplo, modo de criptografia.
- São atribuídas configurações de **Security**, que incluem política de senha, política de logon e método de criação de contas de usuário.

Todas as configurações são aplicadas aos pontos de extremidade do OnSight depois que um usuário do OnSight foi autenticado e autorizado durante o processo de logon.

Ao aplicar alterações em uma página de configurações, você deve clicar em **Save** para confirmar as alterações. Clique em **Reset Changes** para retornar às configurações anteriores salvas para a página.

## 9.1. Tempo limite de autenticação

Para permitir o acesso ao conteúdo e serviços de chamadas no caso de perda de conectividade de rede — os usuários permanecem autenticados localmente por 30 dias no cliente após a sua autenticação on-line inicial. Os clientes devem autenticar novamente no serviço on-line pelo menos uma vez a cada 30 dias.

## 9.2. Conta

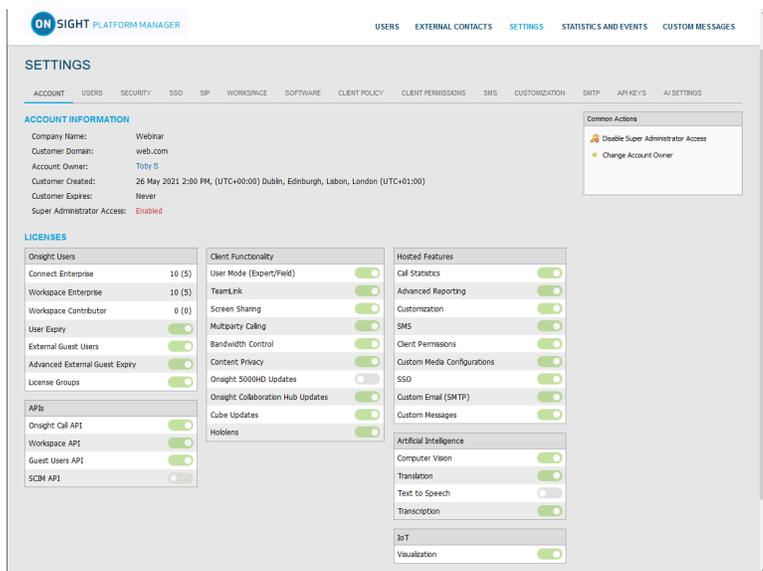


Figura 9-2 Configurações

Clique em **SETTINGS** no menu principal para permitir que você acesse as informações da conta OPM da sua empresa, na guia **ACCOUNT**. A guia ACCOUNT inclui as seguintes seções: Informações da conta, Ações comuns e Licenças.

### Informações da conta

Inclui **Company Name**, **Customer Domain**, **Account Owner**, data de **Customer Created**, data de **Customer Expiry** e **Super Administrator Access**.

### Ações comuns

No painel **Common Actions** à direita, você pode acessar funções adicionais que incluem habilitar/desabilitar  **Disable Super Administrator Access** e  **Change Account Owner**.

### Licenças

As licenças habilitadas no domínio do Onsight estão listadas na seção **LICENSES**.

### Referências relacionadas

[Conta — Práticas recomendadas \(na página 114\)](#)

### 9.2.1. Acesso de superadministrador

No painel **Common Actions**, você pode ativar ou desativar o **Super Administrator Access** ao suporte Librestream. Isso permite especificar o número de horas que deseja conceder ao suporte Librestream para acesso ao seu domínio. A concessão de acesso permite que o suporte Librestream ajude na configuração ou solução de problemas. O acesso de superadministrador pode ser desativado a qualquer momento pressionando **Deny Super Administrator Access**; caso contrário, expirará após o prazo definido.

### NO LOCAL

Ao gerenciar um servidor no local, o acesso de superadministrador não é aplicável. [CONTATO COM O SUPORTE \(na página 107\)](#) se precisar de assistência.

### Referências relacionadas

[Conta — Práticas recomendadas \(na página 114\)](#)

### Informações relacionadas

[CONTATO COM O SUPORTE \(na página 107\)](#)

## 9.2.2. Alterar proprietário da conta

Na seção **Common Actions**, você pode usar **Change Account Owner** para especificar o **OPM Administrator** principal do domínio da conta Onsight. **Change Account Owner** permite que um administrador do Onsight Platform Manager atribua outro usuário como **Account Owner**.

**Dica:** o usuário deve ter privilégios de administrador do Onsight Platform Manager antes de ser designado como proprietário da conta.

### Referências relacionadas

[Conta — Práticas recomendadas \(na página 114\)](#)

## 9.2.3. Licenças

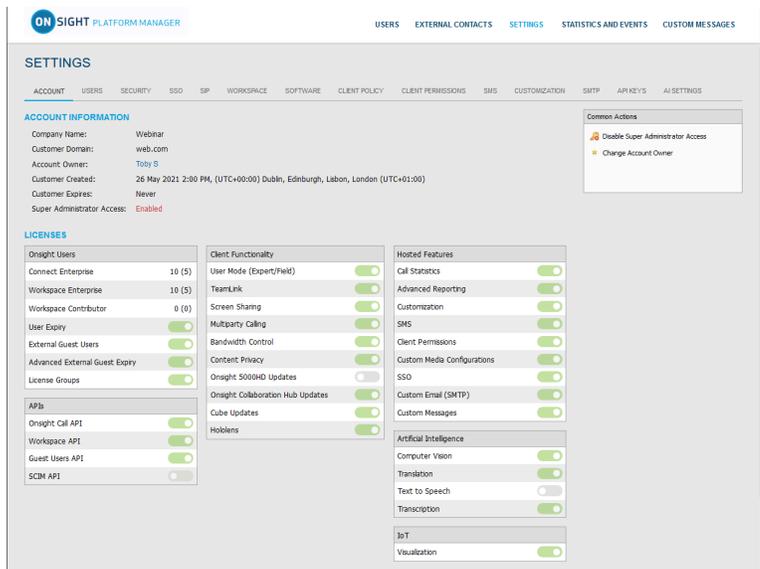


Figura 9-3 Configurações

As licenças habilitadas para o domínio do Onsight estão listadas na seção **LICENSES**. Elas estão divididas em quatro categorias principais:

1. **Onsight Users**
2. **Client Functionality**
3. **APIs**
4. **Hosted Features**

### Referências relacionadas

[Conta — Práticas recomendadas \(na página 114\)](#)

## 9.2.3.1. Usuários Onsight

A seção Usuários Onsight lista o número de licenças por tipo e os recursos de licença. Cada tipo de licença permite funcionalidades dentro dos aplicativos do cliente. Os tipos de licença do usuário incluem:

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

Cada recurso de licença permite a funcionalidade relacionada ao gerenciamento de licenças do usuário. Os recursos de licença incluem:

- **User Expiry** — permite a expiração de contas de usuário
- **External Guest Users** — permite convites para convidados
- **Advanced External Guest Expiry** — permite a expiração de convites para convidados
- **License Groups** — permite o gerenciamento de pool de licenças por grupo

### 9.2.3.2. Interfaces de programação de aplicativos

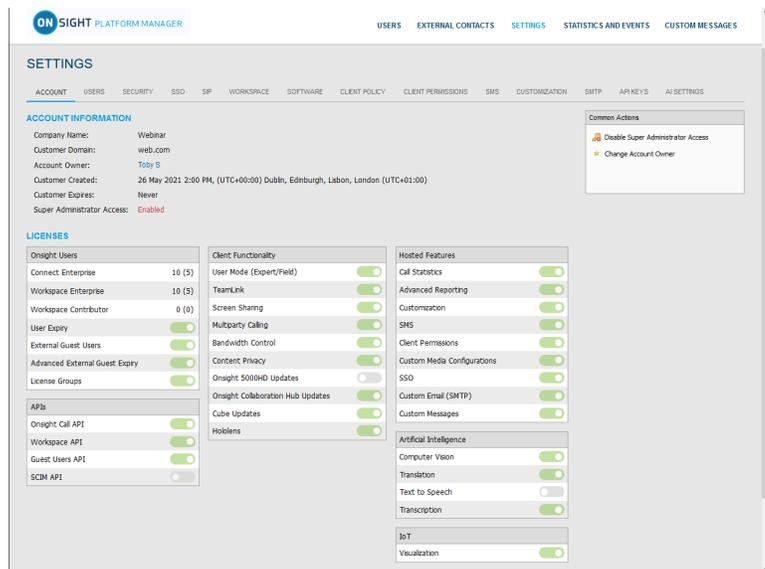


Figura 9-4 Configurações

O OnSight Platform Manager pode ser habilitado para trabalhar com várias APIs (Application Programming Interfaces, interfaces de programação de aplicativos). Clique em **SETTINGS** no menu principal e localize APIs na seção **LICENSES**. As APIs incluem:

- **OnSight Call API** — permite o acesso a **OnSight Call REST API** e **API Key Management**.
- **Workspace API** — permite o acesso a **Workspace REST API** e **API Key Management**.
- **Guest Users API** — permite convidar hóspedes externos.
- **SCIM API** — automatiza o gerenciamento de usuários e grupos.

### 9.2.3.3. Funcionalidade do cliente

Você pode acessar **Client Functionality** clicando em **SETTINGS** no menu principal e localizando-a na seção **LICENSES**. A funcionalidade do cliente pode ser ativada ou desativada para:

- **User Mode (Expert/Field)** — permite que o recurso defina contas de usuário como modo **Expert** ou **Field**. O **Expert Mode** fornece todos os recursos aos usuários. O modo **Field Mode** é uma interface de usuário simplificada com um subconjunto de recursos disponíveis para o usuário. Ao usar o **Field Mode**, devem ser chamados especialistas que controlarão a chamada remotamente.
- **TeamLink** — permite recursos de passagem de firewall do TeamLink para o domínio. O TeamLink permite o túnel de dados HTTPS através de um firewall que não permite tráfego SIP ou de mídia.



**Nota:** ao habilitar o **TeamLink Registration**, você está ativando automaticamente o **TeamLink** para cada ponto de extremidade. Ao habilitar a opção **Always use TeamLink**, você está dizendo ao ponto de extremidade para usar o TeamLink mesmo que as portas SIP no firewall estejam abertas, ou seja, sempre criar túnel do SIP através de HTTP/S.



**Dica:** a Librestream recomenda que a opção **Always use TeamLink** seja **Disabled** e só seja usada por ponto de extremidade para fins de solução de problemas.

- **Screen Sharing** — permite compartilhar qualquer janela com os participantes da chamada.
- **Multiparty Calling** — permite definir PCs Windows e dispositivos Android como hosts de conferência. Quando ativada, o dispositivo pode realizar uma teleconferência com vários participantes. A limitação do número de participantes depende dos recursos de hardware e rede disponíveis para o dispositivo.

 **Dica:** o número máximo de participantes de chamadas pode ser controlado pela **Client Policy**.

- **Bandwidth Control** — permite definir a **Maximum Video Bit Rate** permitida para **Media Configurations**.
- **Content Privacy** — permite controlar a gravação e a captura de imagens em pontos de extremidade usando **Client Policy**.
- **Onsight 5000HD Updates** — permite atualizações da câmera inteligente robusta HD 5000.
- **Onsight Collaboration Hub Updates** — permite implantar atualizações de software em Onsight Collaboration Hubs por meio de clientes iOS ou Android.
- **Cube Updates** — permite atualizações do Onsight Cube.
- **Hololens** — permite a acessibilidade do Hololens à funcionalidade Onsight Connect.

## No local — TeamLink

No momento, o TeamLink não é aceito ao usar em instalações locais, o acesso à Internet pública é necessário para se comunicar com servidores TeamLink.

### 9.2.3.4. Recursos hospedados

Os recursos hospedados podem ser ativados ou desativados para:

- **Call Statistics** — permite capturar estatísticas de chamadas de pontos de extremidade do Onsight.
- **Advanced Reporting** — permite gerar e exportar relatórios avançados de estatísticas de chamadas.
- **Customization** — permite personalizar mensagens do Onsight Platform Manager enviadas aos usuários do Onsight. As mensagens são baseadas em texto e HTML.
- **Client Permissions**
- **SMS** — permite enviar convites para convidados externos via SMS. Permissões do cliente: permite controlar o acesso do usuário às configurações de ponto de extremidade.
- **Custom Media Configurations** — permite implantar configurações personalizadas de mídia pela política do cliente.
- **SSO** — permite o suporte de logon único para o seu domínio. Consulte a seção SSO para obter detalhes de configuração.
- **Custom Email** (SMTP)
- **Custom Messages**

### 9.2.3.5. Inteligência artificial

Os recursos de inteligência artificial (IA) podem ser habilitados ou desabilitados para:

- **Computer Vision** (CV) — permite o acesso aos recursos de CV, inclusive OCR, classificação e localização de objetos, além de marcação automática.
- **Natural Language Processing** (PLN) — permite o acesso ao recurso PLN para acessar o **Onsight Translator**.
- **Transcription** — permite o acesso às funções de transcrição para todas as chamadas.

### 9.2.3.6. Internet das coisas

Os recursos de Internet das coisas (IoT) podem ser habilitados ou desabilitados para **Visualization**. Isso permite o acesso a serviços de IoT, visualização de instrumentos e marcação automática.

### 9.2.4. Anonimização de dados

**Data Anonymization:** essa opção pode ser habilitada mediante solicitação para que seu domínio dê suporte à Lei Geral de Proteção de Dados (LGPD) na Europa e uma legislação relacionada que inclua conformidade com a privacidade dos dados e o Direito ao esquecimento (RTBF).

Quando ativado, os usuários excluídos terão automaticamente seus Dados Pessoais Identificáveis (PII) anônimos. O nome de usuário, o endereço de e-mail e os eventos não estarão mais disponíveis para exibição nos relatórios do Onsight Platform Manager (OPM) nem nas estatísticas de chamadas. Um pseudônimo anônimo será inserido em seu lugar para evitar a identificação do usuário.

 **Nota:** as estatísticas de chamadas, os relatórios e os eventos ainda conterão os dados anônimos para dar suporte a análises e relatórios.

A anonimização dos dados de PII ocorre quando:

- uma conta de usuário é excluída
- um usuário convidado é excluído e/ou sua conta expira

 **Nota:** o conteúdo do Onsight Workspace é propriedade do cliente. Sendo assim, a empresa é responsável por todo o conteúdo. Quando um usuário é excluído, a conta do Workspace também é excluída automaticamente. O cliente deve optar por excluir o conteúdo do usuário conforme necessário.

Além disso, mediante solicitação, a Librestream pode:

- **Anonymize previously deleted users from your domain** — usuários excluídos anteriormente não aparecerão em suas listas de usuários, mas seus dados ainda estarão disponíveis para relatórios se não forem anônimos.
- **Anonymize active user data** — quando habilitado, os dados não serão mais associados ao usuário ativo. Os dados ainda mostrarão a utilização dentro do período determinado.

### 9.2.5. Anonimização programada

A **Scheduled Anonymization** pode ser habilitada mediante solicitação, para que seu domínio converta automaticamente dados pessoais ativos em dados anônimos, conforme definido por um **Data Retention Period** (DRP). No seu próximo ciclo, os dados serão anônimos. Isso elimina a necessidade de processamento manual para os clientes.

 **Nota:** a anonimização programada é desativada por padrão. **Depois que os dados ficam anônimos, isso não é reversível.**

## 9.3. Usuários

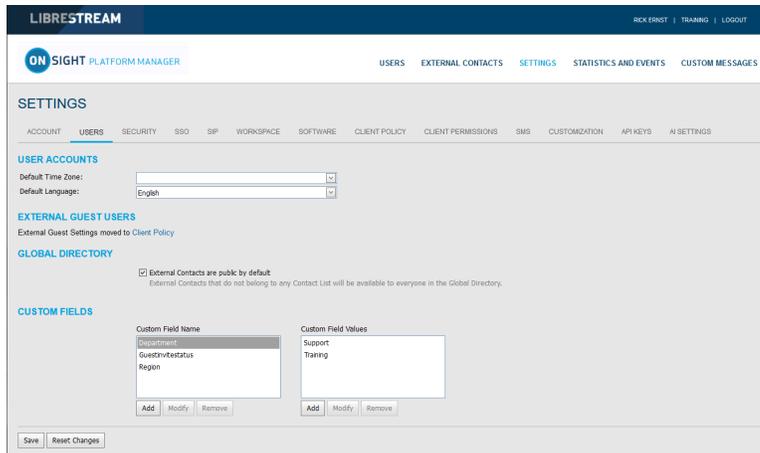


Figura 9-5 Página de usuários

Clique em **SETTINGS** no menu principal e depois na guia **USERS**. A página **USERS** permite definir as configurações globais de convidado externo e usuário para o domínio. A página **USERS** inclui as seguintes seções: **USER ACCOUNTS**, **EXTERNAL GUEST USERS**, **GLOBAL DIRECTORY** e **CUSTOM FIELDS**.

### Referências relacionadas

[Usuários — Práticas Recomendadas \(na página 116\)](#)

### 9.3.1. Contas de usuário

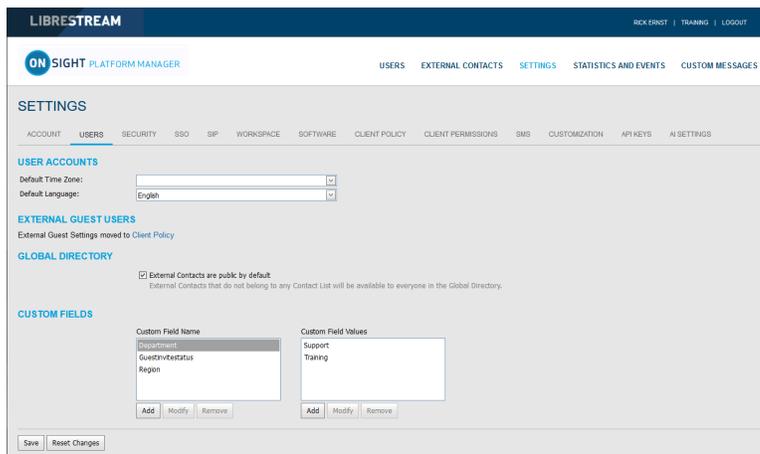


Figura 9-6 Página de usuários

Clique em **SETTINGS** no menu principal e depois na guia **USERS**. A página **USERS** permite modificar as configurações de **USER ACCOUNT** para:

- **Default Time Zone** — selecione o fuso horário desejado para todas as contas de usuário no menu suspenso. Todos os dados relatados pelos clientes OnSight ao OPM são baseados no tempo universal coordenado (UTC). No entanto, a configuração do fuso horário padrão ajustará os dados de registro temporal no OPM apenas para fins de exibição.
- **Default Language** — defina o idioma padrão no menu suspenso.

 **Nota:** os dispositivos OnSight devem ter a data e a hora precisas definidas para usar o serviço OnSight Connect. O HTTPS conta com precisão de tempo/data para realizar a autenticação.

### Referências relacionadas

[Usuários — Práticas Recomendadas \(na página 116\)](#)

## 9.3.2. Usuários convidados externos

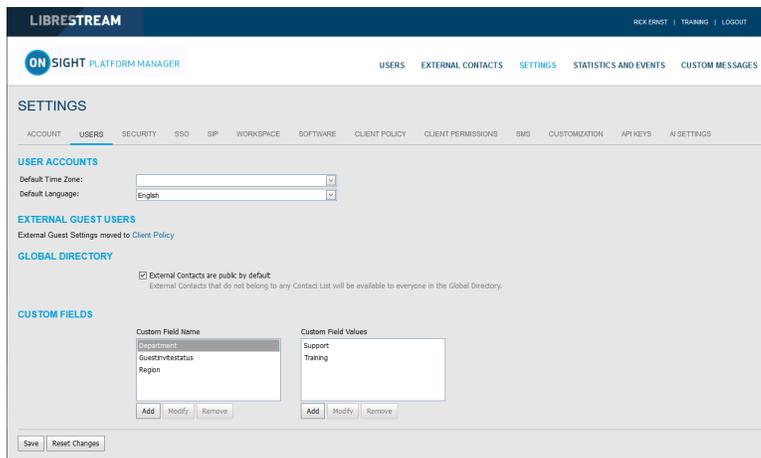


Figura 9-7 Página de usuários

Clique em **SETTINGS** no menu principal e depois na guia **USERS**. A página **USERS** contém uma seção **EXTERNAL GUEST USERS** que permite clicar no atalho da **Client Policy** para modificar essas configurações.



**Nota:** todas as configurações externas de convidados são movidas para **Client Policy**.

### Referências relacionadas

[Usuários — Práticas Recomendadas \(na página 116\)](#)

[Política do cliente — Práticas recomendadas \(na página 120\)](#)

[Permissões do cliente — Práticas recomendadas \(na página 133\)](#)

## 9.3.3. Diretório global

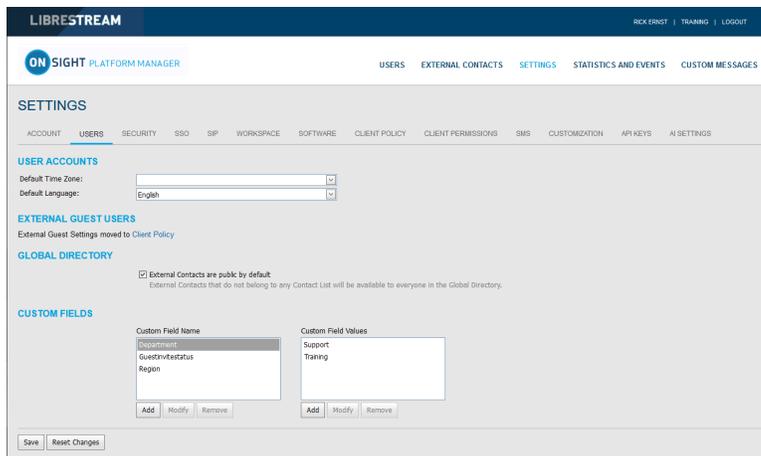


Figura 9-8 Página de usuários

Clique em **SETTINGS** no menu principal e depois na guia **USERS**. A página **USERS** contém uma seção **GLOBAL DIRECTORY**, que controla como os contatos externos são exibidos dentro do Diretório global. Usuários e grupos aparecerão automaticamente no Diretório global em um cliente Onsight. Contatos externos são contatos criados que não são usuários do Onsight — eles incluem pontos de extremidade de vídeo externos ou de terceiros.

Habilite a caixa de seleção **External Contacts are public by default** para verificar se os contatos externos que não pertencem a nenhuma lista de contato estarão disponíveis para todos no Diretório global.



**Nota:** isso se comporta independentemente da configuração de **External Guest Users** que pode desativar o acesso ao Diretório global. Essa configuração controla o acesso padrão do usuário aos **External Contacts** no Diretório global.

### Referências relacionadas

[Usuários — Práticas Recomendadas \(na página 116\)](#)

## 9.3.4. Campos personalizados

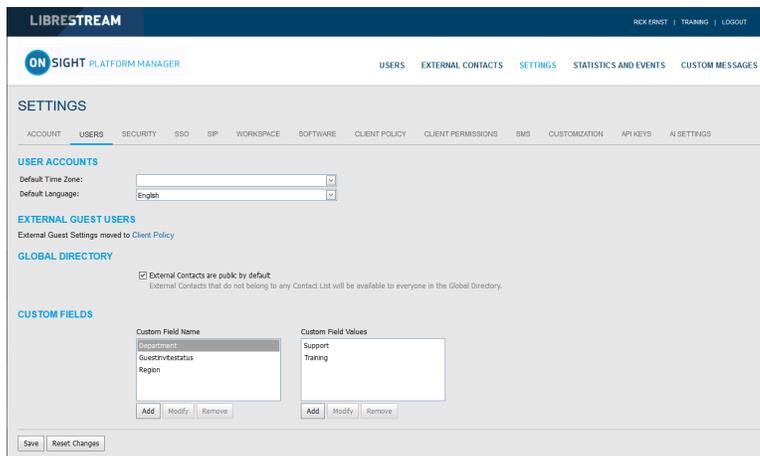


Figura 9-9 Página de usuários

Clique em **SETTINGS** no menu principal e depois na guia **USERS**. A página **USERS** contém uma seção **CUSTOM FIELDS**. Você pode criar campos personalizados para aprender mais sobre seus convidados e melhorar os dados de relatórios. Campos personalizados podem aparecer na página **PROFILE** de um usuário. **Custom Fields** requerem um:

- **Custom Field Name:** adicionar, modificar ou remover o nome do campo personalizado.
- **Custom Field Value:** adicionar, modificar ou remover valores do campo **Custom Field Value**. Os valores do campo personalizado estão incluídos em um relatório de usuário exportado.



**Nota:** os campos personalizados serão incluídos em um relatório de usuário exportado.

### Referências relacionadas

[Usuários — Práticas Recomendadas \(na página 116\)](#)

## 9.4. Segurança

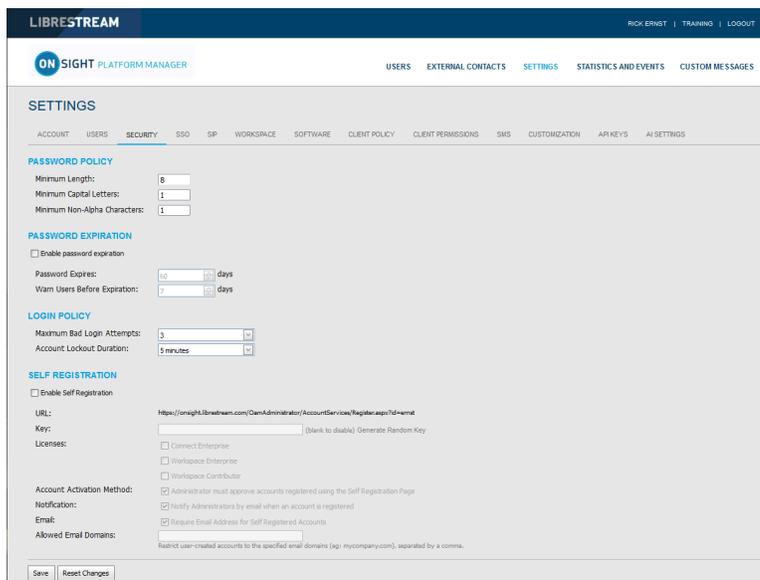


Figura 9-10 Segurança

Clique em **SETTINGS** no menu principal e depois na guia **SECURITY**. A página **SECURITY** é exibida e permite que você modifique suas políticas de senha e logon. As seguintes opções estão disponíveis: **PASSWORD POLICY**, **PASSWORD EXPIRATION**, **LOGIN POLICY** e **SELF REGISTRATION**.

## Referências relacionadas

[Segurança — Práticas recomendadas \(na página 117\)](#)

### 9.4.1. Política de senhas

Clique em **SETTINGS** no menu principal e depois na guia **SECURITY**. A página **SECURITY** é exibida. Localize a seção **PASSWORD POLICY**, onde você pode definir o domínio e a política do cliente para senhas, que incluem:

- **Minimum Length** (caracteres) — digite um valor numérico.
- **Minimum Capital Letters** — digite um valor numérico.
- **Minimum Non-Alpha Characters** — digite um valor numérico.

## Referências relacionadas

[Segurança — Práticas recomendadas \(na página 117\)](#)

### 9.4.2. Expiração de senha

Clique em **SETTINGS** no menu principal e depois na guia **SECURITY**. A página **SECURITY** é exibida. Localize a seção **PASSWORD EXPIRATION** e modifique os seguintes parâmetros:

- Caixa de seleção **Enable password Expiration** — habilite essa opção para forçar a expiração da senha.
- **Minimum** — digite um valor em dias. Por exemplo, Mínimo: 1 dia, Máximo: 365 dias.
- **Warn Users Before Expiration**: defina o comprimento em dias como **Minimum**: 0 dia, ou **Maximum**: 365 dias.

## Referências relacionadas

[Segurança — Práticas recomendadas \(na página 117\)](#)

### 9.4.3. Política de logon

Clique em **SETTINGS** no menu principal e depois na guia **SECURITY**. Localize a seção **LOGIN POLICY** onde você pode modificar sua política de logon para:

- **Maximum Bad Login Attempts** — defina o número de tentativas permitidas antes que o usuário seja bloqueado.
- **Account Lockout Duration** — defina a duração do período de bloqueio como: **5**, **15**, **30** minutos, ou **Forever**, conforme necessário.



**Nota:** a opção **Forever** exige que o administrador desbloqueie a conta para conceder acesso.

## Referências relacionadas

[Segurança — Práticas recomendadas \(na página 117\)](#)

### 9.4.4. Autorregistro

Clique em **SETTINGS** no menu principal e depois na guia **SECURITY**. A página **SECURITY** é exibida. Localize a seção **SELF REGISTRATION**. Essas configurações permitem que os usuários se registrem em uma conta navegando para uma URL de autorregistro. A URL deve ser distribuída pelo administrador e pode ser protegida por uma chave de autorregistro. Os seguintes parâmetros estão disponíveis:

- Caixa de seleção **Enable Self Registration** — permite que o usuário insira suas próprias informações de conta, inclusive nome de usuário, senha inicial, nome, sobrenome, e-mail e a chave de autorregistro (se necessário).
- **URL** — a URL de autorregistro gerada pelo sistema. Isso deve ser distribuído aos usuários que desejam fazer o autorregistro.
- **Key** — digite uma chave de registro para se proteger contra acesso não autorizado a essas contas de usuário. Essa chave deve ser distribuída aos usuários que desejam se autorregistrar.
- **Licenses** — selecione as licenças que cada usuário autorregistrado receberá. Deve haver licenças disponíveis para que o registro seja bem-sucedido.

- **Account Activation Method** — quando habilitado, o administrador deve aprovar contas registradas usando a página de autorregistro.
- **Notification** — habilite a caixa de seleção **Administrator must approve accounts register using the Self Registration Page** para garantir que o administrador seja notificado por e-mail quando uma conta for registrada.
- **Email** — habilite para **Require Email Address for Self-registered Accounts**.
- **Allowed Email Domains** — insira uma lista de valores separados por vírgulas de domínios de e-mail permitidos para usuários autorregistrados. Use essa opção em combinação com a configuração **Required Email** para restringir o acesso a contas autorregistradas.

## Referências relacionadas

Segurança — Práticas recomendadas (na página 117)

## 9.5. Logon único

Figura 9-11 Configurações de SSO

Clique em **SETTINGS** no menu principal e depois na guia **SSO**. A página **SSO** é exibida e permite modificar seus parâmetros de logon. As seguintes opções estão disponíveis: **SINGLE SIGN-ON**, **SAML CONFIGURATION** e **USER IDENTITY FEDERATION**.

O OnSight Platform Manager aceita logon único (SSO) usando Security Assertion Markup Language (SAML v2.0). O SAML é um complemento licenciado para clientes Enterprise e é um padrão aberto para a troca de dados de autenticação e autorização entre duas partes: Um provedor de serviços (SP) e o provedor de identidade (IdP). Nesse caso, o OPM atua como SP para o seu IdP de SSO.

Se você estiver migrando os usuários existentes do OnSight para o SSO, pode pressionar o link **Send Instructions** à direita a fim de selecionar para quais usuários enviar instruções. Você pode selecionar usuários individuais ou grupos. Eles receberão um e-mail com as instruções de logon.

**Nota:** os usuários convidados externos sempre devem fazer logon usando as credenciais do OnSight, ou seja, nome de usuário e senha. Os usuários convidados externos podem fazer logon usando o link de logon incluído no e-mail de convite ou na mensagem SMS que receberam. O nome de usuário e a senha também estão incluídos no e-mail de convite.

**Dica:** entre em contato com <mailto:support@librestream.com> para configurar o SSO.

### 9.5.1. Logon único

Clique em **SETTINGS** no menu principal e depois na guia **SSO**. A página **SSO** é exibida. Localize a seção **SINGLE SIGN-ON**.

Para **Standard Users** e **Administrators**:

- Escolha **Required** ou **Optional** para selecionar se você quer que os usuários apenas façam logon com SSO (obrigatório) ou tenham a opção de se conectarem com sua conta Onsign (opcional).



**Nota:** o proprietário da conta sempre pode fazer logon com suas credenciais de conta Onsign, independentemente de qual opção tenha sido definida.

- **Offline Login:** habilite **Allow clients to operate offline** se quiser que os usuários possam fazer logon nos clientes do Onsign quando o acesso à rede não estiver disponível. Nesse caso, se um usuário não puder acessar o provedor de identidade (IdP), ele ainda poderá fazer logon no Onsign Connect.

## 9.5.2. Configuração do Security Assertion Markup Language

O Security Assertion Markup Language (SAML) é um complemento licenciado para clientes corporativos e é um padrão aberto para a troca de dados de autenticação e autorização entre duas partes.

### 9.5.2.1. Provedor de serviços local

Clique em **SETTINGS** no menu principal e depois na guia **SSO**. A página **SSO** é exibida. Localize **LOCAL SERVICE PROVIDER SETTINGS** na seção **SAML CONFIGURATION**.

Essas configurações habilitam o Onsign Platform Manager como **Service Provider** (SP) no seu **Identity Provider** (IdP).

- **SSO Domain** — fornece o nome do domínio SSO que será usado pelo Onsign. Esse valor é igual ao nome de domínio do Onsign.
- **Entity ID** — fornece o nome do OPM da ID da entidade para o IdP.
- **ACS URL** — fornece o nome do OPM da URL ACS para o IdP.

### 9.5.2.2. Configuração das definições do seu IdP

Faça logon no OPM, selecione **SETTINGS** no menu principal e clique na guia **SSO**. A página **SSO** é exibida. Localize **PARTNER SERVICE PROVIDER SETTINGS** na seção **SAML CONFIGURATION**.

Para configurar manualmente as suas definições de IdP:

1. Pressione o botão **Export SP Metadata** para exportar o arquivo de metadados do provedor de serviços (SP):  
`SPMetadata.xml`.
2. Faça upload do arquivo `SPMetadata.xml` no seu **SSO Identify Provider** (IdP).
3. Baixe o arquivo de metadados de seu IdP.



**Nota:** se necessitar de comunicação criptografada entre o OPM e o seu IdP, você deverá importar o certificado do SP do OPM para o seu IdP.

4. Pressione o botão **Download SP Certificate** para baixar o arquivo de certificado público do **Service Provider** (SP).
5. Faça upload do arquivo `SP Certificate` para o seu **SSO Identify Provider** (IdP). Isso conclui o procedimento.

### 9.5.2.3. Provedor de serviços parceiro

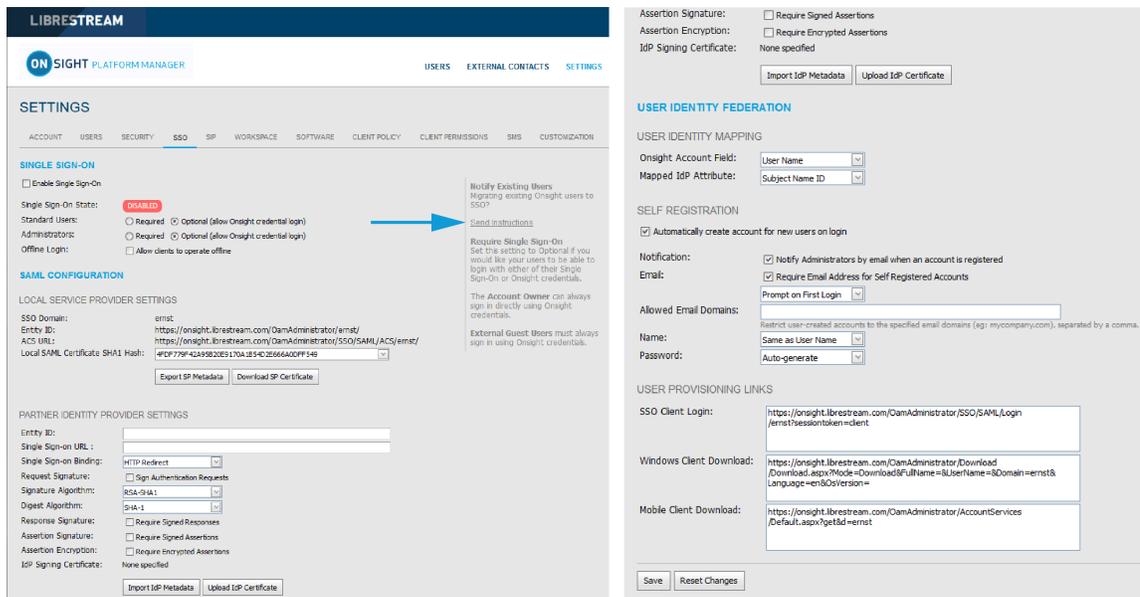


Figura 9-12 Configurações de SSO

Clique em **SETTINGS** no menu principal e depois na guia **SSO**. A página **SSO** é exibida. Localize **PARTNER SERVICE PROVIDER SETTINGS** na seção **SAML CONFIGURATION**.

As configurações do provedor de serviços parceiro informam ao OPM sobre como se comunicar com o **SSO Identity Provider (IdP)**. Na maioria dos casos, você pode usar os botões **Import IdP Metadata** e **Upload IdP Certificate** para configurar o OPM com as definições do seu provedor de identificação de parceiro.

A importação dos metadados fornecerá o seguinte:

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

Você precisará configurar as seguintes opções para corresponder às configurações do seu IdP:

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

Clique em **Import IdP Metadata** para importar o arquivo **IdP metadata** que você baixou do seu provedor de identidade. O arquivo de metadados normalmente contém o certificado público do IdP.

Clique em **Upload IdP Certificate** para fazer upload do **IdP Certificate** (Público). Essa opção é fornecida no caso de ser necessário fazer upload do certificado do IdP manualmente. Na maioria dos casos, o certificado do IdP será fornecido no arquivo de metadados obtido do seu IdP.

### 9.5.2.4. Configuração manual das definições do seu IdP

Faça login no OPM, selecione **SETTINGS** no menu principal e clique na guia **SSO**. A página **SSO** é exibida. Localize **LOCAL SERVICE PROVIDER SETTINGS** na seção **SAML CONFIGURATION**.

Para configurar manualmente as definições do seu IdP:

1. Digite o **Entity ID** ou seu IdP.
2. Digite a **Single Sign-on URL** do seu IdP.
3. Digite o **Sign-on Binding type** (HTTP POST ou redirecionamento HTTP).
4. Se necessário, em Solicitar assinatura, habilite **Sign Authentication Requests**.
5. Se necessário, selecione o **Signature Algorithm** usado pelo seu IdP.
6. Se necessário, selecione o **Digest Algorithm** usado pelo seu IdP.
7. Se necessário, habilite **Require Signed Responses**.
8. Se necessário, habilite **Require Signed Assertions**.
9. Se necessário, habilite **Require Encrypted Assertions**.

### 9.5.3. Federação da identidade do usuário

Clique em **SETTINGS** no menu principal e depois na guia **SSO**. A página **SSO** é exibida. Localize **USER IDENTITY FEDERATION** na seção **SAML CONFIGURATION**.

As configurações da federação da identidade do usuário definem como os usuários corporativos do SSO são associados a contas de usuários do Onsignt.

#### 9.5.3.1. Mapeamento de identidade do usuário

Clique em **SETTINGS** no menu principal e depois na guia **SSO**. A página **SSO** é exibida. Localize **USER IDENTITY FEDERATION** na seção **SAML CONFIGURATION**.

O mapeamento de identidade fornece o link entre as informações do usuário enviadas na declaração SAML e os campos correspondentes da conta Onsignt.

O mapeamento informa ao OPM qual conta de usuário do Onsignt está sendo autenticada pelo SSO. Os atributos mapeados devem ser de igual valor, por exemplo, o **NameID** da declaração SAML deve ser igual ao **Username** do usuário do Onsignt se esses dois atributos forem mapeados. O nome do atributo e os valores diferenciam maiúsculas e minúsculas.

Escolha um dos seguintes métodos de mapeamento:

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

#### 9.5.3.2. Mapeamento do nome de usuário

Faça login no OPM, selecione **SETTINGS** no menu principal e clique na guia **SSO**. A página **SSO** é exibida. Localize **USER IDENTITY MAPPING** na seção **USER IDENTITY FEDERATION**.

Para aplicar o mapeamento de nome de usuário:

1. Selecione o menu suspenso **Onsignt Account Field** para comparar seus valores com o **Mapped IdP Attribute**:
  - **User Name** — nome de usuário da conta Onsignt.
  - **Email Address** — endereço de e-mail: da conta Onsignt.
  - **Federated SSO Id** — ID de SSO federado associado do usuário do Onsignt. Isso é definido pelo administrador do Onsignt e pode ser incluído como parte da lista de usuários importados. Pode ser mapeado para o ID do nome da entidade ou para um atributo da Declaração SAML.

**USER IDENTITY FEDERATION**

USER IDENTITY MAPPING

Onsight Account Field:

Mapped IdP Attribute:  (dropdown menu open with options: User Name, Email Address, Federated SSO 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:

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

Name:

Password:

USER PROVISIONING LINKS

**Figura 9-13 Campo da conta Onsight**

2. Selecione o menu suspenso **Mapped IdP Attribute** para comparar os valores dele com o **Onsight Account Field**:
  - **Subject Name ID**
  - **Attribute** — defina o nome do atributo a ser comparado com o campo de conta Onsight

**USER IDENTITY FEDERATION**

USER IDENTITY MAPPING

Onsight Account Field:

Mapped IdP Attribute:  (dropdown menu open with options: Subject Name ID, Attribute)

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:

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

Name:

Password:

**Figura 9-14 Atributo do IdP mapeado**



**Nota:** importação de usuários: se estiver usando **Federated SSO ID** para fornecer o mapeamento de identidade entre os usuários da sua empresa e as contas de usuários Onsight, você deverá preencher o campo **Federated SSO ID** para cada usuário listado no arquivo UserImport.csv.

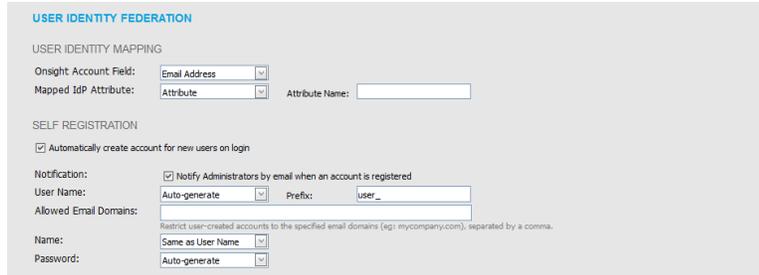
Isso conclui o procedimento.

### 9.5.3.3. Mapeamento de e-mail

Faça login no OPM, selecione **SETTINGS** no menu principal e clique na guia **SSO**. A página **SSO** é exibida. Localize **USER IDENTITY MAPPING** na seção **USER IDENTITY FEDERATION**.

Para aplicar o mapeamento de e-mail:

1. Selecione **Email Address** no menu suspenso **Onsight Account Field**.



**Figura 9-15 Endereço de e-mail**

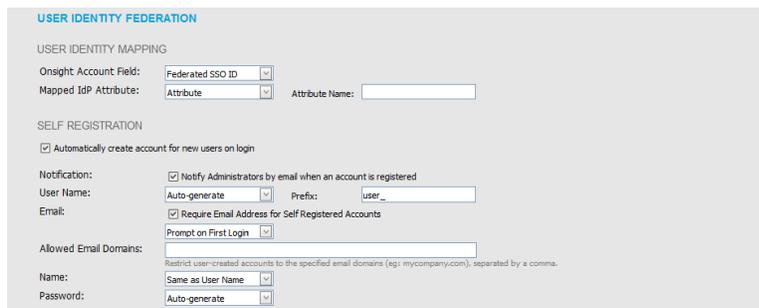
2. Selecione **Attribute** no menu suspenso **Mapped IdP Attribute**.
3. Informe o nome do atributo no campo **Attribute Name**, por exemplo, **Email**. Isso conclui o procedimento.

### 9.5.3.4. Mapeamento de ID de SSO federado

Faça login no OPM, selecione **SETTINGS** no menu principal e clique na guia **SSO**. A página **SSO** é exibida. Localize **USER IDENTITY MAPPING** na seção **USER IDENTITY FEDERATION**.

Para modificar as suas definições de mapeamento de ID de SSO federado:

1. Selecione **Federated SSO ID** no menu suspenso **Onsight Account Field**.



**Figura 9-16 ID de SSO federado**

2. Selecione **Attribute** no menu suspenso **Mapped IdP Attribute**.
3. Informe o nome do atributo no campo **Attribute Name**, por exemplo, **OPMUSER**. (Você poderá definir qualquer nome que quiser.) Isso conclui o procedimento.

## 9.5.4. Autorregistro de SSO

Figura 9-17 Autorregistro de SSO

Clique em **SETTINGS** no menu principal e depois na guia **SSO**. A página **SSO** é exibida. Localize **SELF REGISTRATION** na seção **USER IDENTITY FEDERATION**.

Para ativar o autorregistro, habilite a caixa de seleção **Automatically create account for new users on login**.

 **Nota:** por padrão, se um usuário estiver fazendo logon usando o SSO pela primeira vez e ele ainda não existir como um usuário do OnSight, uma conta OnSight será criada automaticamente para ele.

### Visão geral do autorregistro do SSO

Para habilitar o autorregistro do SSO:

1. Defina suas preferências de **Notification** e **Email**:

- **Notification** — habilite a caixa de seleção **Notify Administrators by email when an account is registered**.
- **Email** — habilite a caixa de seleção **Require Email Address for Self-Registered Accounts**.

2. Defina o método a ser usado para a criação do **User Name**:

- **Attribute** — usa o atributo mapeado como nome de usuário do OnSight.
  - **Attribute Name** — define o nome do atributo que será usado como nome de usuário do OnSight.
- **Auto-generate** — cria o nome de usuário do OnSight.
  - **Prefix** — define o prefixo para nomes de usuário do OnSight gerados automaticamente.
- **Prompt on First Login** — solicita ao usuário que digite um nome de usuário do OnSight.

3. Defina o método **Email** a ser usado para definir o endereço de e-mail do usuário:

- Selecione **Attribute** e o **Attribute Name** para usar no endereço de e-mail do usuário.
- Selecione **Prompt on First Login**, que exigirá que o usuário insira seu endereço de e-mail na primeira vez que fizer logon no OnSight Connect.

 **Nota:** suas configurações de segurança ditam se é necessário um endereço de e-mail para usuários autorregistrados.

4. Defina o nome pessoal do usuário:

- igual a **User Name**.
- **Attribute** — digite os atributos **First Name** e **Last Name** que serão mapeados no nome.
- **Prompt on First Login** — solicita ao usuário que digite o nome e o sobrenome.

5. Defina a opção de criação de **Password**:

- **Auto-generate** — o usuário não precisará saber a senha da conta de usuário do Onsignht. Essa opção só deve ser usada quando o logon de SSO for definido como necessário e for o método de logon aceito.
- **Prompt on First Login** — esta opção deve ser selecionada se (permitir logon de credencial do Onsignht) opcional tiver sido selecionada. Os usuários poderão fazer logon diretamente no Onsignht Connect sem usar suas credenciais de SSO.

## 9.5.5. Links de provisionamento de usuários

**Figura 9-18** Links de provisionamento de usuários

Clique em **SETTINGS** no menu principal e depois na guia **SSO**. A página **SSO** é exibida. Localize **USER PROVISIONING LINKS** na seção **USER IDENTITY FEDERATION**.

Os links a seguir são fornecidos para referência. Você pode incluir esses links em seu e-mail de instruções de implantação da conta Onsignht para seus usuários:

- **SSO Client Login** — o link para a página de logon de SSO.
- **Windows Client Download** — o link de download do Onsignht Connect para Windows.
- **Mobile Client Link** — o link para a página de download do Onsignht Connect para dispositivos móveis.

## 9.5.6. Notificar usuários existentes

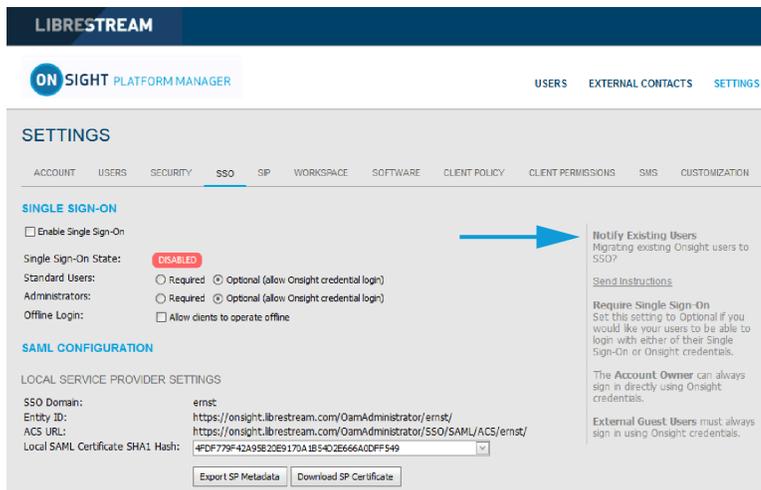


Figura 9-19 Notificar usuários existentes

Clique em **SETTINGS** no menu principal e depois na guia **SSO**. A página **SSO** é exibida. Localize a seção **Notify Existing Users** à direita.

Depois de concluir a configuração de SSO, você pode enviar instruções aos seus usuários existentes por e-mail.

1. Pressione o link **Send Instructions** na seção **Notify Existing Users**.

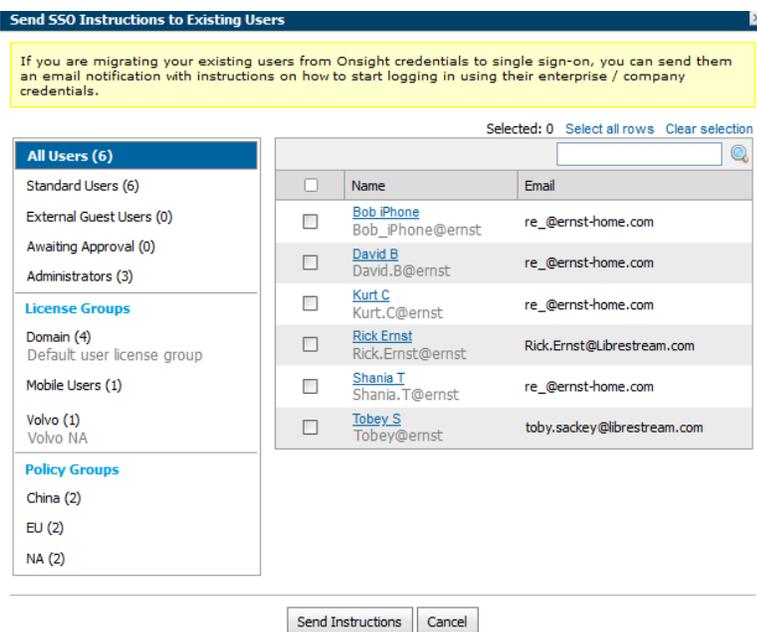


Figura 9-20 Enviar instruções de SSO a usuários existentes

2. Selecione os usuários que deseja notificar e pressione o botão **Send Instructions**. Você pode pressionar o link **Select all rows** para selecionar todos os usuários ou também pode classificar com base nos grupos listados na coluna à esquerda.

## 9.5.7. No local — Configuração do certificado SSO

Para o OPM no local, o servidor que hospeda o OPM deve ter um certificado instalado adequado para criptografia e assinatura SAML. O certificado SSO deve ter as extensões de uso de chave **Digital Signature** e **Key encipherment** e ter o **Extended key usage set** como crítico.

1. Para configurar o OPM para usar o certificado SSO, acesse **Site Administration > Server Settings > General**.
2. Na seção de SSO, cole a impressão digital do SHA1 do certificado na caixa de texto hash do certificado SHA1 do provedor de serviços local.

3. Para verificar o certificado, acesse **Customer Portal > Settings > SSO**.
4. Verifique se o certificado está disponível para uso pelo OPM. Clique no botão **Download SP Certificate**.
5. O certificado deve ser baixado com sucesso.

Consulte o Onsight Platform Manager no local — Guia de instalação para obter detalhes sobre a implantação de certificados de servidor.

## 9.6. Protocolo de início de sessão

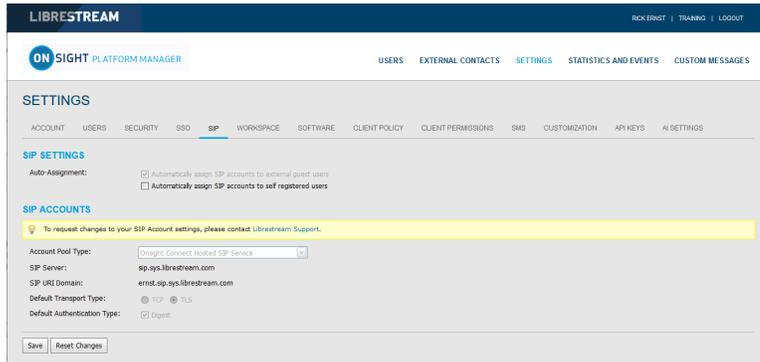


Figura 9-21 Configurações SIP

Clique em **SETTINGS** no menu principal e depois na guia **SIP**. A página **SIP** inclui as seções **SIP SETTINGS** e **SIP ACCOUNTS**.

O protocolo de início de sessão (SIP) é o protocolo de controle de chamadas subjacente que conecta todas as sessões do Onsight Connect. Cada usuário do Onsight Connect terá uma conta SIP automaticamente atribuída a ele. Esta seção descreve as definições do SIP para todos os usuários.

**Dica:** para solicitar alterações nas configurações da sua conta SIP, entre em contato com <mailto:support@librestream.com> para configurar o SSO.

### 9.6.1. Configurações de SIP

#### Atribuição automática de autorregistro

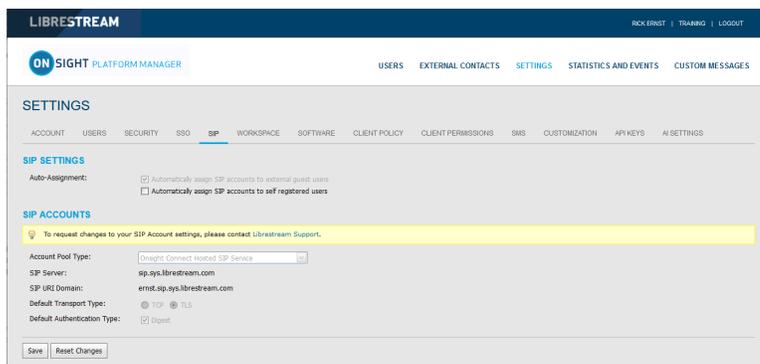


Figura 9-22 Atribuição automática

Clique em **SETTINGS** no menu principal e depois na guia **SIP**. A página **SIP** é exibida. Localize a seção **SIP SETTINGS**.

Quando habilitado, **Automatically assign SIP Accounts to self-registered users** vinculará um usuário recém-registrado a uma conta SIP. Isso deve ser habilitado ao usar o autorregistro.

## 9.6.2. Conta SIP

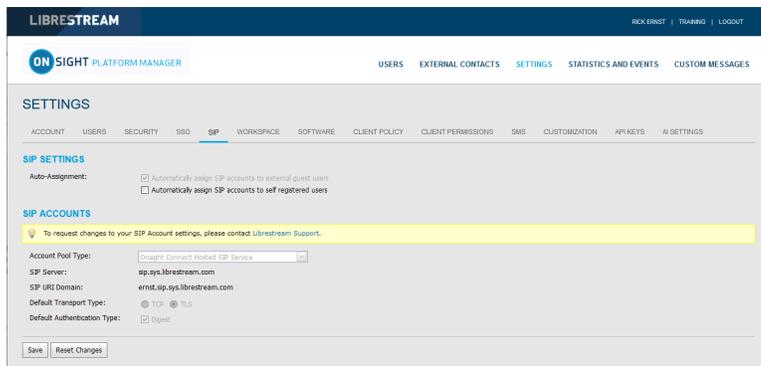


Figura 9-23 Conta SIP

Existem três opções de configuração do servidor SIP acessíveis no menu suspenso **Account Pool Type**.

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

Quando um cliente está hospedando um servidor SIP corporativo, as contas SIP são inseridas no pool de atribuição automática usando várias contas ou uma conta compartilhada.

Ao usar uma conta compartilhada, o servidor SIP deve aceitar nomes de usuário curinga. O URI do SIP (endereço SIP) é gerado automaticamente a partir do domínio URI do SIP e do nome de usuário associado à conta do usuário do OnSight.

O transporte selecionado (TCP ou TLS) deve corresponder à configuração do servidor SIP no qual você está se registrando. O TLS é recomendado para segurança. A data e a hora precisas no ponto de extremidade são um requisito para TLS.

Cada usuário pode receber duas contas SIP: uma pública e uma privada. Isso é para permitir o registro de SIP dependendo da localização da rede. Se um usuário for interno ao Firewall, ele se registrará no servidor privado. Se ele for externo ao Firewall, se registrará no servidor público, por exemplo, no Cisco VCS Expressway e Control.

Os usuários que se registrarem apenas em um servidor SIP (público ou privado) só precisam fornecer configurações de SIP para o servidor único. Use as configurações do SIP público como conta SIP principal.

### 9.6.2.1. Serviço SIP hospedado Onsight Connect

O Serviço SIP hospedado Onsight Connect é o serviço SIP padrão usado quando você se inscreveu no Serviço hospedado Onsight da Librestream.

As configurações são somente leitura, uma vez que as informações da conta SIP são gerenciadas automaticamente pelo OnSight Platform Manager em seu domínio. As contas SIP são automaticamente atribuídas a cada usuário quando uma conta de usuário é criada pelo administrador do OPM.

As configurações do SIP incluem:

- **SIP Server** — lista o servidor SIP Librestream atribuído ao seu domínio.
- **SIP URI Domain** — lista o domínio URI do SIP e aparece como a parte de domínio do endereço SIP de um usuário, por exemplo, user@sipuridomain.com.
- **Default Transport Type** — TCP ou TLS, o padrão é TLS. Isso fornece comunicação criptografada para o protocolo SIP.
- **Default Authentication Type** — resumo fornecido como referência somente leitura.

### 9.6.2.2. Várias contas

Várias contas são usadas quando você está hospedando seu próprio servidor SIP corporativo e tem um número fixo de contas SIP disponíveis para uso com o Onsight Connect. Cada conta SIP é criada em seu servidor SIP corporativo com um nome de autenticação

exclusivo, senha e URI. Em seguida, ela é adicionada manualmente ao pool SIP do OPM para uso à medida que os usuários do Onsight Connect são adicionados.

### 9.6.2.2.1. Criação de várias contas

Faça login no OPM, selecione **SETTINGS** no menu principal e clique na guia **SIP**.

Para criar várias contas SIP:

1. Obtenha as informações da sua conta SIP Enterprise junto do administrador do servidor SIP. As informações da conta SIP devem incluir o endereço do servidor SIP (público e/ou privado), nome de autenticação, senha, nome de usuário e domínio SIP (o nome de usuário e o domínio SIP são combinados para criar o URI do SIP).
2. Na seção **SIP Settings**, selecione **Automatically assign SIP accounts to self-registered users**.
3. Defina **Account Pool Type** como **Multiple Accounts**.
4. Defina **Public Server** como o endereço do servidor público fornecido pelo seu administrador do servidor SIP.
5. Selecione **TCP** ou **TLS** como o tipo de transporte. Recomendamos o TLS.
6. Adicione as informações de contas SIP para cada usuário clicando no botão **New**.
  - Na guia **Public**, informe o URI do SIP (URI do SIP = nome de usuário e domínio SIP, por exemplo, `user@sip.librestream.com`), nome de autenticação e senha de autenticação.
7. Repita as etapas 4 a 6 para o servidor privado, se necessário.
8. Clique em **Save** para salvar as alterações.  
Isso conclui o procedimento.

### 9.6.2.3. Conta compartilhada

Contas compartilhadas são usadas quando você tem contas SIP curinga disponíveis para uso com o Onsight Connect. A conta SIP curinga é primeiramente criada no servidor SIP e adicionada manualmente ao pool SIP do OPM para uso à medida que os usuários do Onsight Connect são adicionados. Cada conta SIP compartilha o mesmo nome de autenticação e senha, mas tem um URI do SIP exclusivo. O URI do SIP é criado automaticamente combinando o nome de usuário do Onsight e o domínio SIP, por exemplo, `jdoe@sipdomain.com`.

#### 9.6.2.3.1. Criação de uma conta compartilhada

Faça login no OPM, selecione **SETTINGS** no menu principal e clique na guia **SIP**.

1. Adquira as informações da sua conta SIP com o administrador do seu servidor SIP. As informações da conta SIP devem incluir **Server Address**, **SIP URI Domain**, **Authentication Name** e **Authentication Password**.
2. Na seção **SIP Settings**, selecione **Automatically assign SIP accounts to self-registered users**.
3. Defina **Account Pool Type** como **Shared Account**.
4. Na guia **Public Server**, defina **Server Address** como o endereço fornecido pelo administrador do seu servidor SIP.
5. Selecione **TCP** ou **TLS** como o transporte. Recomendamos o TLS.
6. Defina **SIP URI Domain** como o domínio fornecido pelo administrador do SIP.
7. Informe **Authentication User Name** e **Authentication Password**.
8. Repita as etapas 3 a 7 na guia **Private Server**, se necessário.
9. Clique em **Save**.  
Isso conclui o procedimento.

## 9.6.2.4. Atribuição manual de contas SIP a usuários

As contas SIP são atribuídas quando uma nova conta de usuário é criada. A caixa de seleção **Automatically assign a SIP account to this user** está habilitada por padrão.

As contas SIP também podem ser atribuídas na guia Usuário e grupos selecionando um usuário existente (marcando a caixa ao lado de seu nome) e, em seguida, selecionando **Assign/Restore SIP Account** do menu suspenso **More**.

Uma vez que as configurações do SIP tenham sido atribuídas/restauradas, as configurações da conta SIP do usuário estarão disponíveis para uso assim que as novas configurações forem recebidas pela conta Onsigth. Isso acontecerá no próximo logon ou, se já estiver conectado, durante a próxima atualização do servidor (dentro de 60 segundos).

## 9.7. Onsigth Workspace

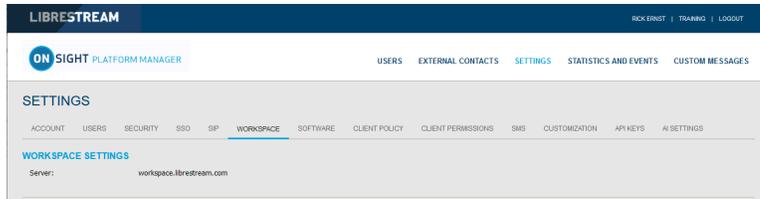


Figura 9-24 Onsigth Workspace

Quando o Onsigth Workspace é habilitado para o seu domínio, o servidor do Workspace é exibido para referência na página de configurações. Como administrador, você deve atribuir a si mesmo uma licença Workspace Enterprise para definir as configurações do Workspace.

Usando o Onsigth Workspace, os usuários autorizados podem fazer upload, visualizar, compartilhar e gerenciar dados, imagens e gravações do Onsigth, bem como conteúdo externo, como manuais de produtos e esquemas. Com controles de permissão detalhados, as empresas podem garantir que apenas equipes e indivíduos autorizados possam acessar conteúdo específico.

O Workspace se integra à plataforma Onsigth completa, fornecendo uma solução prática para auxiliar na gestão do conhecimento e nos requisitos de trilha de auditoria. Os principais recursos do Workspace incluem:

- Upload automático ou manual de dados, imagens ou gravações do Onsigth
- Controles opcionais de upload para gerenciar situações de campo, como o consumo de dados de celular
- Adicionar rapidamente opção para armazenar manuais de produtos, esquemas ou outros arquivos
- Marcação de conteúdo para pesquisa e recuperação rápidas
- Controle de versão automático do conteúdo com recursos de auditoria incorporados
- Arquitetura segura e controles de permissão detalhados
- Relatórios avançados para auditar conteúdo e uso em toda a empresa
- Acesso a conteúdo e dados em seus sistemas de back-office com a API do Workspace
- Seleção dos tipos de licenças Enterprise ou Contributor para controlar e estender a coleta de dados do Workspace

### Referências relacionadas

[Política do cliente — Práticas recomendadas \(na página 120\)](#)

[Permissões do cliente — Práticas recomendadas \(na página 133\)](#)

### 9.7.1. Habilitação do acesso dos usuários ao Workspace

Faça logon no OPM.

Para permitir o acesso ao Workspace aos seus usuários:

1. Acesse a página **Users** e seleccione os usuários a quem você quer dar acesso ao Workspace.

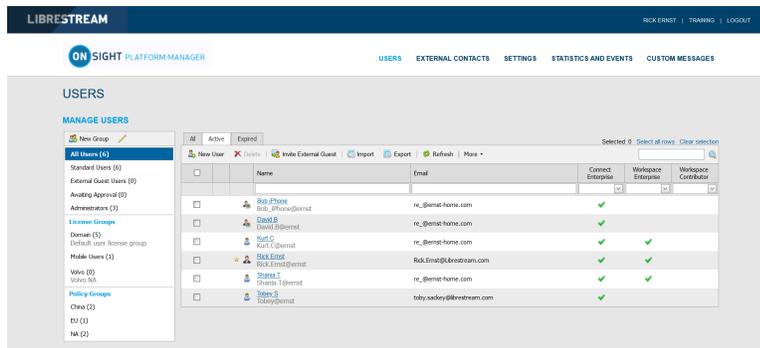


Figura 9-25 Usuários

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

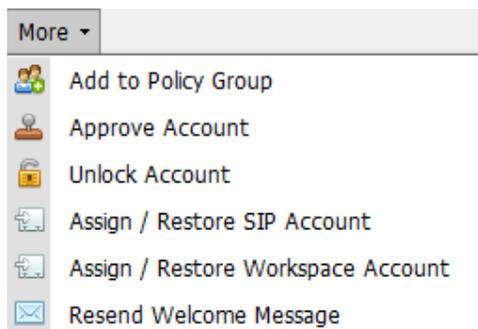


Figura 9-26 Menu suspenso Mais

3. Coloque os usuários do Workspace em um grupo. Você também pode optar por utilizar um grupo existente, como **All Users**.

4. A etapa final é habilitar o Workspace em uma **Group Client Policy** para os usuários.

5. Seleccione o grupo e clique no ícone  **Modify Group** (ícone de lápis).

6. Seleccione a guia **CLIENT POLICY**.

7. Clique em  **Choose Settings**.

8. Seleccione as configurações do **Workspace** a serem habilitadas na **Client Policy** que incluem:

- **Access** — concede acesso ao Workspace.
- **Upload Path** — define o caminho de upload padrão no Workspace.
- **Auto Upload Media** — permite o upload automático de todas as mídias capturadas durante uma chamada quando ela terminar.
- **Maximum Upload Bit Rate (Kbps)** — define a largura de banda máxima dedicada ao fluxo de upload.
- **Restrict Upload Folder Access to the Owner** — só permite o acesso à pasta de upload ao proprietário.
- **Allow Cellular/Mobile Data Usage** — permite o uso de dados de celulares/dispositivos móveis para o upload de mídia no Workspace.

9. Clique em **OK**.

10. Na seção **Workspace**, defina os valores desejados.  
Isso conclui o procedimento.

#### Referências relacionadas

Política do cliente — Práticas recomendadas (na página 120)

Permissões do cliente — Práticas recomendadas (na página 133)

## 9.8. Webhooks do Workspace



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

Figura 9-27 Webhooks

As soluções locais Onsign Workspace e OPM aceitam um mecanismo de notificação de Webhook que permite que um sistema externo notifique você quando alterações são feitas nos ativos do Workspace. A notificação é na forma de retornos de chamada HTTP que são iniciados do Onsign Workspace para o serviço externo designado quando um evento ocorre. Eventos para ativos e documentos do Workspace são acionados quando um item é criado, modificado ou excluído. As notificações do Webhook permitem integrações para uma série de plataformas externas. Para obter mais detalhes, consulte o guia Webhooks do Onsign Workspace.

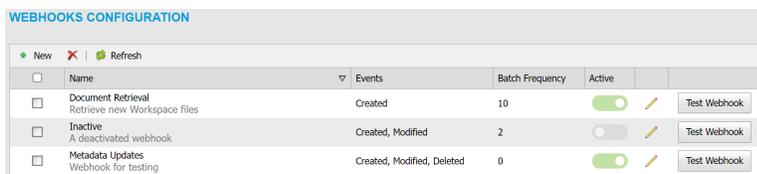
Os Webhooks do Workspace são criados e gerenciados por um administrador do OPM quando o Workspace é ativado e configurado para sua conta.

### 9.8.1. Criação e modificação da configuração de um Webhook

Faça login no OPM como administrador. Clique em **Settings > Workspace**.

Para criar ou modificar a configuração de um Webhook, você vai precisar:

1. Acessar a tabela **Webhooks CONFIGURATION** para exibir uma lista de Webhooks.



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

Figura 9-28 Configuração de Webhooks

2. Clique no ícone  **New** para adicionar a configuração de um Webhook. O formulário New Webhook Configuration é exibido.

Os campos editáveis incluem:

- **Name** (Obrigatório) — um nome amigável para o Webhook que é usado para fins de exibição.
- **Description** — uma descrição opcional para o Webhook.
- **Consumer URI** — o URI absoluto do serviço de destino que receberá notificações de retorno de chamada.
- **HTTP Headers** — fornece uma lista de pares de valores-chave para os cabeçalhos HTTP a serem incluídos em cada notificação enviada a um URI de consumidor.
- **Administrator Email** — o endereço de e-mail do administrador desta configuração de Webhook; todas as notificações de estado e/ou falha de entrega serão enviadas para este endereço de e-mail.
- **Batch Frequency** — a duração máxima dos eventos do Webhook que serão agrupados em lote em uma única notificação em minutos. Se for 0, os eventos serão agrupados em lote dentro de um período mínimo de 10 segundos.
- **User Name/Password** — se definido, a notificação utilizará autenticação HTTP básica com estas credenciais.
- **Active** — se não estiver marcado, não serão entregues notificações para este Webhook.
- **Events** — os tipos de eventos que vão desencadear notificações de Webhook para esta configuração. Você deve selecionar um evento.

**Figura 9-29 Configuração de novos Webhooks**

3. Informe todos os campos necessários e clique em **OK** para salvar a configuração do Webhook.
4. Clique no ícone **Edit**  para mostrar o pop-up **Edit Webhook Configuration**. É idêntico ao pop-up New Webhook Configuration e permite fazer alterações em uma configuração existente.
5. Selecione uma ou mais configurações de Webhook na tabela e clique no ícone **Delete**  para remover permanentemente o(s) Webhook(s). Após a exclusão, nenhuma outra notificação será enviada aos serviços de consumidor para essas configurações.
6. Clique no botão **Test Workbook** na tabela **WEBHOOK CONFIGURATIONS** ou do pop-up **New/Edit Webhook Configuration** para testar a configuração.
  - Uma notificação de evento de teste é acionada imediatamente e enviada ao URI de consumidor a partir do Workspace.
  - O OPM exibirá os resultados dos testes, incluindo a duração do teste e o código de estado devolvido ao Workspace pelo seu serviço de consumidor.

Isso conclui o procedimento.

## 9.9. Atualizações de software

**Figura 9-30 Página Software**

A distribuição de software do OnSight Connect para Windows, do OnSight Cube, do 5000HD e do Collaboration Hub é gerenciada pelo OnSight Platform Manager. A Librestream fornece atualizações como parte do processo de lançamento de software.

### Referências relacionadas

[Software — Práticas recomendadas \(na página 119\)](#)

## 9.9.1. Onsite Connect para Windows

O administrador do OPM pode selecionar qual versão do Onsite Connect para Windows está disponível para download pelos usuários do Onsite Connect. Você pode selecionar a **Latest Published Version** ou uma **Specific Version** na lista suspensa.

Dependendo da sua seleção, os usuários receberão **Welcome emails** ou **External Guest Invites** contendo links para baixar as versões selecionadas do Onsite Connect para Windows.

### Referências relacionadas

[Software — Práticas recomendadas \(na página 119\)](#)

## 9.9.2. Notificações de novos lançamentos

Quando a opção de Última versão publicada for selecionada na página de atualizações de software, os usuários Windows receberão notificações na janela de login do Onsite Connect quando uma nova versão for publicada e estiver disponível para download.

Usuários Android e iOS receberão atualizações de aplicativos através das lojas de aplicativos. Os usuários podem configurar seus telefones para receber atualizações automáticas das lojas de aplicativos. Consulte as instruções da loja de aplicativos do telefone para saber sobre atualizações automáticas.

### Referências relacionadas

[Software — Práticas recomendadas \(na página 119\)](#)

## 9.9.3. Atualizações no Onsite Cube, Collaboration Hub e 5000HD

A Librestream publica as atualizações do Onsite Cube e Collaboration Hub. Elas estão disponíveis no Onsite Platform Manager como parte do processo regular de lançamento de software.

Quando uma nova versão estiver disponível, os usuários poderão usar a opção **Check for Updates** para baixar e instalar a versão de software mais recente, selecionando:

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

## 9.9.4. Atualizações de software no local

Consulte o Onsite Platform Manager — Guia de instalação para obter detalhes sobre a implantação de pacotes de atualização do Onsite Connect para Windows, Onsite 5000HD e Onsite Collaboration Hub. Atualizações de clientes móveis do Onsite estão disponíveis nas lojas de aplicativos para instalações no local.

## 9.10. Política do cliente e Permissões

The left screenshot shows the 'CLIENT POLICY' settings page. It features a sidebar with 'All Users' selected and a main area with a table of settings. The table has columns for 'Description' and 'Value'. Settings include 'User Mode' (Expert), 'Prompt for Permissions' (As Required), 'Enable GPS in Video and Images' (Disabled), 'Screen Sharing' (Disabled), 'Show GPS Overlay' (Disabled), 'Show Device/Time Overlay' (Disabled), 'Copy Captured Image to Gallery / Camera Roll' (Disabled), 'Text Location of Overlay' (Bottom Left), 'Text Size of Overlay' (Small), 'Image Capture Resolution' (Low), 'Wait for Refresh on Last Video Frame' (Disabled), 'Media Path' (empty), and 'Bandwidth Control' (Enable Bandwidth Control).

The right screenshot shows the 'CLIENT PERMISSIONS' table. It has columns for 'Description', 'Action', and 'Calculated Permission'. The table lists various permissions for different user groups, including 'Client Administrators', 'Standard Users', 'External Guest Users', 'License Groups', 'Domain', 'Mobile Users', 'Voice', and 'Policy Groups'. Each row shows a description of the permission, the action (Allow or Deny), and the calculated permission status (Allow or Deny).

Figura 9-31 Política do cliente e Permissões do cliente

**CLIENT POLICY** e **CLIENT PERMISSIONS** podem ser configuradas clicando em **SETTINGS > CLIENT POLICY** ou **CLIENT PERMISSIONS** e são aplicadas ao grupo **All Users**. O grupo Todos os usuários contém todos os usuários no domínio.

**Client Policy** permite que o administrador do OPM escolha quais configurações são aplicadas a um ponto de extremidade Onsite com base na associação ao grupo (Política de grupo) ou em uma política de cliente do usuário atribuída individualmente.

**Group Client Policy** é aplicada a cada membro de um grupo. Selecione a configuração para cada definição com base em grupos. Os usuários podem pertencer a vários grupos, e as configurações que têm uma prioridade maior têm precedência.

**User Client Policy** é a política associada diretamente a uma conta de usuário. É usada para substituir qualquer **Group Policy** aplicada com base na associação ao grupo. Se um usuário pertence a vários grupos, cada um com sua própria **Client Policy** aplicada, o usuário estará sujeito às configurações de política com base na configuração **priorizada** entre as configurações de política de cliente do usuário e do grupo para esse usuário. A política de cliente do usuário padrão para um usuário é **Inherit all** para as configurações, o que significa que **Group Policy** tem precedência. Cada categoria **Client Policy** pode ser definida como **Inherit**, **Override** ou **Clear**.

## Editar política do cliente

Para editar a **Client Policy** para um usuário, selecione o usuário e selecione a guia **CLIENT POLICY**. Defina a política para cada configuração em **Action**. As seguintes opções estão disponíveis:

- **Inherit** — aplica a configuração da política do grupo ao usuário. Este é o padrão para cada configuração quando um novo usuário é criado.
- **Override** — aplica a definição que está configurada na página Política de cliente do usuário, e não na Política do grupo.
- **Clear** — não aplica nenhuma política para as configurações, em vez disso, usa o valor atual no ponto de extremidade.

### Referências relacionadas

[Precedência de prioridade e política do cliente \(na página 109\)](#)

[Política do cliente — Práticas recomendadas \(na página 120\)](#)

[Permissões do cliente — Práticas recomendadas \(na página 133\)](#)

## 9.10.1. Usuários convidados 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', 'Mobile Users', 'VoIP', and 'Policy Groups'. The 'External Guest Users' section is currently selected and displays a table of settings. The table has two columns: 'Description' and 'Value'. 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 (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' (Department and GuestInviteStatus, both Required), and 'Allow Setting User Mode while inviting guest' (Disabled).

Figura 9-32 Política de clientes do grupo

**Nota:** o comportamento do usuário convidado agora é definido no nível do grupo. Não é mais uma configuração de nível de domínio.

- **Allow users to invite external guest** — permite que os usuários enviem convite aos convidados. **Default: Enabled.**
- **Allow text message guest invitations** — permite que os usuários usem mensagens de texto para convites. **Default: Enabled.**
- **SMS Max Message to User Length** — define o número de caracteres permitidos na mensagem SMS. **Default: 100.**

 **Nota:** as mensagens SMS são limitadas a um máximo de 160 caracteres ou menos, dependendo do conjunto de caracteres usado. Exceder esse limite pode quebrar os links contidos na mensagem SMS. Respeite esse limite ao fazer alterações nas mensagens SMS. Consulte a ajuda de mensagens personalizadas na página **PERSONALIZAÇÃO**.

• **Password** — controla se os usuários convidados externos devem alterar a senha temporária no logon inicial. A opção **Default** é **Enabled**.

 **Nota:** você pode desativar esse recurso para usuários convidados a fim de simplificar a sua experiência de chamada do Onsite.

• **Confirmation** — controla se a pessoa que envia o convite receberá uma confirmação por e-mail quando o convite tiver sido enviado. Isso incluirá uma cópia da mensagem de convite. As cores ajudam a comunicar o status de um convite. Por exemplo:

- **Yellow** — o convite foi enviado, e o status é desconhecido. Isso normalmente indica que o provedor de serviços de e-mail ou SMS do convidado não reconheceu o recebimento da mensagem.
- **Green** — o convite foi recebido pelo convidado.
- **Red** — o convite não foi entregue.

 **Nota:** o status do convite é informado ao lado do nome do convidado na lista de contatos da pessoa que envia o convite.

• **Permissions** — defina **Disable recording of images e video** para evitar que um convidado faça gravações do Onsite ou capture imagens estáticas do Onsite. A opção **Default** é **Enabled**, ou seja, usuários convidados externos não podem gravar imagens e vídeos.

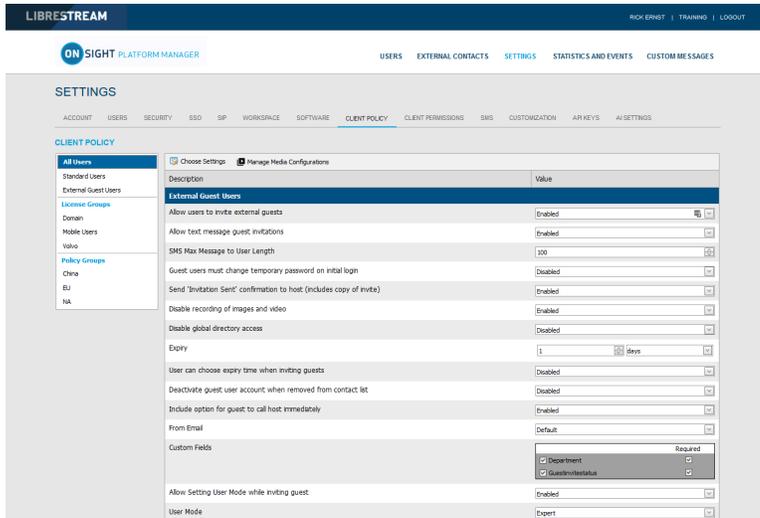
 **Dica:** se desejar, marque **Disable global directory access** para impedir que um convidado pesquise no **Global Contacts Directory**. **Default:** **Disabled**, ou seja, usuários **External Guest** podem acessar o **Global Directory**.

## Referências relacionadas

[Política do cliente](#) — Práticas recomendadas (na página 120)

[Permissões do cliente](#) — Práticas recomendadas (na página 133)

## 9.10.2. Padrões de convite para convidados externos



The screenshot displays the 'CLIENT POLICY' settings in the OnSight Platform Manager. The interface includes a navigation menu on the left with options like 'All Users', 'Standard Users', and 'External Guest Users'. The main content area is a table with columns for 'Description' and 'Value'. The table lists various settings such as 'Allow users to invite external guests' (Enabled), 'SMS Max Message to User Length' (100), and 'Disable global directory access' (Disabled). A 'Custom Fields' section is also visible, showing options for 'Department' and 'Guest/invitee'.

Description	Value						
<b>External Guest Users</b>							
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	<table border="1"><thead><tr><th></th><th>Required</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/> Department</td><td><input type="checkbox"/></td></tr><tr><td><input checked="" type="checkbox"/> Guest/invitee</td><td><input type="checkbox"/></td></tr></tbody></table>		Required	<input checked="" type="checkbox"/> Department	<input type="checkbox"/>	<input checked="" type="checkbox"/> Guest/invitee	<input type="checkbox"/>
	Required						
<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 do cliente de convidado externo

Essas configurações controlam mensagens de convite para convidados:

- **Expiry** — define a expiração padrão da conta de usuário do convidado externo que é criada quando o convite para convidado é enviado. **Default:** 1 dia. **Minimum:** 1 dia, **Maximum:** 365 dias. Os usuários podem escolher o tempo de expiração ao enviar convites para convidados: controla se os usuários podem escolher um tempo de expiração diferente do padrão. A opção **Default** é **Disabled**.
- **Deactivate guest user account when removed from contact list** — controla se a conta do usuário convidado é automaticamente desativada quando a pessoa que envia o convite exclui o convidado de sua lista de contatos. **Default:** **Disabled**.
- **Include option for guest to call host immediately** — controla se o usuário convidado é solicitado a chamar a pessoa que envia o convite na primeira vez que faz logon. A opção **Default** é **Enabled**.
- **From Email Address** — define o endereço de resposta que é exibido no e-mail de convite. Você pode escolher o padrão do sistema ou o endereço de e-mail da pessoa que envia o convite como o endereço de resposta. O **Default** para o Onsight Platform Manager é `no-reply@librestream.com`.



**Nota:** a pessoa que envia o convite deve ter um e-mail configurado para sua conta. Se não houver nenhum e-mail, o padrão do sistema será usado.

- **Custom Fields** — defina **Custom Fields** para incluir no formulário de convite para convidados.
- **Allow Setting User Mode while inviting guest** — define o modo do convidado como **Expert** ou **Field**.

#### Referências relacionadas

[Política do cliente — Práticas recomendadas \(na página 120\)](#)

[Permissões do cliente — Práticas recomendadas \(na página 133\)](#)

### 9.10.3. Precedência da política

Os usuários que pertencem a vários grupos terão configurações aplicadas dando precedência à configuração **priorizada** de **Client Policy**. Por exemplo, se Bob pertence a dois grupos: **Vendas** e **Suporte**. O grupo **Vendas** tem o modo **Encryption** definido como **Off**, mas **Suporte** tem **Encryption** definido como **Auto**. Portanto, quando Bob fizer logon, sua configuração será definida como **Encryption** é **Auto**. Para que Bob receba uma configuração de política do cliente definida como **Encryption** está **Off**, ele pode ser **removido do grupo Suporte**, ou a configuração de **Encryption** pode ser definida como **Override** nas configurações da **Client Policy** do usuário de Bob.

Por padrão, todos os usuários do domínio da conta Onsight pertencem ao grupo **All Users**. No exemplo acima, defina o modo de criptografia como **On** na política **All Users**. Quando Bob fizer logon, sua configuração poderá ser definida como **Encryption** está **On**, uma vez que é uma prioridade maior do que a configuração de criptografia no grupo **Vendas** ou **Suporte**. Como Bob não pode ser removido do grupo **All Users**, a única maneira de dar a ele uma configuração de criptografia de menor prioridade seria a opção de **Override** das configurações da **Client Policy** do usuário de Bob.

#### Referências relacionadas

[Precedência de prioridade e política do cliente \(na página 109\)](#)

[Política do cliente — Práticas recomendadas \(na página 120\)](#)

[Permissões do cliente — Práticas recomendadas \(na página 133\)](#)

#### 9.10.3.1. Configuração da política do cliente

Faça logon no OPM, clique em **SETTINGS** no menu principal e selecione a guia **CLIENT POLICY**.

1. Selecione um **Group** na seção **CLIENT POLICY** à esquerda para aplicar uma política.

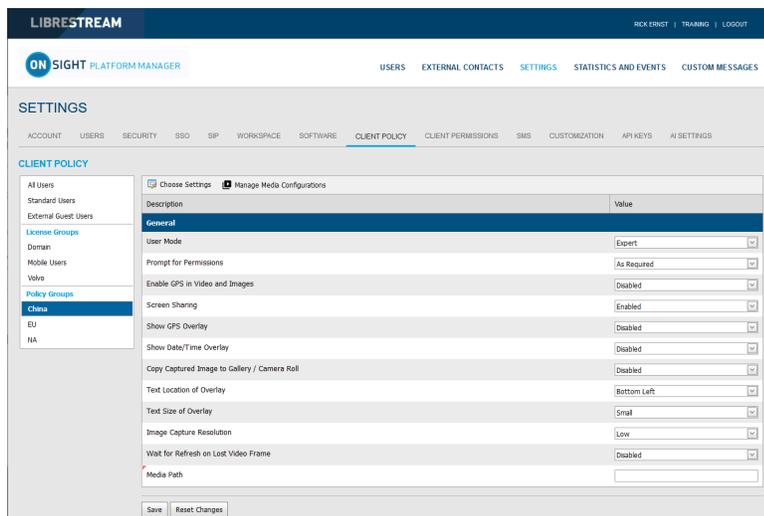


Figura 9-34 Política de clientes do grupo

2. Clique no ícone  **Choose Settings**. Você verá a janela **Choose Settings**.

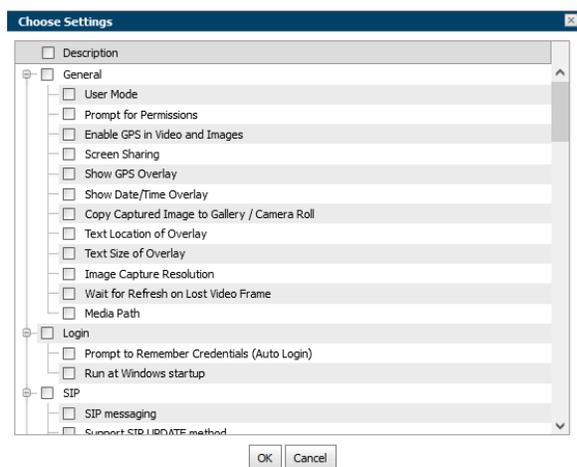


Figura 9-35 Escolher configurações

3. Sob cada categoria, selecione cada configuração que quer gerenciar ou clique no título **Category Section** para ativar todas. Clique em **OK**.
4. Clique em **Save**.
5. Defina o valor apropriado para cada configuração.

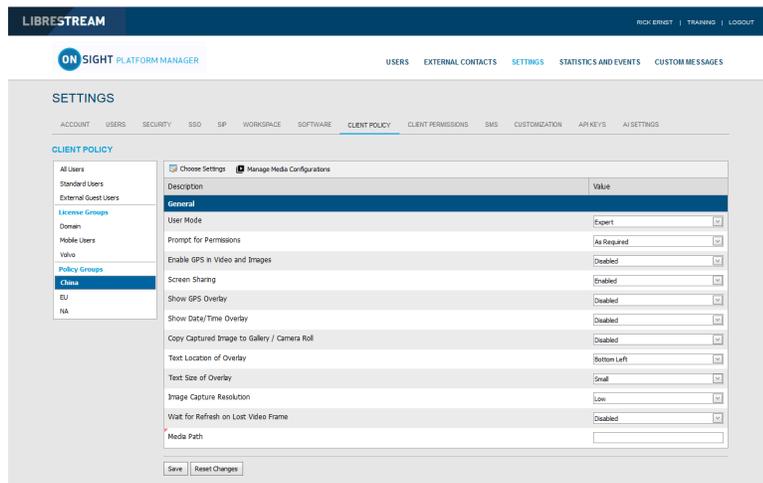


Figura 9-36 Configuração de valores

6. Repita o processo para cada grupo ao qual quer aplicar uma **Client Policy**.



**Nota:** as políticas do cliente podem ser aplicadas a usuários convidados externos, permitindo gerenciar configurações de privacidade.

Isso conclui o procedimento.

### Referências relacionadas

[Política do cliente — Práticas recomendadas \(na página 120\)](#)

[Permissões do cliente — Práticas recomendadas \(na página 133\)](#)

## 9.10.3.2. Configuração das permissões do cliente

Faça login no OPM, clique em **SETTINGS** no menu principal e selecione a guia **CLIENT PERMISSIONS**.

1. Selecione o **Group** que você quer gerenciar.

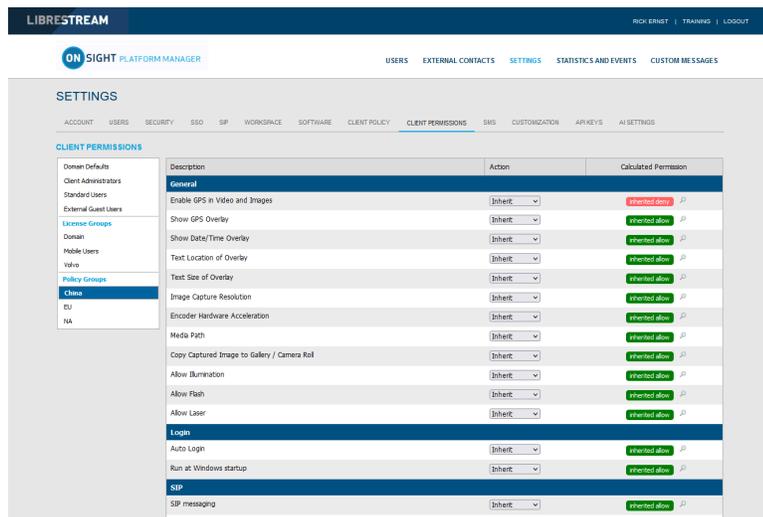


Figura 9-37 Configuração das permissões do grupo

2. Para cada configuração em **Description**, aplique a ação que você quer para a permissão.

- **Allow** — permite que os usuários editem a configuração.
- **Deny** — desativa a capacidade de edição e não permite que os usuários editem a configuração.
- **Inherit** (disponível apenas se o grupo for um filho de um grupo de pais).

- Clique em **Save**.  
Isso conclui o procedimento.

Consulte a seção **Client Policy** e **Permissions** para obter mais detalhes.

### Referências relacionadas

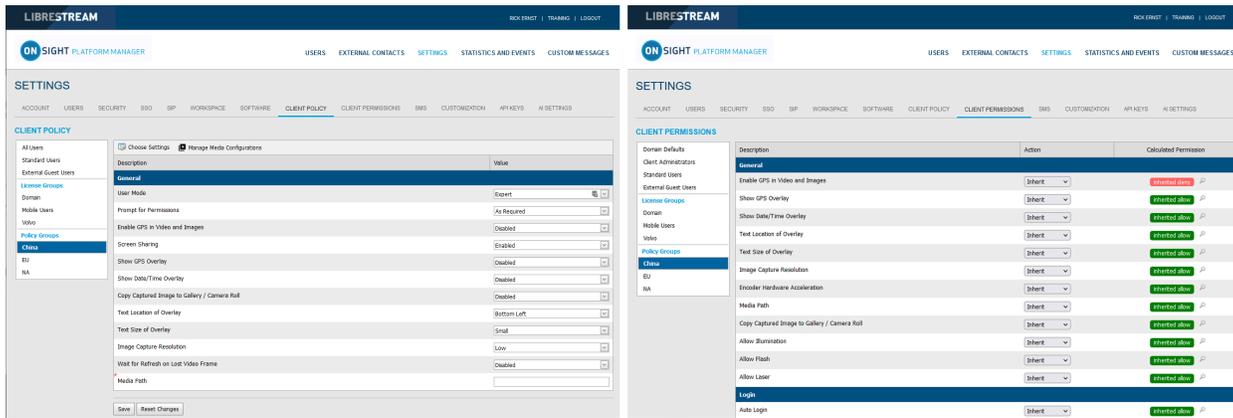
[Política do cliente — Práticas recomendadas \(na página 120\)](#)

[Permissões do cliente — Práticas recomendadas \(na página 133\)](#)

### Informações relacionadas

[Política do cliente e Permissões \(na página 77\)](#)

## 9.10.4. Política e permissões de cliente do grupo



**Figura 9-38** Política e permissões de cliente do grupo

A política de cliente do grupo é gerenciada na página **USERS** editando grupos. Quando uma política de cliente do grupo é criada, ela é aplicada aos membros do grupo cada vez que eles fazem logon em um ponto de extremidade do OnSight Connect. Se os usuários estão fazendo logon em um **PC Windows, iOS, smartphone Android** ou uma **OnSight Smart Camera**, a **Client Policy** atribuída a eles será aplicada.

O modelo de configurações padrão do OnSight Platform Manager descreve todas as configurações disponíveis e fornece diretrizes de práticas recomendadas. Ele está disponível na seção OPM em **Manuals and Guides** no [site de suporte OnSight](#).

As **Client Permissions** do grupo determinam a autorização do acesso do usuário às configurações em um ponto de extremidade do OnSight. Para cada configuração, você pode selecionar **Allow**, **Deny** ou **Inherit** para definir o acesso de permissão para a configuração. Quando um usuário estiver conectado ao software OnSight Connect, **Allow** permitirá que ele edite a configuração, **Deny** impedirá o acesso e **Inherit** aplicará a permissão com base no pai do grupo **Client Permissions** atual. Todos os grupos **Client Permissions** herdarão do grupo pai de padrões de domínio. Consulte a seção de precedência da política [RE Insert XREF] para obter detalhes.

### Referências relacionadas

[Política do cliente — Práticas recomendadas \(na página 120\)](#)

[Permissões do cliente — Práticas recomendadas \(na página 133\)](#)

### Informações relacionadas

[Política do cliente e Permissões \(na página 77\)](#)

## 9.10.5. Privacidade de vídeo remoto

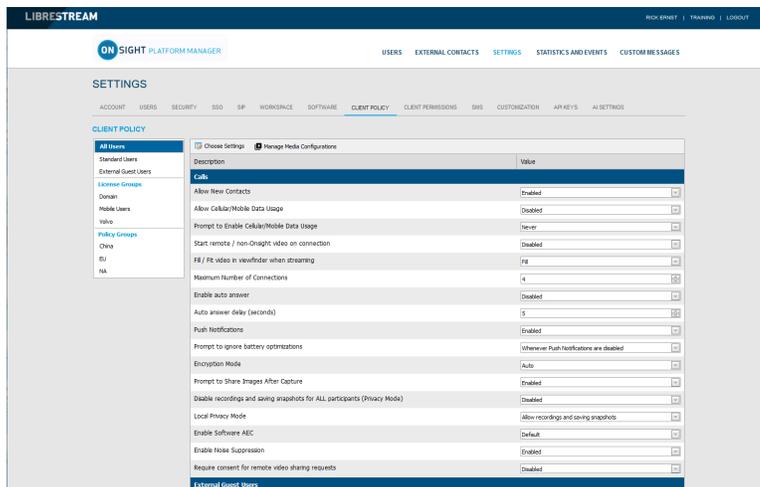


Figura 9-39 Configurações de privacidade

As configurações de privacidade do OnSight exigem consentimento para solicitações de compartilhamento de vídeo remoto durante uma chamada do OnSight. Quando ativado, isso dá aos clientes maior controle sobre o compartilhamento de vídeo, e os usuários devem consentir antes que um participante remoto possa ver o vídeo de sua câmera.

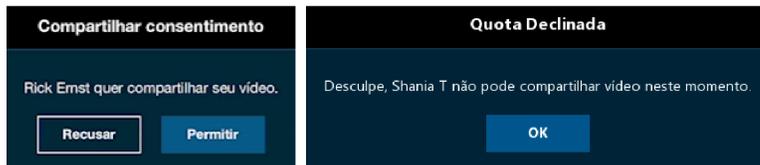


Figura 9-40 Exigência de consentimento

A privacidade de vídeo é aprimorada em locais confidenciais, exigindo que os usuários forneçam consentimento antes de compartilhar vídeo. A privacidade de vídeo remoto afeta:

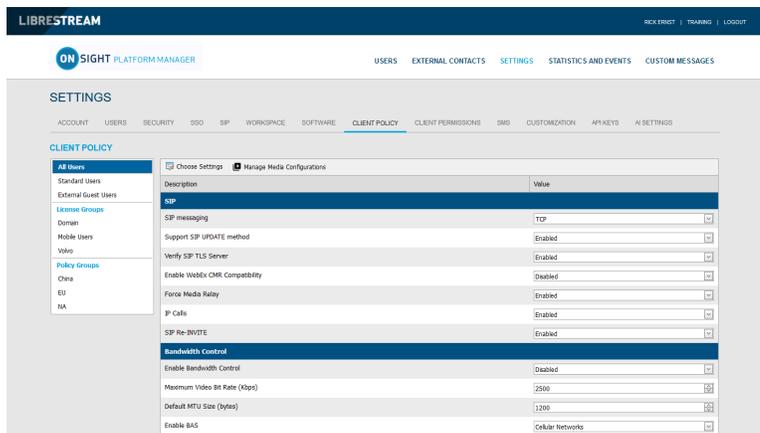
- **Client Policy > Calls** — requer consentimento para solicitações de compartilhamento de vídeo remoto. As opções incluem:
  - **Enabled** — força o usuário a conceder permissão para transmitir conteúdo de sua câmera.
  - **Disabled** (Padrão) — concede automaticamente permissão para transmitir conteúdo de sua câmera.
- **Client Permissions > Calls** — requer consentimento para solicitações de compartilhamento de vídeo remoto. As opções incluem:
  - **Allow** — concede permissão para que a câmera seja compartilhada.
  - **Decline** (Padrão) — nega acesso à câmera com a mensagem: "Não é possível compartilhar vídeo neste momento".

### Referências relacionadas

[Política do cliente](#) — Práticas recomendadas (na página 120)

[Permissões do cliente](#) — Práticas recomendadas (na página 133)

## 9.10.6. Compatibilidade com WebEx CMR



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', 'Video', 'Policy Groups', 'China', 'EU', and 'NA'. The main area is a table with columns 'Description' and 'Value'. Under the 'SIP' section, the following settings are visible:

Description	Value
SIP messaging	TCP
Support SIP UPDATE method	Enabled
Verify SIP TLS Server	Enabled
Enable WebEx CMR Compatibility	Disabled
Force Media Relay	Enabled
P-Calls	Enabled
SIP Re-INVITE	Enabled

Below the SIP section is the 'Bandwidth Control' section with settings like 'Enable Bandwidth Control' (Disabled), 'Maximum Video Bit Rate (Kbps)' (2500), 'Default MTU Size (bytes)' (1200), and 'Enable B4S' (Cellular Networks).

Figura 9-41 Política do cliente

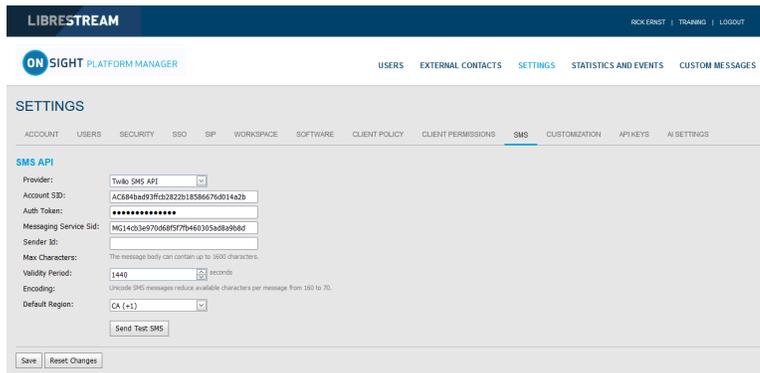
Acesse a **Client Policy** e localize a seção **SIP** para habilitar **WebEx CMR Compatibility**. A **WebEx CMR Compatibility** permite que os pontos de extremidade Onsight liguem para as salas de reunião do WebEx e atuem como um ponto de extremidade de streaming de vídeo/áudio. As salas de reunião do WebEx não aceitarão chamadas do Onsight, a menos que esse recurso esteja habilitado.

### Referências relacionadas

[Política do cliente — Práticas recomendadas \(na página 120\)](#)

[Permissões do cliente — Práticas recomendadas \(na página 133\)](#)

## 9.11. Serviço de mensagens curtas



The screenshot shows the 'SMS' settings page. The 'SMS API' section is expanded, showing the following configuration fields:

- Provider: Twilio SMS API
- Account SID: AC384ba93f02822b18386676d014a2b
- Auth Token: [Redacted]
- Messaging Service Sid: MG1403a97066577b460305a08a9080
- Sender ID: [Redacted]
- Max Characters: The message body can contain up to 1600 characters.
- Validity Period: 1440 seconds
- Encoding: Unicode SMS messages reduce available characters per message from 160 to 70.
- Default Region: CA (+1)

Buttons for 'Send Text SMS', 'Save', and 'Reset Changes' are visible at the bottom.

Figura 9-42 Configurações de SMS

Clique em **SETTINGS** no menu principal e depois na guia **SMS**. A página **SMS** inclui a seção **SMS API** para configurar o serviço de mensagens. Isso está incluído como parte das assinaturas da plataforma Enterprise e Pro.

O SMS permite que os usuários enviem convites para convidados externos por meio do serviço de mensagens SMS para clientes de telefonia móvel.

 **Nota:** a Librestream configura a página de configurações de SMS para o cliente — essas configurações não devem ser alteradas. Entre em contato com o suporte da Librestream para obter assistência se estiver enfrentando algum problema com convites para convidados por SMS.

### Informações relacionadas

[CONTATO COM O SUPORTE \(na página 107\)](#)

## 9.12. Personalização

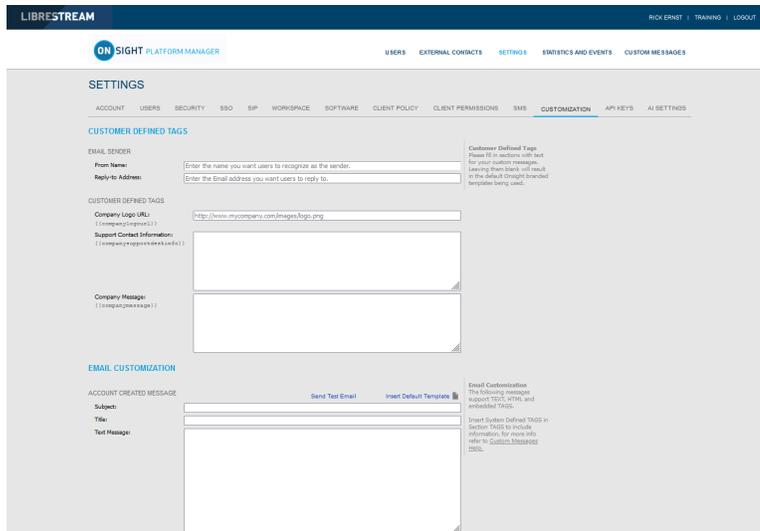


Figura 9-43 Personalização

Clique em **SETTINGS** no menu principal e depois na guia **CUSTOMIZATION**. A página **CUSTOMIZATION** inclui as seguintes seções: **CUSTOMER DEFINED TAGS**, **EMAIL CUSTOMIZATION** e **SMS CUSTOMIZATION**.

A personalização permite personalizar mensagens de e-mail e SMS que os usuários do OnSight Connect recebem do domínio do OnSight da sua empresa.

São enviadas mensagens relativas aos seguintes 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** são usadas para acessar informações específicas da empresa e do usuário para colocação nas mensagens. Para obter mais informações, consulte **Custom Messages Help** na página **CUSTOMIZATION**.

Para exibir as mensagens padrão, clique em **Insert Default Template** ao lado da caixa de texto da mensagem. Você pode editar o modelo de mensagem padrão ou criar suas próprias mensagens. Pressione **Save** para manter as suas alterações.

## 9.13. Chaves de interface de programação de aplicativos

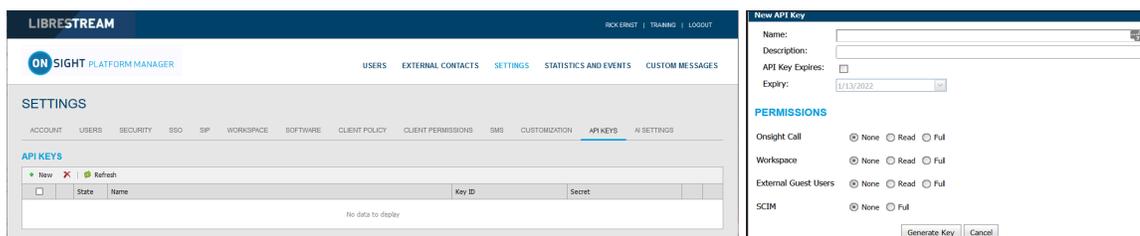


Figura 9-44 Página de chaves de API

Clique em **SETTINGS** no menu principal e depois na guia **APIKEYS**. A página **API KEYS** permite que você gerencie o acesso às APIs REST de chamada do Onsight e do Workspace.

Clique no ícone  **New** para gerar uma nova chave de autorização de API. Forneça os seguintes detalhes para cada chave:

1. **Name**.
2. **Description**.
3. **API Key Expires** seguida de **Expiry Date**.
4. Defina as permissões para **Onsight Call**, **Workspace**, **External Guest Users** etc. como:
  - **None** — sem acesso.
  - **Read** — somente leitura.
  - **Full** — Acesso de leitura/gravação.
5. Clique em **Generate Key**.

### 9.13.1. Chave gerada pela API

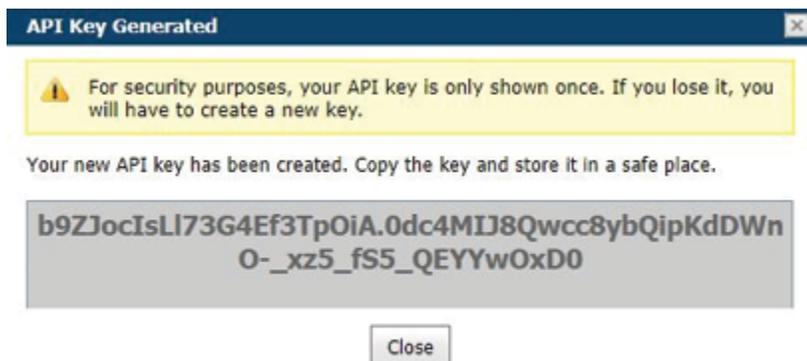


Figura 9-45 Chave gerada pela API

Depois que a chave é gerada, a janela API Key Generated (Chave gerada pela API) é exibida. Ela vai informar:

Para fins de segurança, sua chave de API é mostrada apenas uma vez. Se ela for perdida, você terá de criar uma nova chave.

Quando sua nova chave de API for criada, copie a chave e armazene-a em um lugar seguro. Você precisará desta chave para acessar os pontos de extremidade da API REST.

Após a criação, a chave não pode ser visualizada novamente, mas você pode editar as propriedades associadas, como **Name**, **Description**, Expiração ou Permissões. Clique no botão **Edit** para alterar as propriedades da chave de API.

Você pode bloquear a tecla para que não acesse pontos de extremidade da API REST pressionando o botão **Lock**. Desbloqueie a chave para restaurar o acesso aos serviços.

Consulte os guias de API do Onsight para obter detalhes sobre o uso da chave de API REST.

## 9.14. Configurações de inteligência artificial

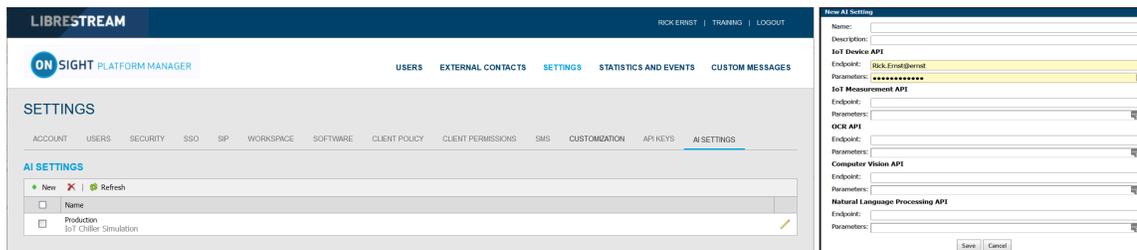


Figura 9-46 Novas configurações de IA

Use a página Configurações de inteligência artificial (IA) para configurar seus pontos de extremidade e parâmetros da API de inteligência artificial. As configurações de IA podem ser adicionadas à **Client Policy** para permitir que os clientes tenham acesso a serviços de IA, inclusive **Computer Vision (VC)**, **Optical Character Recognition (OCR)**, **Internet of Things (IoT)** e **Natural Language Processing (PLN)**.

Pressione o ícone  **New** para criar uma nova configuração de IA. Insira as seguintes informações:

1. **Name.**
2. **Description.**
3. **IoT Device API:**
  - a. **Endpoint** — digite a URL.
  - b. **Parameters** — digite as credenciais.
4. **IoT Measurement API:**
  - a. **Endpoint** — digite a URL.
  - b. **Parameters** — digite as credenciais.
5. **OCR API**
  - a. **Endpoint** — digite a URL.
  - b. **Parameters** — digite as credenciais.
6. **Computer Vision API**
  - a. **Endpoint** — digite a URL.
  - b. **Parameters** — digite as credenciais.
7. **Natural Language Processing API**
  - a. **Endpoint** — digite a URL.
  - b. **Parameters** — digite as credenciais.
8. **Transcription API**
  - a. **Endpoint** — digite a URL.
  - b. **Parameters** — digite as credenciais.

Depois que os perfis de configuração de IA são criados, eles ficam disponíveis para seleção na política do cliente sob a lista suspensa **Artificial Intelligence > AI Setting Profiles**. Você deve adicionar **AI settings** à política antes que elas possam ser configuradas. Clique em  **Choose Settings** na página **Client Policy**.

Um usuário deve pertencer a um grupo que inclui um **AI Setting Profile** para acessar serviços de IA.

Você pode optar por combinar ou separar cada serviço de IA em um perfil de configuração de IA personalizado. Por exemplo, os serviços de IoT podem ser configurados por um perfil de configuração de IA que apenas descreve o ponto de extremidade e os parâmetros da API do dispositivo de IoT. No entanto, apenas um perfil de configuração de IA pode ser aplicado a uma política do cliente, portanto, todos os serviços de IA devem ser combinados em um **único perfil de configuração de IA** se você quiser que os membros de um grupo acessem mais de um serviço de IA.

# 10. ESTATÍSTICAS E EVENTOS

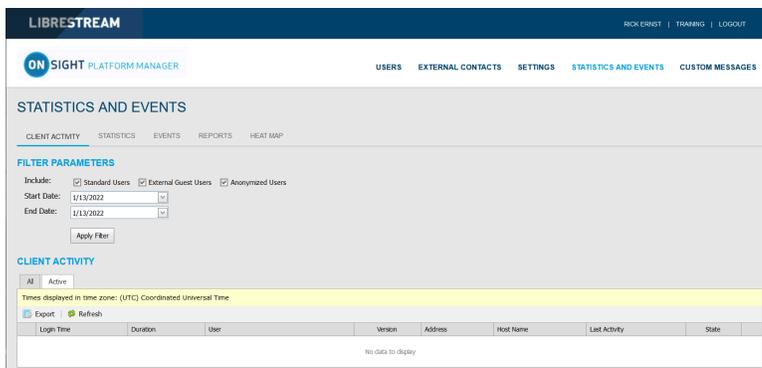


Figura 10-1 Estatísticas e eventos

Clique em **STATISTICS AND EVENTS** no menu principal para definir configurações que permitem gerar relatórios de atividades e eventos do cliente para sua organização. **STATISTICS AND EVENTS** permite que você acesse as seguintes seções: **CLIENT ACTIVITY**, **STATISTICS**, **EVENTS**, **REPORTS** e **HEAT MAP**. Atividades e eventos do cliente podem ser visualizados na página **STATISTICS AND EVENTS**.

## PARÂMETROS DE FILTRO

Em termos gerais, modifique os **FILTER PARAMETERS** usando as caixas de seleção para filtrar suas informações seguidas por menus suspensos para definir seus parâmetros específicos e clique em **Apply Filter** para gerar um relatório.

## 10.1. Atividade do cliente

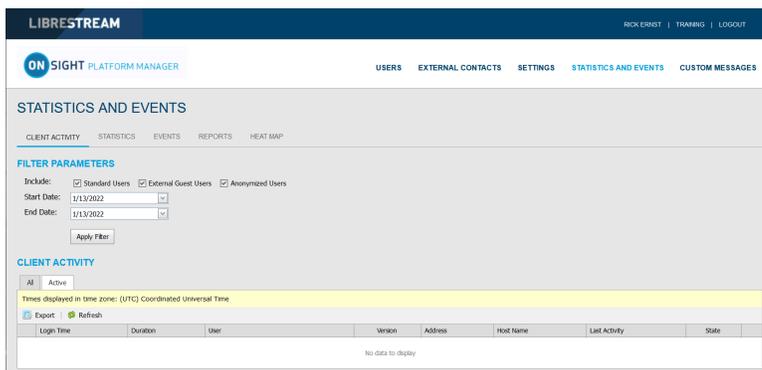


Figura 10-2 Atividade do cliente

Clique em **STATISTICS AND EVENTS** no menu principal para acessar sua página **CLIENT ACTIVITY**. A página **CLIENT ACTIVITY** contém **FILTER PARAMETERS** e uma seção **CLIENT ACTIVITY**.

### Atividade do cliente

A seção de atividades do cliente exibe todos os resultados em uma tabela e rastreia a atividade do usuário para o Serviço Onsign Connect. O administrador pode exibir esses resultados usando as guias. Selecione entre:

- **All** — exibe toda a atividade.
- **Active** — exibe quem está ativamente conectado.

### 10.1.1. Geração de um relatório de atividades do cliente

Faça login no OPM, selecione **STATISTICS AND EVENTS** no menu principal e selecione a guia **CLIENT ACTIVITY**.

Para gerar um relatório de atividades do cliente, você deverá modificar seus **FILTER PARAMETERS**.

1. Determine quais usuários serão incluídos habilitando uma ou mais caixas de seleção para:

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

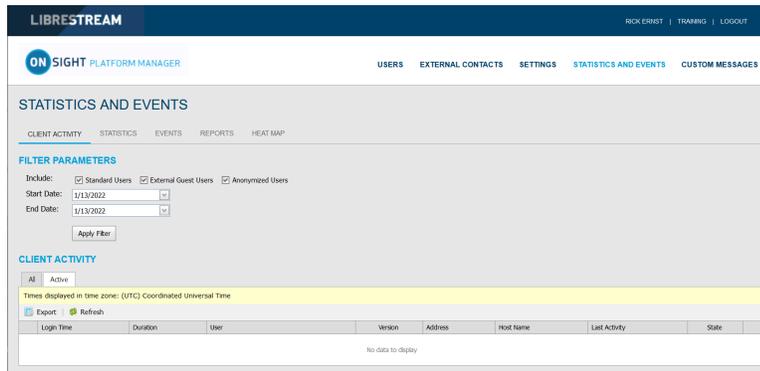


Figura 10-3 Filtragem de usuários

2. Defina seus parâmetros de **data**. Clique no menu suspenso e selecione uma:

- a. **Start Date** usando o menu pop-up **Calendar**.
- b. **End Date** usando o menu pop-up **Calendar**.

3. Clique em **Apply Filter** para exibir resultados na guia **CLIENT ACTIVITY ALL**.

4. **CLIENT ACTIVITY** exibe:

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

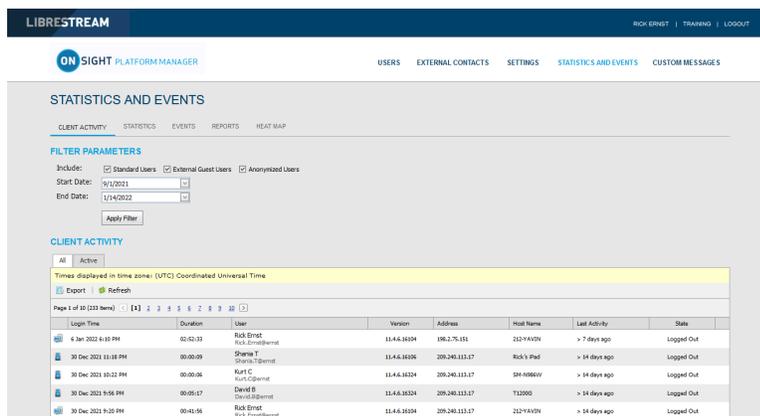


Figura 10-4 Resultados da atividade do cliente

5. Clicar em **Refresh** atualiza a lista.

6. Clicar em **Export** permite salvar um arquivo CSV (valores separados por vírgulas) do relatório. Isso conclui o procedimento.

## 10.2. Estatísticas

Figura 10-5 Relatório de estatísticas

Clique em **STATISTICS AND EVENTS** no menu principal e selecione a guia **STATISTICS**. A página **STATISTICS** contém **FILTER PARAMETERS** e a seção **CALLS**.

A página **STATISTICS** permite que você gere relatórios de estatísticas relacionadas a chamadas. Estatísticas relacionadas às chamadas estão disponíveis para usuários com licença **Connect Enterprise**.

 **Nota:** clique no ícone **Call Details** (lupa) para exibir mais informações.

### 10.2.1. Geração de um relatório estatístico

Faça login no OPM, selecione **STATISTICS AND EVENTS** no menu principal e selecione a guia **STATISTICS**.

Para gerar um relatório estatístico, você deverá modificar seus **FILTER PARAMETERS**.

1. Determine quais usuários serão incluídos habilitando uma ou mais caixas de seleção para:
  - **Standard Users**
  - **External Guest Users**
  - **Anonymized Users**

Figura 10-6 Filtragem de usuários

2. Defina seus parâmetros de data. Clique no menu suspenso e selecione uma:
  - a. **Start Date** usando o menu suspenso Calendar.
  - b. **End Date** usando o menu pop-up Calendar.

3. Clique em **Apply Filter** para exibir resultados dentro da seção **CALLS**.

4. **CALLS** exibe os seguintes campos:

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

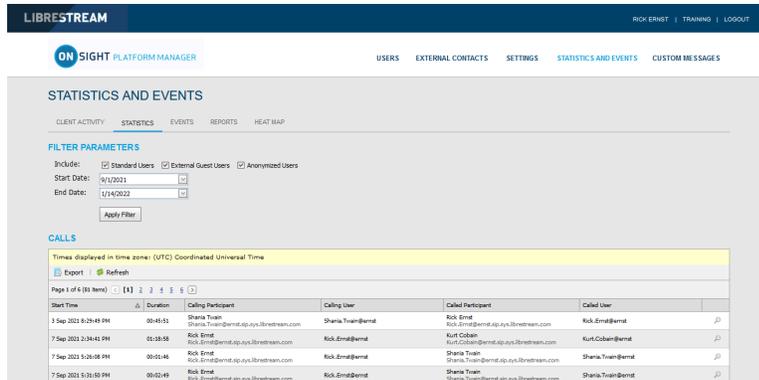


Figura 10-7 Resultados do relatório estatístico

5. Clicar em **Refresh** atualiza a lista.

6. Clicar em **Export** permite salvar um arquivo CSV (valores separados por vírgulas) do relatório.

### Exibição dos detalhes da chamada

7. Para ver os detalhes de um usuário, clique no ícone **Call Details** (lupa).

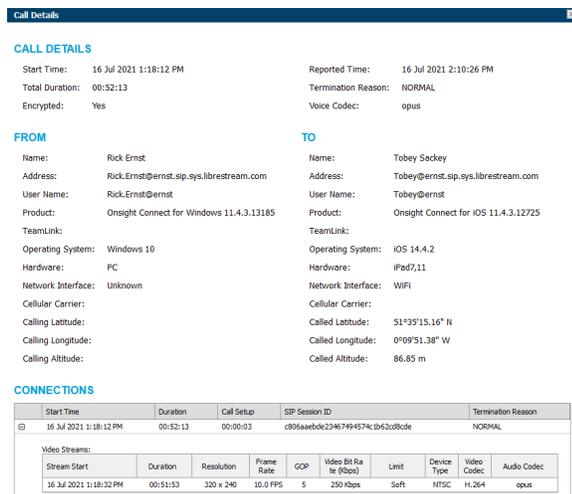


Figura 10-8 Detalhes da chamada estatística

8. A página **Call Details** exibe:

- 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. GOP

g. Video Bit Rate

h. Limit

i. Device Type

j. Video Codec

k. Audio Codec

12. Saia da página quando terminar a visualização.  
Isso conclui o procedimento.

## 10.3. Eventos

The screenshot shows the 'STATISTICS AND EVENTS' page in the SIGHT Platform Manager. The 'EVENTS' tab is active. Under 'FILTER PARAMETERS', the 'Severity' options are 'Information', 'Warning', 'Error', and 'Fatal', all of which are checked. The 'Include' options are 'Standard Users', 'External Guest Users', and 'API Users', all of which are checked. The 'Start Date' is set to 9/6/2021 and the 'End Date' is set to 1/13/2022. An 'Apply Filter' button is present. Below the filter section is the 'EVENT LOG' section, which displays a table of events. The table has columns for 'Time', 'User', 'API Key', 'Description', and 'Details'. The events listed are all 'User logged in successfully' for the user 'Rick.Ernst@ernst.com' from various IP addresses.

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

Figura 10-9 Eventos

Clique em **STATISTICS AND EVENTS** no menu principal e selecione a guia **EVENTS**. Esta página contém **FILTER PARAMETERS** e uma seção **EVENT LOG**.

A página **EVENTS** rastreia a atividade do administrador e do usuário no OPM, bem como mensagens de evento baseadas no servidor. Defina **FILTER PARAMETERS** e clique em **Apply Filter** para exibir os resultados na seção **EVENT LOG**.

### 10.3.1. Geração de um relatório de eventos

Faça login no OPM, selecione **STATISTICS AND EVENTS** no menu principal e selecione a guia **EVENTS**.

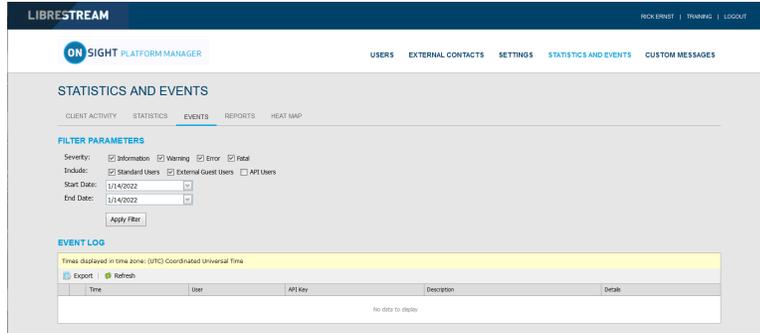
Para gerar um relatório de **eventos**, você deverá modificar os seus **FILTER PARAMETERS**.

1. Defina as opções de **Severity** ativando as caixas de seleção para:

- **Information**
- **Warning**

- **Error**

- **Fatal**



**Figura 10-10 Filtragem por severidade e usuários**

2. Determine quais usuários serão incluídos habilitando uma ou mais caixas de seleção para:

- **Standard Users**

- **External Guest Users**

- **API Users**

3. Defina os seus parâmetros de **data**. Clique no menu suspenso e selecione uma:

a. **Start Date** usando o menu pop-up Calendário.

b. **End Date** usando o menu pop-up Calendário.

4. Clique em **Apply Filter** para exibir os resultados na seção **EVENT LOG**.

5. O registro de eventos exibe:

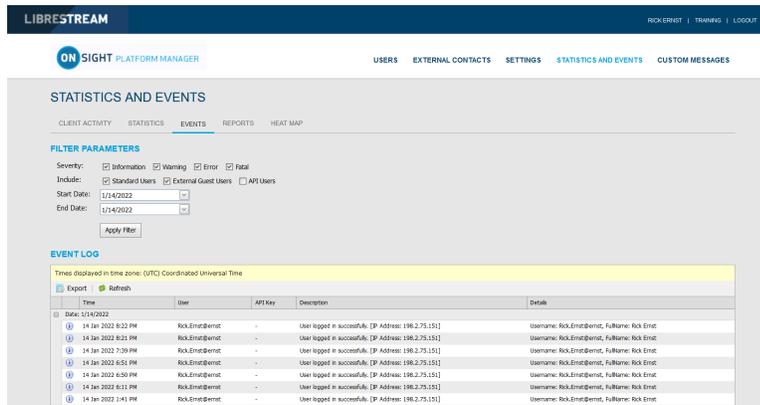
a. **Time**

b. **User**

c. **API Key**

d. **Description**

e. **Details**



**Figura 10-11 Resultados do relatório estatístico**

6. Clicar em **Refresh** atualiza a lista.

7. Clicar em **Export** permite salvar um arquivo CSV (valores separados por vírgulas) do relatório. Isso conclui o procedimento.

## 10.4. Relatórios

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

Figura 10-12 Relatórios

Clique em **STATISTICS AND EVENTS** no menu principal e selecione a guia **REPORTS**. A página **REPORTS** contém a seção **FILTER PARAMETERS**. Quando um relatório é gerado, a seção **RESULTS** é exibida com os dados do relatório.

Os relatórios permitem que você gere estatísticas de uso, incluindo quem fez logon no software, quantas chamadas uma pessoa fez e recebeu, bem como a duração total e média das chamadas, para ajudar a determinar o nível de adoção da tecnologia. Alguns dos benefícios da revisão regular de maior e menor utilização incluem:

- Identificação dos principais usuários como líderes potenciais.
- Identificação de candidatos para mentoria/coaching.
- Destacar o apoio e o interesse da gestão pela nova tecnologia.

Relatórios de resumo de uso geral e licença listam o número de licenças usadas ou de chamadas feitas durante um período.

 **Nota:** se a anonimização de dados estiver ativada para o seu domínio, todos os dados que excedem o período de retenção de dados (DRP) ficarão anônimos. Registros de chamadas anônimos podem ser:

- Usados para fornecer tendências históricas.
- Incluídos nas contagens de relatórios de chamadas.
- Atribuídos aos grupos de usuário, país, campos personalizados e outros filtros.
- Incluídos em um arquivo CSV exportado.
- Visíveis na tabela Atividade do cliente.
- Filtrados usando campos personalizados.

 **Nota:** o histórico de chamadas é armazenado localmente em clientes e não é anônimo. Ele pode ser removido quando o aplicativo é desinstalado. Dados de usuários excluídos anteriormente podem ficar anônimos mediante solicitação.

### 10.4.1. Geração de um relatório

Faça logon no OPM, selecione **STATISTICS AND EVENTS** no menu principal e selecione a guia **REPORTS**.

Para gerar um relatório, você deverá modificar os seus **FILTER PARAMETERS**.

1. Selecione o nome do relatório a ser executado no menu suspenso **Report Name**. Selecione entre:
  - a. **Top Usage** (Chamadas)
  - b. **Least Usage** (Chamadas)
  - c. **Top Usage** (Logons)
  - d. **Least Usage** (Logons)
  - e. **Top Usage** (Largura de banda)
  - f. **Least Usage** (Largura de banda)
  - g. **License Usage Summary** — fornece uma lista do número de licenças utilizadas durante o período.
  - h. **Guest Invite Summary** — fornece uma lista do número de convites enviados para o período incluindo remetente, convidado, status do convite etc.
  - i. **Overall Usage Summary** — fornece uma lista do número de chamadas e a duração total para o período.

**Figura 10-13 Parâmetros do relatório**

2. Defina **Start Date** e **End Date** para o relatório clicando nos menus suspensos para acessar um pop-up **Calendar**.
3. Defina o tipo de usuário no menu suspenso **User Account Type**. Selecione entre:
  - **Standard Users**
  - **External Guest Users**
  - **All Users**
4. (Opcional) Clique para habilitar as caixas de seleção para os **Groups** a serem incluídos no relatório. O padrão é **All Users**.
5. (Opcional) Clique para ativar as caixas de seleção para o **Country** a ser filtrado. O padrão é **All Countries**.
6. (Opcional) Selecione **Custom Fields** para filtragem (opcional — por padrão, inclui todos os campos personalizados).
7. Defina a **Call Duration** utilizando o menu suspenso. Selecione entre:
  - a. **any**
  - b. **greater or equal**
  - c. **less or equal**
  - d. **between**
8. Defina o **Number of Results** usando o menu suspenso para inclusão no relatório. Selecione entre **10, 25, 50, 100** etc.
9. Habilite a opção da caixa de seleção para **Include anonymous records** (incluir registros anônimos), conforme necessário.
10. (Opcional) Clique em **Run Report** para visualizar os resultados.

**REPORT PARAMETERS**

Report Name: Top Usage (Calls) [v]  
 Start Date: 9/1/2021 [v]  
 End Date: 1/14/2022 [v]  
 User Account Type: Standard Users [v]  
 Groups: Domain:EU/NA;Volvo;China;Mobile Users [v]  
 Country: Afghanistan;Albania;Algeria;American Sam [v]  
 Custom Fields: Department;Region [v]  
 Department: Training;Support [v]  
 Region: Optional (default to All Region) [v]  
 Call Duration: any [v]  
 Number of Results: Unlimited [v]  
 Include anonymous records  
 Run Report

**RESULTS**

TOP USAGE (CALLS)

Times displayed in time zone: (UTC) Coordinated Universal Time

Export

Name	# of Calls	Duration (h:mm)
Bob_Phone Bob_Phone@emist	0	00:00:00

Figura 10-14 Resultados do relatório

- (Opcional) Clique em **Export** para salvar, baixar e ver os resultados como um arquivo CSV (valores separados por vírgulas). Isso conclui o procedimento.

## 10.5. Mapas de calor

**STATISTICS AND EVENTS**

CLIENT ACTIVITY | STATISTICS | EVENTS | REPORTS | **HEAT MAP**

**FILTER PARAMETERS**

Heat Map For: Login [v]  
 Start Date: 1/14/2022 [v]  
 End Date: 1/14/2022 [v]  
 Apply Filter

**HEAT MAP**

Country | Counts

No data

Print | Export

Figura 10-15 Página Mapa de calor

Clique em **STATISTICS AND EVENTS** no menu principal para acessar a página **HEAT MAP**. A página **HEAT MAP** contém **FILTER PARAMETERS** e uma seção **HEAT MAP**.

Os mapas de calor apresentam quantidades de chamadas ou logons que são filtradas por localização de endereço IP e quantidade. As chamadas podem ser filtradas para exibir o **Caller**, **Callee** ou **Both** no mapa.

**Nota:** o mapa de calor representa um número de conexões do cliente com base no endereço IP aparente. Pode ocorrer alguma variação devido ao roteamento para torres de celular ou entrada de firewall na Internet pública.

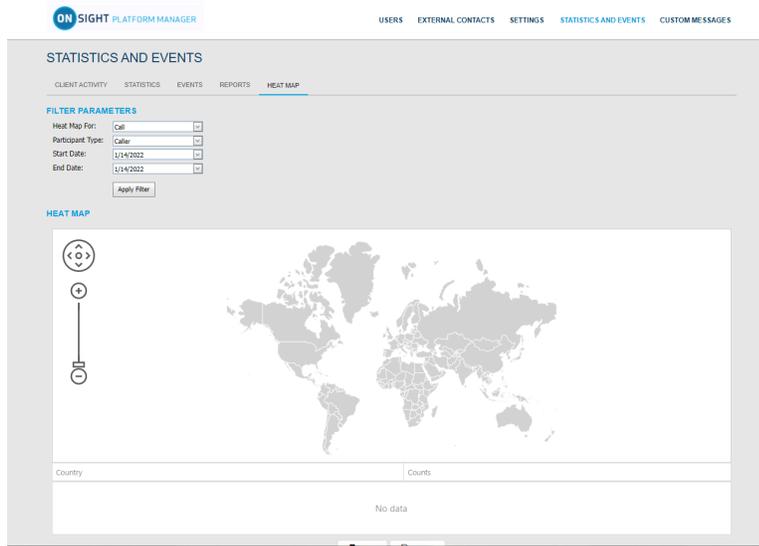
### 10.5.1. Geração de um relatório de mapa de calor

Faça logon no OPM e selecione **STATISTICS AND EVENTS** no menu principal; selecione a guia **HEAT MAP**.

Para gerar um relatório de mapa de calor, é necessário modificar seus **FILTER PARAMETERS**.

1. Utilize o menu suspenso **Heat Map For** para escolher a fonte de informação para a geração do relatório. Selecione entre:

- **Call**
- **Login**



**Figura 10-16** Parâmetros do filtro do mapa de calor

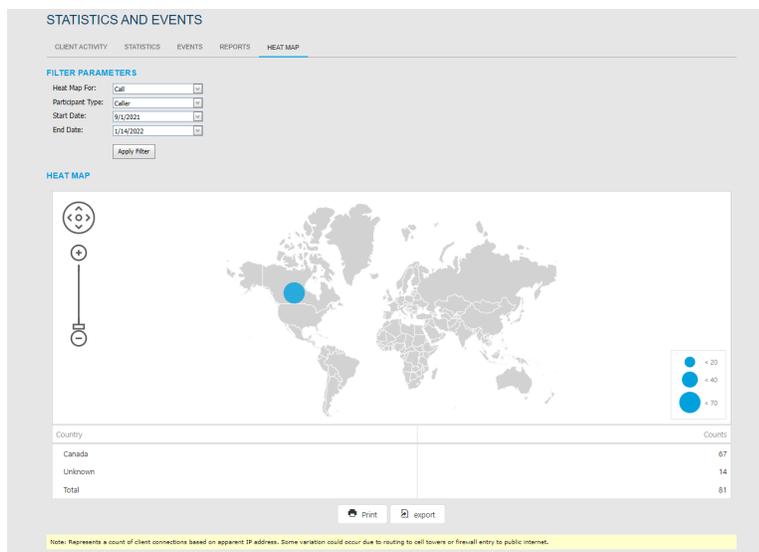
2. Apenas a opção **Call** — permite também selecionar o **Participant Type** como:

- **Caller**
- **Callee**
- **Both**

3. Defina **Start Date** e **End Date** do relatório clicando nos menus suspensos para acessar um pop-up de calendário.

4. Clique em **Apply Filter** para executar o relatório.

O mapa de calor será exibido indicando a localização e a quantidade de chamadas/logons.



**Figura 10-17** Resultados do relatório de mapa de calor

5. (Opcional) Clique em **Print** para imprimir uma cópia do mapa em PDF.

6. (Opcional) Clique em **Export** para salvar, baixar e ver os resultados como um arquivo CSV (valores separados por vírgulas). Isso conclui o procedimento.



# 11. SUPORTE A IDIOMAS

O Onsight Connect aceita os seguintes idiomas para Windows, smartphones e tablets:

- Inglês
- Francês
- Chinês (simplificado)
- Japonês
- Alemão
- Italiano
- Português (Portugal e Brasil)
- Espanhol
- Sueco
- Russo
- Coreano

O OPM exibirá as páginas solicitadas pelo Onsight Connect com base no idioma do sistema cliente. Nenhuma configuração é necessária nem seu domínio do Onsight.

O Onsight Platform Manager está atualmente disponível apenas em inglês, mas exibe páginas localizadas no navegador do cliente para o seguinte:

## 1. Convidar um convidado

- Download do **Onsight Connect for Windows**
- **Register for an Account**
- **Forgot Password**
- **Reset Password**
- Logon **SSO**

## 2. Os e-mails originários do OPM são localizados e incluem:

- Conta registrada (HTML, texto)
- Confirmação do usuário convidado (texto)
- Convite do usuário convidado (HTML, texto, SMS)
- Solicitação de redefinição de senha (texto, SMS)
- Senha do usuário alterada (texto, SMS)



## 12. MENSAGENS PERSONALIZADAS



Figura 12-1 Mensagens personalizadas

**Custom Messages** podem ser exibidas no aplicativo OnSight Connect no logon ou antes de iniciar uma gravação. **Custom Messages** devem ser reconhecidas por um usuário antes da conclusão do logon ou de uma gravação ser iniciada. Se a mensagem não for aceita pelo usuário, a ação não será permitida. Os usuários devem pressionar **OK** para continuar ou o usuário será devolvido à janela de logon e a gravação não será iniciada.

 **Dica:** normalmente, as mensagens personalizadas são usadas para exibir os termos de uso para usar o OnSight Connect em sua empresa.

### 12.1. Criação de uma mensagem personalizada (formulário)

Faça logon no OPM e clique em **CUSTOM MESSAGES** no menu principal para gerenciar formulários de mensagens personalizadas.

1. Pressione o ícone  **New** para criar uma nova mensagem personalizada.

Figura 12-2 Novo formulário

2. Informe os seguintes parâmetros:
  - a. **Name** — este campo só é visível dentro do OPM.
  - b. Ative a caixa de seleção **Available for Use** se quiser que o formulário esteja disponível para uso em **Client Policy**.
  - c. **Title** — este campo é apresentado no aplicativo.
  - d. **Message** — esta é a mensagem que os usuários vão ver. Existe um limite de 500 caracteres.
  - e. **Trigger** — selecione o evento que vai desencadear a exibição da mensagem, **Login** ou **Recordings**.
  - f. **Button Styles** — selecione o estilo de botões de resposta que pretende exibir. Atualmente, **OK/Cancel** é a única opção.

g. **Message Options** — define se você pretende que o usuário possa selecionar a opção **Don't show again** (Não mostrar novamente). Se quiser que um usuário seja avisado sempre que fizer o logon ou uma gravação, desative essa opção.

h. Clique em **OK** para salvar a sua mensagem personalizada. Clique em **Cancel** se não quiser salvar as suas alterações.

Isso conclui o procedimento.

## 12.2. Mensagens personalizadas e política do cliente

As mensagens personalizadas devem ser adicionadas a uma **Client Policy** para serem exibidas no Onsite Connect. Você pode exibir uma ou mais mensagens personalizadas no aplicativo, ou seja, tanto as mensagens de **Login** quanto **Recording** podem ser usadas na mesma política do cliente.

### 12.2.1. Modificação da política do cliente para suporte a mensagens personalizadas

Faça logon no OPM.

1. Clique em **USERS** no menu principal e selecione um grupo.
2. Pressione o ícone  **New Group**.
3. Selecione a guia **CLIENT POLICY**.
4. Selecione  **Choose Settings**.
  - a. Selecione **Login** se quiser exibir uma mensagem de logon.
  - b. Selecione **Recording** se quiser exibir uma mensagem de gravação.
5. Clique em **OK** para voltar à seção **Client Policy**.
6. Desça a página até a seção **Custom Messages**.
  - a. Selecione a mensagem de **Login** que quer exibir.
  - b. Selecione a mensagem de **Recording** que quer exibir.

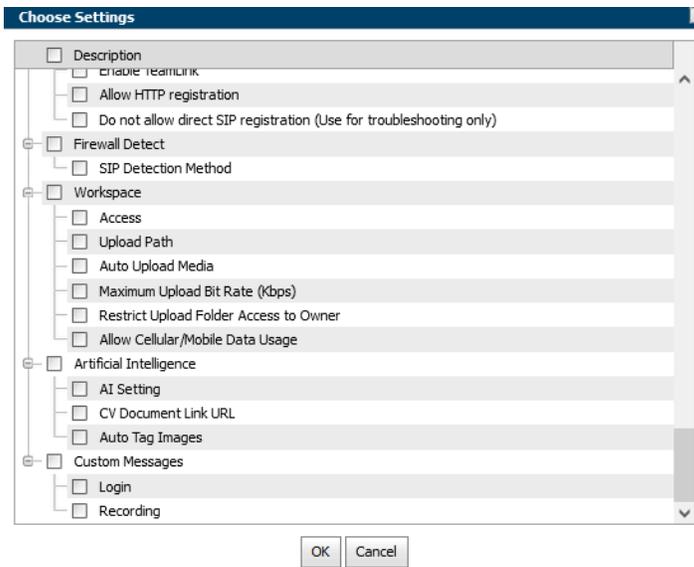


Figura 12-3 Escolher configurações

7. Pressione **Save** para manter as suas alterações. Isso conclui o procedimento.

## 13. CONTRATO DE LICENÇA DE USUÁRIO FINAL

Este software é licenciado sob os termos de um Contrato de licença de usuário final (EULA), cuja versão mais recente pode ser encontrada em:

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



## 14. CONTATO COM O SUPORTE



**Figura 14-1** Código QR de contato com o suporte

Para consultas de suporte:

- **E-mail:** <mailto:support@librestream.com>
- **Web:** <https://librestream.com/contact-us-support/>
- **Telefone:** 1.800.849.5507 ou +1.204.487.0612



# APPENDICES

## Precedência de prioridade e política do cliente

Item de política do cliente	Prioridade (alta a baixa)
<b>General</b> (Geral)	
<b>User Mode</b> (Modo de usuário)	<ol style="list-style-type: none"> <li>1. <b>Field</b> (Campo)</li> <li>2. <b>Expert</b> (Especialista)</li> </ol>
<b>Prompt for Permissions</b> (Solicitação de permissões)	<ol style="list-style-type: none"> <li>1. <b>On Login</b> (No logon)</li> <li>2. <b>As Required</b> (Como exigido)</li> </ol>
<b>Enable GPS Location in Video and Images</b> (Habilitar localização GPS em vídeo e imagens)	<ol style="list-style-type: none"> <li>1. <b>FALSE</b> (FALSO)</li> <li>2. <b>TRUE</b> (VERDADEIRO)</li> </ol>
<b>Show GPS Overlay</b> (Mostrar sobreposição de GPS)	<ol style="list-style-type: none"> <li>1. <b>FALSE</b> (FALSO)</li> <li>2. <b>TRUE</b> (VERDADEIRO)</li> </ol>
<b>Show Date/Time Overlay</b> (Mostrar sobreposição de data/hora)	<ol style="list-style-type: none"> <li>1. <b>FALSE</b> (FALSO)</li> <li>2. <b>TRUE</b> (VERDADEIRO)</li> </ol>
<b>Copy Captured Image to Gallery / Camera Roll</b> (Copiar imagem capturada para a galeria/o rolo da câmera)	<ol style="list-style-type: none"> <li>1. <b>FALSE</b> (FALSO)</li> <li>2. <b>TRUE</b> (VERDADEIRO)</li> </ol>
<b>Text Location of Overlay</b> (Localização do texto da sobreposição)	<ol style="list-style-type: none"> <li>1. <b>Bottom Left</b> (Inferior à esquerda)</li> <li>2. <b>Bottom Right</b> (Inferior à direita)</li> <li>3. <b>Top Left</b> (Superior à esquerda)</li> <li>4. <b>Top Right</b> (Superior à direita)</li> </ol>
<b>Text Size of Overlay</b> (Tamanho do texto da sobreposição)	<ol style="list-style-type: none"> <li>1. <b>Large</b> (Grande)</li> <li>2. <b>Medium</b> (Médio)</li> <li>3. <b>Small</b> (Pequeno)</li> </ol>
<b>Image Capture Resolution</b> (Resolução da captura de imagem)	<ol style="list-style-type: none"> <li>1. <b>Max</b> (Máx.)</li> <li>2. <b>High</b> (Alta)</li> <li>3. <b>Medium</b> (Médio)</li> <li>4. <b>Low</b> (Baixa)</li> </ol>
<b>Media Path</b> (Caminho de mídia)	<b>Undefined</b> — esta configuração aceita o valor para o último grupo da lista.
<b>Login</b> (Logon)	
<b>Prompt to Remember Credentials (Auto Login)</b> (Solicitar para lembrar credenciais [logon automático])	<ol style="list-style-type: none"> <li>1. <b>Disabled</b> (Desabilitado)</li> <li>2. <b>Enabled</b> (Habilitado)</li> </ol>
<b>Run at Windows startup</b> (Executar na inicialização do Windows)	<ol style="list-style-type: none"> <li>1. <b>FALSE</b> (FALSO)</li> <li>2. <b>TRUE</b> (VERDADEIRO)</li> </ol>

Item de política do cliente	Prioridade (alta a baixa)
<b>SIP</b>	
<b>SIP messaging</b> (Mensagens SIP)	<ol style="list-style-type: none"> <li>1. <b>UDP</b></li> <li>2. <b>TCP</b></li> <li>3. <b>&lt;Not defined&gt;</b> (&lt;Não definido&gt;)</li> </ol>
<b>Support SIP UPDATE method</b> (Suporte ao método de ATUALIZAÇÃO DE SIP)	<ol style="list-style-type: none"> <li>1. <b>FALSE</b> (FALSO)</li> <li>2. <b>TRUE</b> (VERDADEIRO)</li> </ol>
<b>Verify SIP TLS Server</b> (Verificar o servidor SIP TLS)	<ol style="list-style-type: none"> <li>1. <b>TRUE</b> (VERDADEIRO)</li> <li>2. <b>FALSE</b> (FALSO)</li> </ol>
<b>Enable WebEx CMR Compatibility</b> (Habilitar a compatibilidade com WebEx CMR)	<ol style="list-style-type: none"> <li>1. <b>TRUE</b> (VERDADEIRO)</li> <li>2. <b>FALSE</b> (FALSO)</li> </ol>
<b>Force Media Relay</b> (Forçar retransmissão de mídia)	<ol style="list-style-type: none"> <li>1. <b>FALSE</b> (FALSO)</li> <li>2. <b>TRUE</b> (VERDADEIRO)</li> </ol>
<b>Media Configurations</b> (Configurações de mídia)	
<b>Custom Media Configurations</b> (Configurações personalizadas de mídia)	<b>Combined list from all groups</b> (Lista combinada de todos os grupos)
<b>Bandwidth Control</b> (Controle de largura de banda)	
<b>Enable Bandwidth Control</b> (Habilitar controle de largura de banda)	<ol style="list-style-type: none"> <li>1. <b>TRUE</b> (VERDADEIRO)</li> <li>2. <b>FALSE</b> (FALSO)</li> </ol>
<b>Maximum Video Bit Rate (Kbps)</b> (Taxa máxima de bits de vídeo (Kbps))	<ol style="list-style-type: none"> <li>1. <b>Lower Value</b> (Valor menor)</li> <li>2. <b>Higher Value</b> (Valor maior)</li> </ol>
<b>Enable BAS</b> (Habilitar BAS)	<ol style="list-style-type: none"> <li>1. <b>On</b> (Ativado)</li> <li>2. <b>Cellular Networks</b> (Redes celulares)</li> <li>3. <b>Off</b> (Desativado)</li> </ol>
<b>Media Configuration on Connection</b> (Configuração de mídia na conexão)	<b>Undefined</b> — esta configuração aceita o valor para o último grupo da lista.
<b>Pause Video While Transferring Image</b> (Pausar vídeo ao transferir imagens)	<ol style="list-style-type: none"> <li>1. <b>FALSE</b> (FALSO)</li> <li>2. <b>TRUE</b> (VERDADEIRO)</li> </ol>
<b>Preferred Voice Codec</b> (Codec de voz preferencial)	<ol style="list-style-type: none"> <li>1. <b>Low Bandwidth (GSM)</b> (Baixa largura de banda [GSM])</li> <li>2. <b>Default (G.711)</b> (Padrão [G.711])</li> </ol>
<b>Preferred Subject Audio Codec</b> (Codec de áudio de sujeito preferencial)	<ol style="list-style-type: none"> <li>1. <b>Disabled</b> (Desabilitado)</li> <li>2. <b>Low Bandwidth (GSM)</b> (Baixa largura de banda [GSM])</li> <li>3. <b>Default (G.711)</b> (Padrão [G.711])</li> </ol>
<b>Audio Efficiency</b> (Eficiência de áudio)	<ol style="list-style-type: none"> <li>1. <b>Lower bandwidth</b> (Largura de banda mais baixa)</li> <li>2. <b>Mid</b> (Média)</li> <li>3. <b>Lower latency</b> (Menor latência)</li> </ol>
<b>Calls</b> (Chamadas)	
<b>Allow Cellular / Mobile Data Usage</b> (Permitir o uso de dados de celulares/dispositivos móveis)	<ol style="list-style-type: none"> <li>1. <b>FALSE</b> (FALSO)</li> <li>2. <b>TRUE</b> (VERDADEIRO)</li> </ol>

Item de política do cliente	Prioridade (alta a baixa)
<b>Prompt to Enable Cellular / Mobile Data Usage</b> (Solicitação para ativar o uso de dados de celulares/dispositivos móveis)	<ol style="list-style-type: none"> <li>1. <b>On Every Login</b> (Em cada logon)</li> <li>2. <b>On First Login</b> (No primeiro logon)</li> <li>3. <b>Never</b> (Nunca)</li> </ol>
<b>Start remote / non-Onsight video on connection</b> (Iniciar vídeo remoto/não Onsight na conexão)	<ol style="list-style-type: none"> <li>1. <b>FALSE</b> (FALSO)</li> <li>2. <b>TRUE</b> (VERDADEIRO)</li> </ol>
<b>Fill / Fit video in viewfinder when streaming</b> (Preencher/ajustar vídeo no visor ao transmitir)	<ol style="list-style-type: none"> <li>1. <b>Fill</b> (Preencher)</li> <li>2. <b>Fit</b> (Ajustar)</li> <li>3. <b>Actual Size</b> (Tamanho real)</li> </ol>
<b>Maximum Number of Connections</b> (Número máximo de conexões)	<ol style="list-style-type: none"> <li>1. <b>Lower Value</b> (Valor menor)</li> <li>2. <b>Higher Value</b> (Valor maior)</li> </ol>
<b>Enable auto answer</b> (Habilitar a resposta automática)	<ol style="list-style-type: none"> <li>1. <b>FALSE</b> (FALSO)</li> <li>2. <b>TRUE</b> (VERDADEIRO)</li> </ol>
<b>Auto answer delay (seconds)</b> (Atraso de resposta automática [segundos])	<ol style="list-style-type: none"> <li>1. <b>Lower Value</b> (Valor menor)</li> <li>2. <b>Higher Value</b> (Valor maior)</li> </ol>
<b>Push Notifications</b> (Notificações por push)	<ol style="list-style-type: none"> <li>1. <b>TRUE</b> (VERDADEIRO)</li> <li>2. <b>FALSE</b> (FALSO)</li> </ol>
<b>Prompt to ignore battery optimizations</b> (Solicitação para ignorar otimizações de bateria)	<ol style="list-style-type: none"> <li>1. <b>Only when user disables Push Notifications</b> (Somente quando o usuário desativar as notificações por push)</li> <li>2. <b>Whenever Push Notifications are disabled</b> (Sempre que as notificações por push são desativadas)</li> </ol>
<b>Encryption Mode</b> (Modo de criptografia)	<ol style="list-style-type: none"> <li>1. <b>On</b> (Ativado)</li> <li>2. <b>Auto</b> (Automático)</li> <li>3. <b>Off</b> (Desativado)</li> </ol>
<b>Prompt to Share Images After Capture</b> (Solicitar compartilhar imagens após a captura)	<ol style="list-style-type: none"> <li>1. <b>FALSE</b> (FALSO)</li> <li>2. <b>TRUE</b> (VERDADEIRO)</li> </ol>
<b>Disable recordings and saving snapshots for ALL participants (Privacy Mode)</b> (Desativar gravações e salvamento de instantâneos para TODOS os participantes [Modo de privacidade])	<ol style="list-style-type: none"> <li>1. <b>TRUE</b> (VERDADEIRO)</li> <li>2. <b>FALSE</b> (FALSO)</li> </ol>
<b>Local Privacy Mode</b> (Modo de privacidade local)	<ol style="list-style-type: none"> <li>1. <b>Disable recordings and saving snapshots</b> (Desativar gravações e salvamento de instantâneos)</li> <li>2. <b>Disable recordings</b> (Desativar gravações)</li> <li>3. <b>Disable saving snapshots</b> (Desativar o salvamento de instantâneos)</li> <li>4. <b>Allow recordings and saving snapshots</b> (Permitir gravações e salvamento de instantâneos)</li> </ol>

Item de política do cliente	Prioridade (alta a baixa)
<b>Networking</b> (Sistema de rede)	
<b>Diffserv DSCP (Voice)</b> (Diffserv DSCP [Voz])	<ol style="list-style-type: none"> <li>1. <b>Voice</b> (Voz)</li> <li>2. <b>Audio / Video / Guaranteed</b> (Áudio/Vídeo/Garantido)</li> <li>3. <b>Controlled Load</b> (Carga controlada)</li> <li>4. <b>Best Effort</b> (Melhor esforço)</li> </ol>
<b>Diffserv DSCP (Video)</b> (Diffserv DSCP [Vídeo])	<ol style="list-style-type: none"> <li>1. <b>Voice</b> (Voz)</li> <li>2. <b>Audio / Video / Guaranteed</b> (Áudio/Vídeo/Garantido)</li> <li>3. <b>Controlled Load</b> (Carga controlada)</li> <li>4. <b>Best Effort</b> (Melhor esforço)</li> </ol>
<b>Diffserv DSCP (Subject Audio)</b> (Diffserv DSCP [Áudio do sujeito])	<ol style="list-style-type: none"> <li>1. <b>Voice</b> (Voz)</li> <li>2. <b>Audio / Video / Guaranteed</b> (Áudio/Vídeo/Garantido)</li> <li>3. <b>Controlled Load</b> (Carga controlada)</li> <li>4. <b>Best Effort</b> (Melhor esforço)</li> </ol>
<b>Diffserv DSCP (Data Stream)</b> (Diffserv DSCP [Fluxo de dados])	<ol style="list-style-type: none"> <li>1. <b>Voice Audio</b> (Áudio de voz)</li> <li>2. <b>Video</b> (Vídeo)</li> <li>3. <b>Guaranteed Controlled Load Best Effort</b> (Melhor esforço de carga controlada garantido)</li> </ol>
<b>TeamLink</b>	
<b>Enable TeamLink</b> (Habilitar o TeamLink)	<ol style="list-style-type: none"> <li>1. <b>TRUE</b> (VERDADEIRO)</li> <li>2. <b>FALSE</b> (FALSO)</li> </ol>
<b>Allow HTTP registration</b> (Permitir registro HTTP)	<ol style="list-style-type: none"> <li>1. <b>TRUE</b> (VERDADEIRO)</li> <li>2. <b>FALSE</b> (FALSO)</li> </ol>
<b>Do not allow direct SIP registration (User for troubleshooting only)</b> (Não permitir o registro direto de SIP [usuário apenas para solução de problemas])	<ol style="list-style-type: none"> <li>1. <b>TRUE</b> (VERDADEIRO)</li> <li>2. <b>FALSE</b> (FALSO)</li> </ol>
<b>Firewall Detect</b> (Detecção de firewall)	
<b>SIP Detection Method</b> (Método de detecção de SIP)	<ol style="list-style-type: none"> <li>1. <b>SIP Server — Full</b> (Servidor SIP — Completo)</li> <li>2. <b>SIP Server — Basic</b> (Servidor SIP — Básico)</li> <li>3. <b>TeamLink</b></li> </ol>
<b>Workspace</b>	
<b>Access</b> (Acesso)	<ol style="list-style-type: none"> <li>1. <b>TRUE</b> (VERDADEIRO)</li> <li>2. <b>FALSE</b> (FALSO)</li> </ol>
<b>Upload Path</b> (Caminho de upload)	<b>Undefined</b> — esta configuração aceita o valor para o último grupo da lista.
<b>Auto Upload Media</b> (Upload automático de mídia)	<ol style="list-style-type: none"> <li>1. <b>TRUE</b> (VERDADEIRO)</li> <li>2. <b>FALSE</b> (FALSO)</li> </ol>
<b>Maximum Upload Bit Rate (Kbps)</b> (Taxa máxima de bits de upload [Kbps])	<ol style="list-style-type: none"> <li>1. <b>Lower Value</b> (Valor menor)</li> <li>2. <b>Higher Value</b> (Valor maior)</li> </ol>

Item de política do cliente	Prioridade (alta a baixa)
<b>Restrict Upload Folder Access to Owner</b> (Restringir o acesso da pasta de upload ao proprietário)	1. <b>TRUE</b> (VERDADEIRO) 2. <b>FALSE</b> (FALSO)
<b>Allow Cellular / Mobile Data Usage</b> (Permitir o uso de dados de celulares/dispositivos móveis)	1. <b>TRUE</b> (VERDADEIRO) 2. <b>FALSE</b> (FALSO)
<b>Custom Messages</b> (Mensagens personalizadas)	
<b>Login</b> (Logon)	<b>Undefined</b> — esta configuração aceita o valor para o último grupo da lista.
<b>Recording</b> (Gravação)	<b>Undefined</b> — esta configuração aceita o valor para o último grupo da lista.

**Informações relacionadas**

[Política do cliente e Permissões \(na página 77\)](#)

[Precedência da política \(na página 80\)](#)

## Práticas recomendadas

### 15.2.1. Conta — Práticas recomendadas

Tabela 15-2 Conta — Práticas recomendadas

Configurações		Descrição	Práticas recomendadas/Dicas
<b>ACCOUNT INFORMATION</b> (INFORMAÇÕES DA CONTA)			
<b>Company Name</b> (Nome da empresa):		Digite o nome de uma empresa	
<b>Customer Domain</b> (Domínio do cliente):		Digite o domínio da empresa	
<b>Account Owner</b> (Proprietário da conta):			
<b>Customer Created</b> (Cliente criado):		Data e hora em que o cliente foi criado	
<b>Customer Expires</b> (Expiração do cliente):		Data em que o uso da conta expirará	
<b>Super Administrator Access</b> (Acesso de superadministrador):		Capacidade de remover o acesso das operações internas da Librestream à conta.   <b>Nota:</b> habilite o acesso quando o suporte Librestream precisar rever as configurações do seu OPM.	
<b>ACTIVATION</b> (ATIVAÇÃO) — exibido apenas para instalações locais.			
<b>Status:</b>		informa o status atual da licença.	
<b>Type</b> (Tipo):		informa o tipo de instalação.	
<b>Expires</b> (Expiração):		exibe a data de validade da licença.	
<b>LICENSES</b> (LICENÇAS)		As licenças ativas no domínio.	
<b>LICENSES &gt; Onsight Users</b>			
<b>Connect Enterprise</b>		Nº de licenças de usuário do domínio	
<b>Workspace Enterprise</b>		Nº de licenças de usuário do Workspace	
<b>Workspace Contributor</b>		Nº de licenças de usuário do Workspace Contributor	
<b>User Expiry</b> (Expiração do usuário)		Suporte para datas de validade da conta do usuário.	
<b>External Guest Users</b> (Usuários convidados externos)		Habilita usuários convidados externos	
<b>Advanced External Guest Expiry</b> (Expiração avançada do convidado externo)			
<b>License Group</b> (Grupo de licenças)		Permite a atribuição de pools de licenças a grupos, cada grupo gerencia seu próprio pool de licenças.	

Tabela 15-2 Conta — Práticas recomendadas

Configurações		Descrição	Práticas recomendadas/Dicas
<b>LICENSES &gt; Client Functionality</b>			
<b>User Mode (Expert/Field)</b> (Modo de usuário [Especialista/Campo])		Permite os modos Especialista e Campo para usuários.	
<b>TeamLink</b>		Quando habilitado, o Onsite Platform Manager determinará se o firewall permite o registro direto de SIP ou se deve usar mensagens SIP de HTTPS para proxy pelos servidores do TeamLink.	
<b>Multiparty Calling</b> (Chamada com vários participantes)		Permite a hospedagem de conferências em PCs Windows.	
<b>Bandwidth Control</b> (Controle de largura de banda)		Permite o controle de largura de banda para a política do cliente.	
<b>Content Privacy</b> (Privacidade de conteúdo)		Permite o controle de privacidade sobre gravações e imagens.	
<b>Onsite 5000HD Updates</b> (Atualizações do Onsite 5000HD)		Permite atualizações de software do 5000HD.	
<b>Onsite Collaboration Hub Updates</b> (Atualizações do Onsite Collaboration Hub)		Permite atualizações de software do Onsite Collaboration Hub.	
<b>Cube Updates</b> (Atualizações do Cube)		Permite atualizações de software do Onsite Cube.	
<b>LICENSES &gt; Hosted Features</b>			
<b>Call Statistics</b> (Estatísticas de chamadas)		Permite a coleta de dados estatísticos de chamadas.	
<b>Advanced Reporting</b> (Relatórios avançados)		Permite relatórios avançados de estatísticas de chamadas.	
<b>Customization</b> (Personalização)		Permite a personalização de mensagens.	
<b>SMS</b>		Permite convites para convidados externos por SMS.	
<b>Client Permissions</b> (Permissões do cliente)		Permite o controle de permissões do cliente.	
<b>Custom Media Configurations</b> (Configurações personalizadas de mídia)		Permite a configuração personalizada de mídia para a política do cliente.	
<b>SSO</b>		Permite suporte a SSO.	
<b>Custom Email (SMTP)</b> (E-mail personalizado [SMTP])		Permite o envio de e-mails a partir do servidor de e-mail dos clientes.	
<b>Custom Messages</b> (Mensagens personalizadas)		Permite o uso de mensagens personalizadas.	
<b>LICENSES &gt; Common Actions</b>			
<b>Change Account Owner</b> (Alterar proprietário da conta)		Permite que você atribua um proprietário da conta com base em uma lista de usuários atuais.	

**Tabela 15-2 Conta — Práticas recomendadas**

Configurações		Descrição	Práticas recomendadas/Dicas
<b>Disable Super Admin Access</b> (Desativar o acesso de superadministrador)		Desativa a capacidade da Librestream de acessar o domínio para fins de suporte. O acesso pode ser concedido pelo seu administrador do OPM, se necessário.	

**Informações relacionadas**

*Conta (na página 52)*

## 15.2.2. Usuários — Práticas Recomendadas

**Tabela 15-3 Usuários — Práticas Recomendadas**

CONTAS DE USUÁRIO	Valor	Padrão	Descrição	Práticas recomendadas/Dicas
<b>Default Time Zone</b> (Fuso horário padrão):	(UTC) Tempo coordenado		Defina o fuso horário padrão para sua região.	Se operar em várias regiões, defina o fuso horário onde o administrador reside.
<b>Default Language</b> (Idioma padrão):	Chinês, inglês, alemão, italiano, japonês, coreano, português, português (Brasil), russo, espanhol e sueco	Inglês		
<b>EXTERNAL GUEST USERS (USUÁRIOS CONVIDADOS EXTERNOS)</b>				
<b>External Guest Settings moved to Client Policy</b> (Configurações de convidados externos movidas para a política do cliente)	Mudou para a política do cliente [LINK]			
<b>GLOBAL DIRECTORY (DIRETÓRIO GLOBAL)</b>				
<b>Global Directory Availability</b> (Disponibilidade do Diretório global)	<input checked="" type="checkbox"/> <b>External Contacts are public by default</b> (Contatos externos são públicos por padrão) (Contatos externos que não pertencem a nenhuma lista de contatos estarão disponíveis para todos no Diretório global)	padrão habilitado	Quando marcados, todos os contatos que não estão em uma lista definida ficarão visíveis no Diretório global; se não forem marcados, apenas os contatos que pertencem a uma lista de contatos ficarão visíveis no Diretório global.	Isso permite que você tenha contatos que não são visíveis para todos, mas podem ser adicionados manualmente pelo administrador às listas de contato dos usuários. Deixe desmarcado se quiser que os contatos que não estão em uma lista não apareçam no Diretório global.

**Tabela 15-3 Usuários — Práticas Recomendadas**

CONTAS DE USUÁRIO	Valor	Padrão	Descrição	Práticas recomendadas/Dicas
<b>CUSTOM FIELDS</b> (CAMPOS PERSONALIZADOS)		Opcional		Os campos personalizados estão incluídos em um relatório de usuário exportado.
<b>Custom Field Name</b> (Nome do campo personalizado)		Departamento, região	Informar um nome	Você pode criar campos personalizados que podem ser usados como filtros de relatório.
<b>Custom Field Value</b> (Valor do campo personalizado)		Nulo	Digite um valor ou uma lista de valores	Crie um valor ou uma lista de valores que podem ser usados em relatórios.

**Informações relacionadas**

[Usuários \(na página 57\)](#)

### 15.2.3. Segurança — Práticas recomendadas

**Tabela 15-4 Segurança — Práticas recomendadas**

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>PASSWORD POLICY (POLÍTICA DE SENHA)</b>			
<b>Minimum Length</b> (Comprimento mínimo):	8	Defina o comprimento mínimo das senhas permitidas.	Siga a política de segurança da sua empresa.
<b>Minimum Capital Letters</b> (Mínimo de letras maiúsculas):	1	Defina o número mínimo de letras maiúsculas exigidas.	
<b>Minimum Non-Alpha Characters</b> (Mínimo de caracteres não alfabéticos):	1	Defina o número mínimo de caracteres não alfabéticos necessários.	
<b>PASSWORD EXPIRATION (EXPIRAÇÃO DA SENHA)</b>			
<b>Password Expiration</b> (Expiração da senha):	<input type="checkbox"/> <b>Enable password expiration</b> (Habilitar expiração de senha)	padrão desabilitado	Siga a política de segurança da sua empresa.
<b>Password expires</b> (Expiração da senha):	60 dias		
<b>Warn Users Before Expiration</b> (Avisar os usuários antes da expiração):	3 dias		

Tabela 15-4 Segurança — Práticas recomendadas

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>LOGIN POLICY (POLÍTICA DE LOGON)</b>			
<b>Maximum Bad Login Attempts</b> (Número máximo de tentativas de logon com falha):	3	padrão 3	Siga a política de segurança da sua empresa.
<b>Account Lockout Duration</b> (Duração do bloqueio da conta):	5 minutos	padrão 5 minutos	
<b>SELF REGISTRATION</b> (AUTORREGISTRO)	padrão desabilitado	As configurações de autorregistro aplicam-se a contas criadas usando a página de autorregistro e contas fornecidas automaticamente por logon único	
<b>Enable Self Registration</b> (Habilitar o autorregistro)	padrão habilitado <input checked="" type="checkbox"/> <b>Enable self registration page</b> (Habilitar a página de autorregistro)	Habilitar a página de autorregistro	O autorregistro pode facilitar a preparação para sessões de treinamento e implantação, não sendo necessário ter uma lista de todos os usuários com antecedência. Normalmente, você apenas envia as instruções de autorregistro.
<b>URL:</b>	<a href="https://onsight.librestream.com/OamDev/AccountServices/Register.aspx?id=librestream.com">https://onsight.librestream.com/OamDev/AccountServices/Register.aspx?id=librestream.com</a>	id=domain, identifica o domínio do cliente no qual o usuário está fazendo o autorregistro. No exemplo, o domínio = librestream.com	Distribua a URL para associados que precisarão se registrar em uma conta Onsignt.
<b>Key</b> (Chave):	xxxxxxxxxxxxxxxxxxxxxxxxxxx: padrão desabilitado	Quando preenchido com um valor, o usuário deve inserir esta chave para se autorregistrar em uma conta Onsignt.	Defina uma chave para garantir que os usuários estejam autorizados a solicitar uma conta. Use Generate Random Key (Gerar chave aleatória) para inserir um valor.
<b>Licenses</b> (Licenças):	<input type="checkbox"/> padrão desabilitado	Se o autorregistro estiver ativado, você poderá especificar o tipo de licença	
<b>Account Activation Method</b> (Método de ativação da conta):	padrão habilitado <input checked="" type="checkbox"/> <b>Administrator must approve accounts registered using the Self Registration key</b> (O administrador deve aprovar contas registradas usando a chave de autorregistro)	Quando habilitado, todas as solicitações de conta devem ser aprovadas por um administrador antes de serem atribuídas.	Recomenda-se habilitar essa opção. No entanto, se um número significativo de usuários estiver se autorregistrando e você não quiser aprovar cada solicitação de conta, deixe essa opção desmarcada. Recomenda-se que você use <b>Self Registration Key</b> e defina <b>Allowed Email domains</b> como uma precaução adicional.
<b>Notification</b> (Notificação):	padrão habilitado <input checked="" type="checkbox"/> <b>Notify Administrators by email when an account is registered</b> (Notificar os administradores por e-mail quando uma conta estiver registrada)	Os administradores do OPM receberão e-mails sempre que um usuário se registrar.	

**Tabela 15-4 Segurança — Práticas recomendadas**

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>Email</b> (E-mail)	padrão habilitado  <input checked="" type="checkbox"/> <b>Require Email Address for Self Registered Accounts</b> (Exigir endereço de e-mail para contas autorregistradas)	Os endereços de e-mail são necessários para notificações do usuário.	<b>Require Email Addresses...</b> (Exigir endereços de e-mail...) deve estar habilitado para que as notificações do usuário sejam recebidas.  É obrigatório se você quiser o recurso <b>Forgot Password</b> disponível para todos os usuários. Normalmente, a única vez que você não exigiria senhas para contas de usuários é quando sua política de segurança não permite que endereços de e-mail sejam armazenados externamente.
<b>Allowed Email Domains</b> (Domínios de e-mail permitidos):	company.com	A lista de domínios de e-mail permitidos a partir dos quais um usuário pode se registrar.	Defina isso para o domínio da sua empresa e qualquer outro parceiro de terceiros para restringir o acesso.

**Informações relacionadas**

[Segurança \(na página 59\)](#)

## 15.2.4. Software — Práticas recomendadas

**Tabela 15-5 Software — Práticas recomendadas**

ATUALIZAÇÕES DE SOFTWARE	Padrão	Descrição	Práticas recomendadas/Dicas
<b>Onsight Connect for Windows</b> (Onsight Connect para Windows)	<b>Latest Published Version</b> (Última versão publicada)	Defina a versão do software que você quer que usuários de PCs Windows e usuários convidados externos instalem.	Você pode escolher "A mais recente..." ou uma versão específica. Se os usuários não tiverem direitos administrativos, a instalação padrão será aplicada.
<b>Onsight 5000HD</b>	<b>Latest Published Version</b> (Última versão publicada)	Defina a versão do software que você quer que os dispositivos Onsight 5000HD instalem.	

**Informações relacionadas**

[Atualizações de software \(na página 76\)](#)

## 15.2.5. Política do cliente — Práticas recomendadas

Tabela 15-6 Política do cliente — Práticas recomendadas

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>External Guest Users</b> (Usuários convidados externos)			
<b>Allow users to invite external guests</b> (Permitir que os usuários convidem convidados externos)	<input checked="" type="checkbox"/> padrão habilitado	Permite que os usuários enviem convites para convidados	
<b>Allow text message guest invitations</b> (Permitir convites por mensagens de texto)	<input checked="" type="checkbox"/> padrão habilitado	Permite que os usuários enviem convites para convidados por texto.	
<b>SMS Max Message to User Length</b> (Comprimento máx. da mensagem SMS para o usuário)	100	Comprimento máximo de caracteres	
<b>Guest users must change temporary password on initial login</b> (Os usuários convidados devem alterar a senha temporária no logon inicial)	<input type="checkbox"/> padrão desabilitado		
<b>Send 'Invitation Sent' confirmation to host (includes copy of invite)</b> (Enviar a confirmação "Invitation Sent" [Convite enviado] para o host [inclui cópia do convite])	<input checked="" type="checkbox"/> padrão habilitado	Permite que você visualize uma cópia do convite	
<b>Disable recording of images and video</b> (Desativar gravação de imagens e vídeo)	<input checked="" type="checkbox"/> padrão habilitado		
<b>Disable global directory access</b> (Desativar o acesso ao Diretório global)	<input checked="" type="checkbox"/> padrão desabilitado	Não habilitado para usuários convidados	
<b>Expiry</b> (Expiração)	1	Dia	
<b>User can choose expiry time when inviting guests</b> (O usuário pode escolher o tempo de expiração ao enviar convites para convidados)	<input type="checkbox"/> padrão desabilitado		

Tabela 15-6 Política do cliente — Práticas recomendadas

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>Deactivate guest user account when removed from contact list</b> (Desativar conta do usuário convidado quando removido da lista de contatos)	<input type="checkbox"/> padrão desabilitado	Quando ativado, e um convidado exclui um contato de convidado da lista de contatos e seleciona desabilitar a conta de convidados desse usuário; se a anonimização dos dados estiver habilitada, os dados pessoais do usuário convidado ficarão anônimos.	A habilitação dessa configuração disponibilizará licenças assim que a conta do convidado não for mais necessária.
<b>Include option for guest to call host immediately</b> (Incluir opção para o convidado chamar o host imediatamente)	<input checked="" type="checkbox"/> padrão habilitado	Quando habilitada, esta configuração permite que o convidado ligue para a pessoa que envia o convite o mais cedo possível. Ela também prevê um link para participar da chamada no formulário. Quando desabilitada, a opção de participar da chamada é substituída pelo logon no Onsite Connect.	Deixe essa configuração habilitada para facilitar a entrada do convidado na chamada.
<b>From Email</b> (Do e-mail)	Padrão	Isso determina se o convite do convidado vem do e-mail do sistema ou do e-mail pessoal da pessoa que envia o convite.	Definir isso para o endereço de e-mail da pessoa que envia o convite pode ajudar a identificar e-mails como provenientes de uma fonte confiável.
<b>Custom Fields</b> (Campos personalizados)	Obrigatório	Quando definido como exigido, a pessoa que envia o convite deve preencher os campos personalizados ao enviar convites para convidados.	Deixe esta configuração como exigido para fornecer mais informações ao gerar relatórios.
<b>Allow Setting User Mode while inviting guest</b> (Permitir definir o modo de usuário ao enviar convite para o convidado)	<input type="checkbox"/> Desabilitado	Quando desabilitado, o usuário não pode especificar um modo de usuário ao enviar um convite a um convidado. Quando habilitado, o usuário pode especificar o modo Especialista (usuário experiente) ou o modo Campo (usuário com experiência limitada).	Habilite essa configuração quando quiser que seus usuários tenham mais flexibilidade em termos de atribuição de modos de usuário aos convidados.
<b>User Mode</b> (Modo de usuário)	<b>Expert</b> ou <b>Field</b>	Defina o modo de usuário padrão para convites para convidados.	Defina o modo de usuário padrão para melhor se encaixar no seu caso de uso.
<b>General</b> (Geral)			
<b>User Mode</b> (Modo de usuário)	<b>Expert</b>	Define o modo em que o usuário opera quando conectado a um dispositivo Onsite.	A maioria dos usuários será Especialista. Você pode considerar o uso do modo de campo para convidados externos ou a equipe de serviço de campo.
<b>Prompt for Permissions</b> (Solicitação de permissões)	As Required (Como exigido)*	Os usuários de smartphones devem conceder permissões para acessar recursos, como uso de dados e imagens.	

\* Todos os valores padrão são marcados com um asterisco.

**Tabela 15-6 Política do cliente — Práticas recomendadas**

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>Allow GPS in Video and Images</b> (Permitir GPS em vídeo e imagens)	<input type="checkbox"/> Desabilitado*	Os metadados de GPS serão incorporados em gravações e imagens	
<b>Screen Sharing</b> (Compartilhamento de tela)	<input checked="" type="checkbox"/> Habilitado*	Permite o compartilhamento de tela entre os participantes.	
<b>Show GPS Overlay</b> (Mostrar sobreposição de GPS)	<input type="checkbox"/> Desabilitado*		
<b>Show Date/Time Overlay</b> (Mostrar sobreposição de data/hora)	<input type="checkbox"/> Desabilitado*		
<b>Copy Captured Image to Gallery/Camera Roll</b> (Copiar imagem capturada para a galeria/o rolo da câmera)	<input type="checkbox"/> Desabilitado*	Se habilitado, cópias de fotos/vídeos serão colocadas na galeria/no rolo da câmera	
<b>Text Location of Overlay</b> (Localização do texto da sobreposição)	Bottom Left (Inferior à esquerda)*		
<b>Text Size of Overlay</b> (Tamanho do texto da sobreposição)	Small (Pequeno)*		
<b>Image Resolution</b> (Resolução de imagem)	Low (Baixa)*	Define a resolução máxima com a qual as imagens serão capturadas localmente. Esta configuração também determinará a mais alta resolução de imagem que pode ser compartilhada em uma chamada para imagens do Onsite. As imagens da galeria/do rolo da câmera serão compartilhadas na resolução nativa em que foram capturadas. As resoluções são definidas com base na altura da imagem em pixels: baixa (768), média (1080), alta (1440) e máxima (depende da resolução máxima da câmera do dispositivo).	Quando uma imagem for compartilhada durante uma chamada, ela será compartilhada inicialmente usando a baixa resolução padrão de 1024 x 768. Se a imagem for capturada em uma resolução mais alta localmente, a imagem de maior resolução será disponibilizada durante uma sessão de compartilhamento de imagens, permitindo que um usuário solicite a imagem de resolução mais alta pressionando o botão High-res no visor.   <b>Nota:</b> imagens da galeria/do rolo da câmera são compartilhadas em sua resolução nativa quando o botão High-res é pressionado.
<b>Copy captured images to Gallery/Camera Roll</b> (Copiar imagens capturadas para a galeria/o rolo da câmera)	desativado*	Copia todas as imagens capturadas para a galeria/o rolo da câmera do usuário	

Tabela 15-6 Política do cliente — Práticas recomendadas

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>Wait for Refresh on Lost Video Frame</b> (Aguardar a atualização do quadro de vídeo perdido)	<input type="checkbox"/> Desabilitado *	Quando habilitada, essa configuração melhora a qualidade do vídeo incluindo ajustes na unidade máxima de transmissão (MTU) que otimiza a entrega de pacotes de mídia em ambientes desafiadores. Esse recurso permite exibir a última melhor imagem até que pacotes de vídeo completos sejam recebidos.	Essa capacidade é ideal em situações nas quais a qualidade da imagem é mais importante do que o movimento.   <b>Nota:</b> essa configuração exige que os usuários do Onsight Connect baixem e instalem o software Onsight Connect mais recente e habilitem a configuração Wait for refresh on packet loss (Aguardar a atualização do pacote perdido). No Onsight Connect, clique em SETTINGS > CALLS > Video e habilite a opção Wait for refresh on packet loss (Aguardar a atualização do pacote perdido).
<b>Media Path</b> (Caminho de mídia)	{ApplicationData}	Define o caminho padrão para o armazenamento de mídia do Onsight no PC Windows do usuário.	O armazenamento no caminho de mídia deve ser rápido o suficiente para aceitar velocidades de gravação de arquivos em tempo real a fim de acompanhar o salvamento de fluxos de vídeo como gravações. A impossibilidade de acompanhar a velocidade de gravação fará com que os quadros sejam descartados na gravação e poderá causar corrupção de arquivos. Atrasos na rede podem afetar a qualidade da gravação.
<b>Login</b> (Logon)			
<b>Prompt to Remember Credentials (Auto Login)</b> (Solicitar para lembrar credenciais [logon automático])	<input type="checkbox"/> Desabilitado *	Os usuários podem inserir suas credenciais de logon para permitir o logon automático quando o aplicativo for iniciado.	Não recomendado para usuários que compartilham dispositivos.
<b>Run at Windows startup</b> (Executar na inicialização do Windows)	<input type="checkbox"/> Desabilitado *		
<b>SIP</b>			
<b>SIP messaging</b> (Mensagens SIP)	TCP *	O transporte padrão para o protocolo SIP.	
<b>Support SIP UPDATE method</b> (Suporte ao método de ATUALIZAÇÃO DE SIP)	<input checked="" type="checkbox"/> Habilitado *	Um recurso de compatibilidade de SIP usado por alguns servidores SIP para atualizar parâmetros de sessão.	

**Tabela 15-6 Política do cliente — Práticas recomendadas**

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>Verify SIP TLS Server</b> (Verificar o servidor SIP TLS)	<input checked="" type="checkbox"/> Habilitado*	Determina se os servidores SIP devem ter seus certificados verificados como autênticos antes de permitir chamadas. Isso significa que o ponto de extremidade deve ter o certificado público da Autoridade de Certificação (CA) que emitiu o certificado do servidor SIP.	A habilitação pode bloquear algumas chamadas se o servidor SIP de terceiros estiver usando certificados autoassinados. O certificado público autoassinado da CA deve ser instalado para que a verificação seja bem-sucedida e, claro, você deve confiar na CA de autoassinatura.
<b>Enable WebEx CMR Compatibility</b> (Habilitar a compatibilidade com WebEx CMR)	<input type="checkbox"/> Desabilitado*	Necessário para compatibilidade com o WebEx CMR.	Ao realizar uma chamada do Onsite no CMR, ela aparecerá como se uma "chamada dupla" estivesse acontecendo, mas a chamada se conectará com sucesso. A chamada dupla é quando a chamada inicial é atendida, mas desconecta-se imediatamente; o Onsite ligará imediatamente de volta para se conectar ao WebEx com os parâmetros de chamada aceitos.
<b>Force Media Relay</b> (Forçar retransmissão de mídia)	<input checked="" type="checkbox"/> Habilitado*	Força todas as mídias a passarem pelos servidores de mídia em vez de permitir o roteamento de mídia ponto a ponto quando os clientes estão na mesma sub-rede.	Isso é ativado por padrão para evitar que o tráfego de mídia seja bloqueado por redes que não permitem o tráfego ponto a ponto. Você pode desabilitar essa opção se tiver certeza de que o tráfego ponto a ponto é permitido; se seus clientes estiverem atrasados no uso de "redes convidadas" em locais de terceiros, eles podem ter suas chamadas bloqueadas se não for permitido.
<b>Media Configurations</b> (Configurações de mídia)			
<b>Custom Media Configurations</b> (Configurações personalizadas de mídia)	Gerenciar configurações de mídia	Crie configurações personalizadas de mídia e selecione-as para distribuir por meio da política do cliente.	As configurações personalizadas de mídia podem ser definidas com base na localização ou situação. Por exemplo, você sabe que um grupo de funcionários do serviço de campo sempre se depara com condições precárias de rede celular em um determinado local. Defina uma configuração de mídia específica para esse local e atribua essa configuração à política do cliente do grupo de serviço de campo.

**Tabela 15-6 Política do cliente — Práticas recomendadas**

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>Bandwidth Control</b> (Controle de largura de banda)			
<b>Bandwidth Control</b> (Controle de largura de banda)	<input type="checkbox"/> Desabilitado*	Quando habilitado, permite que o administrador defina a taxa máxima de bits de vídeo permitida para configurações de mídia em um ponto de extremidade.	
<b>Maximum Video Bit Rate (Kbps)</b> (Taxa máxima de bits de vídeo [Kbps])	2.500*	Define a taxa máxima de bits de vídeo permitida. (8 — 6.000)	
<b>Default MTU Size (bytes)</b> (Tamanho da MTU padrão [bytes])	1.200	Por padrão, a unidade máxima de transmissão (MTU) é definida como 1.200 bytes. Os clientes podem ajustar essas configurações em ambientes difíceis para melhorar a qualidade do vídeo.	
<b>Bandwidth Adaptive Streaming (BAS)</b> (Streaming adaptável de largura de banda [BAS])	Cellular Networks (Redes celulares)*	Habilita o BAS (streaming adaptável de largura de banda) para usuários de Smartphones. O BAS soltará dinamicamente os quadros para manter uma conexão em redes de baixa largura de banda, dando preferência aos pacotes de áudio.	O BAS é recomendado para garantir a conectividade de chamadas em redes não confiáveis, como redes celulares. O áudio é priorizado em uma chamada para manter a comunicação durante uma chamada do Onsite. Os usuários podem ajustar a configuração de mídia para resoluções mais baixas e compartilhar imagens estáticas de alta resolução em condições de baixa largura de banda.
<b>Media configuration on connection</b> (Configuração de mídia na conexão)	Nulo	Defina a configuração padrão de mídia usada ao conectar chamadas.	Isso deve ser definido como uma configuração de mídia de largura de banda mais baixa, uma vez que as chamadas podem estar acontecendo em condições de rede desconhecidas. Configurações de mídia de maior resolução/largura de banda podem ser selecionadas durante a chamada. Os usuários normalmente executariam um teste de largura de banda para determinar a largura de banda máxima disponível durante a chamada.
<b>Pause Video While Transferring Image</b> (Pausar vídeo ao transferir imagens)	<input checked="" type="checkbox"/> Habilitado*	Esta configuração pausa o vídeo durante uma transferência de imagem. O ponto de extremidade que é a fonte de vídeo ativa ditará se o vídeo é pausado com base nessa configuração.	

**Tabela 15-6 Política do cliente — Práticas recomendadas**

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>Preferred Voice Codec</b> (Codec de voz preferencial)	Padrão*	Determina a largura de banda de áudio usada para áudio de voz em uma chamada.	O Opus Audio Codec usará 24 Kbps como taxa de bits-alvo quando definido como padrão e 10 Kbps quando definido como "Baixa taxa de bits". Isso não inclui a sobrecarga do pacote associada a pacotes de áudio.
<b>Preferred Subject Audio Codec</b> (Codec de áudio de sujeito preferencial)	Padrão*	Determina a largura de banda de áudio para áudio associado a vídeo, também conhecido como áudio do sujeito. A maioria dos usuários não exigirá que o áudio do sujeito seja habilitado.	O Opus Audio Codec usará 24 Kbps como taxa de bits-alvo quando definido como padrão e 10 Kbps quando definido como "Baixa taxa de bits". Isso não inclui a sobrecarga do pacote associada a pacotes de áudio. O áudio do sujeito deve ser usado quando o isolamento de áudio for necessário como parte da solução de problemas. Por exemplo, ruído de um motor. Normalmente, um microfone externo é usado com um Onsite Collaboration Hub ou com o adaptador de várias portas do 5000HD.
<b>Audio Efficiency</b> (Eficiência de áudio)	Menor latência*	Usada para determinar como os pacotes de áudio de voz são entregues em uma chamada. A menor latência enviará pacotes de áudio à medida que forem gerados. A largura de banda inferior irá agrupar pacotes de áudio para reduzir a sobrecarga de rede associada gerada pelo envio individual de pacotes.	Para redes de grande largura de banda: > 1 Mbps, escolha MENOR LATÊNCIA. Para redes de largura de banda média: 500 Kbps — 1 Mbps, escolha LATÊNCIA/LARGURA DE BANDA MÉDIA. Para redes de baixa largura de banda: < 500 Kbps, escolha MENOR LARGURA DE BANDA. Para redes de satélite: < 500 Kbps com alta latência, escolha MAIOR LATÊNCIA
<b>Calls (Chamadas)</b>			
<b>Allow New Contacts</b> (Permitir novos contatos)	<input type="checkbox"/> Desabilitado*	Desabilitada por padrão, essa configuração permite que os clientes adicionem contatos fora de sua organização usando um endereço SIP. Quando habilitada, os usuários só podem acessar o Diretório global de sua organização, e o sinal de adição está ausente da janela de contatos.	Use a configuração padrão, a menos que o cliente tenha preocupações de privacidade e queira que esse recurso seja habilitado para restringir chamadas apenas para seu Diretório global e membros do grupo.
<b>Allow Cellular/Mobile Data Usage</b> (Permitir o uso de dados de celulares/dispositivos móveis)	<input type="checkbox"/> Desabilitado*	Necessário para usuários de smartphones sem acesso Wi-Fi.	Os usuários de dados de celular devem ter isso habilitado. Por exemplo, usuários do serviço de campo que não têm acesso a redes sem fio 802.11.

Tabela 15-6 Política do cliente — Práticas recomendadas

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>Prompt to Enable Cellular/Mobile Data Usage</b> (Prompt para ativar o uso de dados de celulares/dispositivos móveis)	Never (Nunca)*	Define quando você solicita ao usuário permissão para usar dados de celular.	
<b>Start remote / non-Onsight video on connection</b> (Iniciar vídeo remoto/não Onsight na conexão)	<input type="checkbox"/> Desabilitado*	Ao chamar pontos de extremidade que não são do Onsight, a transmissão de vídeo é iniciada automaticamente.	Isso evita confusão ao ligar para videoconferências ou salas de reunião de terceiros. Às vezes, os usuários esquecem de iniciar a transmissão de vídeo.
<b>Fill / Fit video in viewfinder when streaming</b> (Preencher/ajustar vídeo no visor ao transmitir)	Fill (Preencher)*	Fill — preenche o visor horizontalmente. A parte superior e a inferior podem ser cortadas para caber. Fit — preenche a tela verticalmente. Uma borda preta pode aparecer nas laterais do visualizador. Actual Size: exibe o vídeo em sua resolução nativa. O vídeo pode aparecer com uma borda preta ao redor dele.	
<b>Maximum Number of Connections</b> (Número máximo de conexões)	4	O PC Windows pode atuar como um host de conferências e adicionar vários participantes a uma chamada. O hardware do PC e a largura de banda de rede disponíveis para o PC Windows podem afetar a qualidade da chamada.	
<b>Auto Answer</b> (Resposta automática)	<input type="checkbox"/> Desabilitado*	Permite responder automaticamente a uma chamada recebida.	Útil para pontos de extremidade autônomos, como Onsight Rugged Smart Cameras.
<b>Auto answer delay (seconds)</b> (Atraso de resposta automática [segundos])	5	Define o atraso antes que uma chamada recebida seja atendida automaticamente.	
<b>Push Notifications</b> (Notificações por push)	<input checked="" type="checkbox"/> Habilitado*	Determina se os clientes Android usarão notificações por push quando o aplicativo estiver em segundo plano ou não estiver em execução. Os dispositivos iOS sempre usam notificações por push de acordo com a política da Apple.	Habilitar notificações por push permite que o Onsight Connect tenha a bateria otimizada por um dispositivo Android; se as notificações por push forem desativadas, o Onsight Connect deverá ser ignorado pela otimização da bateria para que possa acessar a rede enquanto um dispositivo estiver no modo de espera ou hibernação.

Tabela 15-6 Política do cliente — Práticas recomendadas

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>Prompt to Ignore Battery Optimizations</b> (Prompt para ignorar otimizações da bateria)	<input checked="" type="checkbox"/> Habilitado*	Existem duas opções: sempre que as notificações por push estiverem desabilitadas. Somente quando o usuário desabilitar as notificações por push.	Ignorar as otimizações da bateria permite que um aplicativo acesse a rede quando o dispositivo está no modo de espera ou hibernação. Para dispositivos Android: quando um usuário desabilita as notificações por push, isso desencadeia um pop-up, solicitando ao usuário que habilite a opção para ignorar otimizações da bateria. Isso o levará às configurações externas de otimização de bateria do Android, onde devem selecionar o Onsite para removê-lo da lista de aplicativos com otimização de bateria no dispositivo.   <b>Nota:</b> se um usuário optar por não ativar a opção para ignorar otimizações da bateria, ele não receberá notificações quando o dispositivo estiver no modo de hibernação. E ele não precisará habilitar a opção para ignorar otimizações da bateria novamente, a menos habilite e depois desabilite de novo as notificações por push.
<b>Encryption Mode</b> (Modo de criptografia)	Auto (Automático)*	O padrão deve ser Auto, isso garante que todas as conexões do Onsite terão criptografia habilitada durante a chamada. A opção Auto também dá a flexibilidade de chamar sistemas de videoconferência que não possuem a criptografia configurada.	Se não quiser chamar sistemas que não possuem a criptografia configurada, defina a criptografia para On (Ativada). Pontos de extremidade que não dão suporte a criptografia não são aceitos como uma conexão válida.
<b>Prompt to Share Images After Capture</b> (Solicitar compartilhar imagens após a captura)	<input checked="" type="checkbox"/> Habilitado*	O usuário será solicitado a compartilhar após uma captura de imagem.	Habilitar para usuários iniciantes e convidados.
<b>Allow recording video/audio and saving images for ALL participants (Privacy Mode)</b> (Permitir gravação de vídeo/áudio e salvamento de imagens para TODOS os participantes [Modo de privacidade])	<input type="checkbox"/> Desabilitado*	Desativa gravações e instantâneos para todos os participantes em uma chamada.	Pode ser usado para convidados externos ou grupos específicos com base em requisitos de privacidade.
<b>Local Privacy Mode</b> (Modo de privacidade local)	Allow recordings and saving snapshots (Permitir gravações e salvamento de instantâneos)*	Permite flexibilidade em quais mídias podem ser armazenadas pelos usuários.	Pode ser usado para convidados externos ou grupos específicos com base em requisitos de privacidade.

**Tabela 15-6 Política do cliente — Práticas recomendadas**

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>Software Acoustic Echo Cancellation (AEC)</b> (Software de cancelamento de eco acústico [AEC])	<input checked="" type="checkbox"/> Habilitado	Padrão ativado ou desativado	A definir
<b>Software Acoustic Echo (AEC)</b> (Software de cancelamento de eco acústico [AEC])	A definir	Padrão ativado ou desativado	A definir
<b>Noise Suppression</b> (Supressão de ruído)	<input checked="" type="checkbox"/> Habilitado	Padrão ativado ou desativado	
<b>Save Call Transcript</b> (Salvar transcrição de chamada)	<input checked="" type="checkbox"/> Habilitado	Padrão habilitado	Permite que todas as chamadas sejam transcritas no idioma (padrão).
<b>Require consent for remote video sharing requests</b> (Exigir consentimento para solicitações de compartilhamento de vídeo remoto)	<input type="checkbox"/> Desabilitado*	O padrão é desabilitado. Quando habilitado, o consentimento deve ser dado antes de iniciar uma transmissão de vídeo com um participante.	Pode ser usado para convidados externos ou grupos específicos com base em requisitos de privacidade. Essa configuração oferece aos clientes maior controle sobre o compartilhamento de vídeo durante uma chamada do Onsite. A privacidade de vídeo é aprimorada em locais confidenciais, exigindo que os usuários forneçam consentimento antes de compartilhar vídeo.
<b>Networking</b> (Sistema de rede)			
<b>Diffserv DSCP (Voice)</b> (Diffserv DSCP [Voz])	Melhor esforço*	Melhor esforço: 0, Carga controlada: 24, Áudio/Vídeo/Garantido: 40, Voz: 56	
<b>Diffserv DSCP (Video)</b> (Diffserv DSCP [Vídeo])	Melhor esforço*		
<b>Diffserv DSCP (Subject Audio)</b> (Diffserv DSCP [Áudio do sujeito])	Melhor esforço*		
<b>Diffserv DSCP (Data Stream)</b> (Diffserv DSCP [Fluxo de dados])	Melhor esforço*		
<b>TeamLink</b>			
<b>Enable TeamLink</b> (Habilitar o TeamLink)	<input checked="" type="checkbox"/> Habilitado*	Quando habilitado, o TeamLink determinará se o firewall deve permitir o registro direto de SIP ou se ele deve usar mensagens SIP de HTTPS para proxy por meio dos servidores do TeamLink.	
<b>Allow HTTP registration</b> (Permitir registro HTTP)	<input checked="" type="checkbox"/> Habilitado*	Usado para solução de problemas.	O HTTPS é usado por padrão e é o transporte preferido para o TeamLink; o HTTP só será usado se o HTTPS não estiver disponível.

Tabela 15-6 Política do cliente — Práticas recomendadas

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>Do not allow direct SIP registration (Use for troubleshooting only)</b> (Não permitir o registro direto de SIP [Usar apenas para solução de problemas])	<input type="checkbox"/> Desabilitado *	Quando habilitado, o TeamLink fará proxy de todo o tráfego em HTTPS.	Isso só é recomendado para solução de problemas. Forçar o TeamLink pode resultar em seu uso quando não for necessário.
<b>Firewall Detect</b> (Detecção de firewall)			
<b>SIP Detection Method</b> (Método de detecção de SIP)	TeamLink *	Usado para determinar quais servidores são alvo do TeamLink para o teste de detecção de firewall. O teste de detecção de firewall determinará o melhor método a ser usado para passar pelo firewall.	Essa configuração não deve ser alterada, a menos que você tenha consultado o suporte da Librestream.
<b>Workspace</b>			
<b>Access</b> (Acesso)	<input checked="" type="checkbox"/> Habilitado *	Autoriza o acesso dos membros do grupo ao Onsight Workspace.	Só habilite o Onsight Workspace quando os usuários precisarem fazer upload, visualizar e editar arquivos ao usar o Onsight Connect.
<b>Upload Path</b> (Caminho de upload)	~/onsight	Define a estrutura de diretório de alto nível no Workspace. Todos os arquivos carregados serão colocados no caminho de upload em uma pasta de chamada.	Todos os membros do grupo terão suas pastas de chamada colocadas no caminho de upload. Use um caminho de upload diferente para diferentes grupos.
<b>Auto Upload Media</b> (Upload automático de mídia)	<input type="checkbox"/> Desabilitado *	Quando habilitado, todos os arquivos capturados durante uma chamada do Onsight serão automaticamente carregados no Workspace assim que a chamada terminar.	Os usuários não terão controle sobre quais arquivos serão carregados.
<b>Maximum Upload Bit Rate (Kbps)</b> (Taxa máxima de bits de upload [Kbps])	0 *	Quando definido para 0, o upload de arquivos continuará sem quaisquer restrições de largura de banda controladas pelo aplicativo. Quando definido para um limite, o upload de arquivos não excederá o valor máximo em Kbps.	 <b>Nota:</b> a taxa de bits de upload estará sujeita a quaisquer limitações de rede na largura de banda.

Tabela 15-6 Política do cliente — Práticas recomendadas

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>Restrict Upload Folder Access to Owner</b> (Restringir o acesso da pasta de upload ao proprietário)	<input type="checkbox"/> Desabilitado*	Por padrão, todos os usuários do Workspace podem visualizar todas as pastas. Quando habilitado, os usuários só podem acessar as pastas de upload que possuem. As permissões de pasta no Workspace deverão ser editadas manualmente para reverter essa configuração.	As permissões de arquivos e pastas podem ser editadas por um administrador fazendo logon no Onsight Workspace. Tenha cuidado ao habilitar essa configuração, desfazer as permissões para permitir o compartilhamento pode ser cansativo para vários diretórios.   <b>Nota:</b> mesmo que todos os usuários tenham acesso total a todas as pastas do Workspace, os arquivos originais estão sempre protegidos contra a edição. As edições só podem ser realizadas em cópias com versão dos arquivos originais.
<b>Allow cellular/mobile data usage</b> (Permitir o uso de dados de celulares/dispositivos móveis)	<input checked="" type="checkbox"/> Habilitado*	Quando habilitado, os arquivos serão carregados usando os dados de celular/móveis se não houver uma conexão sem fio disponível. Quando desabilitado, os arquivos não serão carregados até que uma conexão de rede sem fio esteja disponível.	A prioridade será para o upload de arquivos por uma rede sem fio. Os dados de celular/dispositivos móveis só serão usados na ausência de uma rede sem fio.
<b>Artificial Intelligence</b> (Inteligência artificial)			
<b>AI Setting</b> (Configuração de IA)	Nenhum	Define o perfil de IA padrão.	 <b>Nota:</b> apenas um perfil de configuração de IA pode ser aplicado a uma política do cliente. Recomendamos combinar todas as configurações de IA dentro de um único perfil.
<b>CV Document Link URL</b> (URL do link de documentos de CV)	Nenhum	Define a URL do link de documentos de visão computacional	Digite a URL dentro no campo <b>CV Document Link URL</b> . Isso permitirá que você gerencie todos os seus links de documentos a partir de um único local.   <b>Nota:</b> links personalizados (Documento) não funcionarão se <b>Local Privacy Mode</b> estiver ativado para sua conta de domínio, grupo ou usuário.

**Tabela 15-6 Política do cliente — Práticas recomendadas**

Configurações	Valor	Descrição	Práticas recomendadas/Dicas
<b>Auto Tag Images</b> (Marcação automática de imagens)	<input type="checkbox"/> Desabilitado *		
<b>Transcription Language</b> (Idioma de transcrição)		Define o idioma padrão para transcrições.	
<b>Custom Messages</b> (Mensagens personalizadas)			
<b>Login</b> (Logon)		Define a mensagem personalizada de logon quando um usuário se conecta.	A definir
<b>Recording</b> (Gravação)		Define uma mensagem personalizada de gravação que é exibida para todos os participantes quando uma chamada começa a ser gravada.	A definir

## 15.2.6. Permissões do cliente — Práticas recomendadas

Tabela 15-7 Permissões do cliente — Práticas recomendadas

Configurações	Ação					Práticas recomendadas/Dicas
	Padrões de domínio	Administrador do cliente	Usuários padrão	Usuários convidados externos	Grupo de licenças de domínio	
<b>General (Geral)</b>						
<b>Enable GPS in Video and Images</b> (Habilitar GPS em vídeo e imagens)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Não use Inherit como ação para o grupo de Usuários convidados externos sem considerar o acesso que o convidado terá à configuração. Por exemplo, se você definiu o modo de Privacidade local para desativar gravações e salvar instantâneos para o grupo de Usuários convidados externos, mas concedeu permissões para editar a configuração, você efetivamente permitiu que o usuário convidado tivesse acesso para salvar gravações e instantâneos se ele editar a configuração localmente no ponto de extremidade.
<b>Show GPS Overlay</b> (Mostrar sobreposição de GPS)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Show Date/Time Overlay</b> (Mostrar sobreposição de data/hora)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Text Location of Overlay</b> (Localização do texto da sobreposição)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Text Size of Overlay</b> (Tamanho do texto da sobreposição)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Image Capture Resolution</b> (Resolução da captura de imagem)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Permite que o usuário defina a resolução de captura de imagem.
<b>Encoder Hardware Acceleration</b> (Aceleração de hardware do codificador)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Aplica-se apenas aos PCs Windows.
<b>Media Path</b> (Caminho de mídia)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Copy Captured Image to Gallery / Camera Roll</b> (Copiar imagem capturada para a galeria/o rolo da câmera)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	

\* Todos os valores padrão são marcados com um asterisco.

**Tabela 15-7 Permissões do cliente — Práticas recomendadas**

Configurações	Ação					Práticas recomendadas/Dicas
	Padrões de domínio	Administrador do cliente	Usuários padrão	Usuários convidados externos	Grupo de licenças de domínio	
<b>Allow Illumination</b> (Permitir iluminação)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Aplica-se a qualquer cliente que dê suporte a iluminação.
<b>Allow Flash</b> (Permitir flash)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Aplica-se a qualquer cliente que dê suporte a Flash.
<b>Allow Laser</b> (Permitir laser)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Aplica-se apenas ao Cube.
<b>Login</b> (Logon)						
<b>Auto Login</b> (Logon automático)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Não recomendado para usuários que compartilham um dispositivo.
<b>Run at Windows startup</b> (Executar na inicialização do Windows)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>SIP</b>						
<b>SIP messaging</b> (Mensagens SIP)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Support SIP UPDATE method</b> (Suporte ao método de ATUALIZAÇÃO DE SIP)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Verify SIP TLS Server</b> (Verificar o servidor SIP TLS)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Enable WebEx CMR Compatibility</b> (Habilitar a compatibilidade com WebEx CMR)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Force Media Relay</b> (Forçar retransmissão de mídia)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>IP Calls</b> (Chamadas IP)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Media Configurations</b> (Configurações de mídia)						
<b>Low Profile</b> (Perfil baixo)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Medium Profile</b> (Perfil médio)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>High Profile</b> (Perfil alto)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>HD (720p) Profile</b> (Perfil HD [720p])	Allow*	Allow*	Inherit*	Inherit*	Inherit*	

**Tabela 15-7 Permissões do cliente — Práticas recomendadas**

Configurações	Ação					Práticas recomendadas/Dicas
	Padrões de domínio	Administrador do cliente	Usuários padrão	Usuários convidados externos	Grupo de licenças de domínio	
<b>Full HD (1080p) Profile</b> (Perfil Full HD [1080p])	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Custom Profiles</b> (Perfis personalizados)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Bandwidth Control</b> (Controle de largura de banda)						
<b>Enable Bandwidth Control</b> (Habilitar controle de largura de banda)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Maximum Video Bit Rate</b> (Taxa máxima de bits de vídeo)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Enable BAS</b> (Habilitar BAS)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Você pode querer possibilitar aos usuários a edição de BAS, pois pode não ser necessário em redes celulares não congestionadas. O BAS pode restringir a taxa de quadros desnecessariamente se a rede sofrer uma queda temporária na largura de banda.
<b>Media MTU</b> (MTU de mídia)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	Um usuário médio nunca deve precisar ajustar o MTU. A equipe de TI pode achar isso útil ao solucionar problemas de rede.
<b>Media configuration on connection</b> (Configuração de mídia na conexão)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Isso deve ser definido como uma configuração de mídia de largura de banda mais baixa, uma vez que as chamadas podem estar acontecendo em condições de rede desconhecidas. Configurações de mídia de maior resolução/largura de banda podem ser selecionadas durante a chamada. Os usuários normalmente executariam um teste de largura de banda para determinar a largura de banda máxima disponível durante a chamada.
<b>Pause Video while transferring image</b> (Pausar vídeo ao transferir imagens)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Em redes ruins, transmitir vídeo durante a transferência de uma imagem pode afetar a qualidade da chamada, você pode querer possibilitar que os usuários definam "Pause video while transferring".
<b>Preferred Voice Codec</b> (Codec de voz preferencial)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	O G.7.11 pode ser usado quando a largura de banda da rede é boa (> 300 Kbps), o GSM deve ser usado em condições de baixa largura de banda. Em condições ruins de rede, pode ser vantajoso mudar para o codec de largura de banda inferior (GSM). No entanto, a prática recomendada é controlar codecs de áudio com a política do cliente.

Tabela 15-7 Permissões do cliente — Práticas recomendadas

Configurações	Ação					Práticas recomendadas/Dicas
	Padrões de domínio	Administrador do cliente	Usuários padrão	Usuários convidados externos	Grupo de licenças de domínio	
<b>Preferred Subject Audio Codec</b> (Codec de áudio de sujeito preferencial)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	O áudio do sujeito deve ser usado quando o isolamento de áudio for necessário como parte da solução de problemas. Por exemplo, ruído de um motor. Normalmente, um microfone externo é usado com um Onsite Collaboration Hub ou com o adaptador de várias portas do 5000HD. Se um usuário precisa de áudio de sujeito ocasionalmente, isso deve ser definido como "Allow".
<b>Audio Efficiency</b> (Eficiência de áudio)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Esta configuração pode ser útil para usuários que estão transmitindo pelo satélite BGAN. No entanto, os usuários do BGAN devem ter a eficiência de áudio definida como "Lower Bandwidth" por meio da política do cliente.
<b>Calls (Chamadas)</b>						
<b>Allow Cellular/Mobile Data Usage</b> (Permitir o uso de dados de celulares/dispositivos móveis)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Start remote / non-Onsite video on connection</b> (Iniciar vídeo remoto/não Onsite na conexão)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Maximum Number of Connections</b> (Número máximo de conexões)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Enable auto answer</b> (Habilitar a resposta automática)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Necessário para compatibilidade com alguns sistemas de videoconferência de terceiros.
<b>Auto answer delay (seconds)</b> (Atraso de resposta automática [segundos])	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Push Notifications</b> (Notificações por push)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Apenas para clientes Android.
<b>Encryption Mode</b> (Modo de criptografia)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Prompt to Share Images After Capture</b> (Solicitar compartilhar imagens após a captura)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	

Tabela 15-7 Permissões do cliente — Práticas recomendadas

Configurações	Ação					Práticas recomendadas/Dicas
	Padrões de domínio	Administrador do cliente	Usuários padrão	Usuários convidados externos	Grupo de licenças de domínio	
<b>Disable recordings and saving snapshots for all participants</b> (Desativar gravações e salvar instantâneos para todos os participantes)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Local Privacy Mode</b> (Modo de privacidade local)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
Exigir consentimento para solicitações de compartilhamento de vídeo remoto	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Networking</b> (Sistema de rede)						
<b>Diffserv DSCP (QoS)</b>	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
<b>TeamLink</b>						
<b>Enable/Disable TeamLink</b> (Habilitar/desabilitar TeamLink)	Allow	Allow	Inherit*	Inherit*	Inherit*	
<b>Change TeamLink Settings</b> (Alterar configurações do TeamLink)	Deny*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Firewall Detect</b> (Detecção de firewall)						
<b>SIP Detection Method</b> (Método de detecção de SIP)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	
<b>Workspace</b>						
<b>Maximum Upload Bit Rate (Kbps)</b> (Taxa máxima de bits de upload [Kbps])	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Permitir que os usuários editem a taxa de bits de upload pode ser útil para uploads de arquivos grandes.
<b>Allow cellular/mobile data usage</b> (Permitir o uso de dados de celulares/dispositivos móveis)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Permitir que os usuários editem o uso de dados de celulares/dispositivos móveis pode afetar os planos de dados.

**Tabela 15-7 Permissões do cliente — Práticas recomendadas**

Configurações	Ação					Práticas recomendadas/Dicas
	Padrões de domínio	Administrador do cliente	Usuários padrão	Usuários convidados externos	Grupo de licenças de domínio	
<b>Software Updates</b> (Atualizações de software)						
<b>Install Software Updates</b> (Instalar atualizações de software)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Permite que os usuários instalem atualizações de software do OPM (PC, Cube, 5000HD, Hub).
<b>Update Server</b> (Atualizar servidor)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Permite que um usuário insira uma URL de atualização de software em uma rede local que aponta para um pacote de atualização do Onsite.
<b>Check for updates automatically</b> (Verificar se há atualizações automaticamente)	Allow*	Allow*	Inherit*	Inherit*	Inherit*	Permite alertas automáticos de atualização de software quando o usuário faz logon em um cliente.

**Informações relacionadas**

[Política do cliente e Permissões \(na página 77\)](#)

# Índice Remissivo

## Caracteres Especiais

- Última atividade 89
- Última versão publicada 77, 77

## Numéricos

- 443 9
- 5000HD 76, 77
- 802.11 a/b/g/n 9

## A

- Ação 77
- Acesso 73
- Acesso à Internet pública 54
- Acesso ao conteúdo 51
- Acesso ao Workspace 19
- Acesso de leitura/gravação 86
- Acesso de superadministrador 52
- Ações comuns 13, 25, 27, 29, 31, 34, 35, 52, 52, 53
- Adicionar à lista 48
- Adicionar aos contatos 14
- Adicionar membros 34
- Adicionar membros selecionados 34
- Adicionar um contato externo manualmente 45
- Adicionar um grupo manualmente 23
- Adicionar usuários 25
- Adicionar/Remover contatos externos de listas 48
- Adicionar/Remover membros do grupo 34
- Administração do local 69
- Administrador 13, 16, 23, 25, 31, 51
- Administrador de grupo 25, 31, 31, 31
- Administrador do cliente 25
- Administrador do OnSight 43
- Administrador do OPM 53, 77
- Administrador do servidor SIP 72
- Administrador principal 13
- Administrador temporário 16
- Administradores 13, 61
- Administradores adicionais 31
- Administradores de grupo 34, 34, 35
- Advertência 94
- Ajuda de mensagens personalizadas 86
- Alemão 101
- Algoritmo da assinatura 63, 63
- Algoritmo Digest 63, 63
- Alterar configurações 31
- Alterar proprietário da conta 52, 53
- Alterar senha 13
- Alterar senhas 31
- Alterar tipo de conta 31
- Amarelo 78
- Ambos 98, 98
- Android 28, 77
- Anonimização de dados 56, 96
- Anonimização de dados de PII 56
- Anonimização programada 56
- Anonimizar dados de usuários ativos 56
- Anonimizar usuários excluídos anteriormente do seu domínio 56
- Anônimo 56
- Apenas em inglês 101
- API de chamada do OnSight 54
- API de medição de IoT 87
- API de OCR 87
- API de processamento de linguagem natural 87
- API de SMS 85
- API de usuários convidados 54
- API de visão computacional 87
- API do dispositivo de IoT 87
- API do SCIM 54
- API do Workspace 54, 73
- APIs 53
- Aplicar filtro 89, 91, 94, 94, 98
- Aplicativo de planilhas 40
- App Store do iOS 28
- Arquitetura da plataforma de realidade aumentada do OnSight 7
- Arquitetura segura 73
- Arquivo Contacts.xml 40
- Arquivo CSV 40
- Arquivo de metadados do IdP 62
- Arquivo de valores separados por vírgula (CSV) 39
- Arquivo para importação 40, 40
- Assinar solicitações de autenticação 63, 63
- Assinatura digital 69
- Associação ao grupo 39, 77
- Associação ao grupo de licenças 25, 25
- Associação ao grupo de políticas 25, 40
- Atividade do cliente 89, 96
- Ativo 75, 89
- Ativos 19
- Ativos do Workspace 75
- Atribuição automática de autorregistro 70
- Atribuição automática de contas SIP a novos usuários 39, 40
- Atribuição automática de contas SIP a usuários autorregistrados 72
- Atribuição de administradores de grupo 35
- Atribuição de licenças 39
- Atribuição de um administrador a um grupo 31
- Atribuição manual de contas SIP 73
- Atribuir automaticamente uma conta SIP a este usuário 16, 25, 73
- Atribuir contas SIP automaticamente a usuários autorregistrados 70
- Atribuir usuários a um grupo 31
- Atribuir/restaurar conta do Workspace 73
- Atribuir/Restaurar conta SIP 25, 73
- Atributo 64, 65, 66, 67
- Atributo de IdP mapeado 40
- Atributo de SSO 29
- Atributo do IdP mapeado 64, 64, 65, 66
- Atualizações 77
- Atualizações automáticas 77
- Atualizações de software 76, 77
- Atualizações do cliente móvel do OnSight 77
- Atualizações do OnSight Collaboration Hub 54
- Atualizar 91
- Atualizar registros existentes 40, 46
- Auditar conteúdo 73
- Autenticação 57
- Autenticação HTTP básica 75
- Autenticado 51
- Autenticado localmente por 30 dias no cliente 51
- Autenticar novamente 51
- Automatizar o processo de logon 28

Autorizado 51  
 Autorregistro 25, 59, 60, 70  
 Autorregistro de SSO 67

**B**

Baixar certificado do SP 62, 69  
 Baixar modelo de importação 40, 46  
 Bem-vindo ao e-mail do Onsite 43  
 Bloquear 87

**C**

Cabeçalhos de colunas 39  
 Cabeçalhos HTTP 75  
 Caminho de upload 73  
 Campo da conta Onsite 64, 64, 66  
 Campos da conta Onsite 64  
 Campos personalizados 57, 59, 79, 96, 96, 96  
 Captura de imagens estáticas 54  
 Capturar conteúdo 19  
 Casos especiais 39  
 Certificado do IdP 63, 63  
 Certificado do SP 62  
 Certificado público do IdP 63  
 Certificado SHA1 do provedor de serviços local 69  
 Chamada 98  
 Chamada com vários participantes 54  
 Chamada de altitude 91  
 Chamada de latitude 91  
 Chamada de participante 91  
 Chamada de usuário 91  
 Chamada do Onsite 20  
 Chamadas 91  
 Chamador 98, 98  
 Chave 60  
 Chave de API 94  
 Chave de autorregistro 43  
 Chave de registro 60  
 Chave gerada pela API 87  
 CHAVES DE API 86  
 Chaves de interface de programação de aplicativos 86  
 Chinês (simplificado) 101  
 Cisco VCS Expressway 71  
 Cliente criado 52  
 Cliente Onsite 58  
 Cliente Onsite Connect 7, 13  
 Clientes corporativos 61, 62  
 Codec de áudio 91  
 Codec de vídeo 91  
 Codec de voz 91  
 Codificação de chave 69  
 Código de desafio 43  
 Código QR de contato com o suporte 107  
 Colaborador 19  
 Colaborar 19  
 Coleta de dados do Workspace 73  
 Collaboration Hub 76, 77  
 Com filtro 38  
 Compartilhamento de tela 54  
 Compartilhamento de vídeo 84  
 Compartilhar áudio 7  
 Compartilhar conteúdo 19  
 Compartilhar dados 73  
 Compartilhar gravações 73  
 Compartilhar imagens 7, 73  
 Compartilhar vídeo 7  
 Compatibilidade com WebEx CMR 85  
 Complemento licenciado 62  
 Completo 86

Comportamento do usuário convidado 78  
 Comprimento máx. da mensagem SMS para o usuário 88  
 Comprimento mínimo 60  
 Conceder acesso 60  
 Configuração 52  
 Configuração da chamada 91  
 Configuração da política do cliente 80  
 Configuração das definições do seu IdP 62  
 Configuração das permissões do cliente 82  
 Configuração de IIS 9  
 Configuração de SAML 61, 62, 62, 63, 63, 64, 64  
 Configuração de um Webhook 75  
 Configuração do certificado SSO 69  
 Configuração do nível de domínio 78  
 Configuração do provedor de identidade parceiro 63  
 Configuração do Security Assertion Markup Language 62  
 Configuração do servidor 69  
 Configuração manual das definições do seu IdP 63  
 Configurações 29, 51, 52  
 Configurações de clientes de usuários 25  
 Configurações de domínio 31  
 Configurações de IA 87  
 Configurações de inteligência artificial (IA) 87  
 Configurações de mídia 54  
 Configurações de nível de grupo 31  
 Configurações de privacidade 84  
 Configurações de segurança e SSO 29  
 Configurações de SSO 40  
 Configurações do cliente 16, 25, 31  
 Configurações do provedor de serviços do parceiro 62  
 Configurações do provedor de serviços local 63  
 Configurações do servidor SIP privado 39  
 Configurações do SIP 40, 72  
 Configurações do SIP público 71  
 Configurações globais de convidados externos 57  
 Configurações personalizadas de mídia 55  
 Configurações pessoais 13, 13, 14  
 Confirmação 78  
 Confirmação de alteração de senha 86  
 Confirmação de convidado externo 86  
 Confirmação de usuário convidado (texto) 101  
 Confirmar as alterações 51  
 Conformidade com privacidade de dados 56  
 Connect Enterprise 19, 19, 25, 40, 53, 91  
 Connect Enterprise com Workspace Contributor 19  
 Connect Enterprise com Workspace Enterprise 19  
 Consentimento 84  
 Consumo de dados de celular 73  
 Conta 52  
 Conta compartilhada 71, 71, 72, 72, 72  
 Conta criada 86  
 Conta de usuário 57  
 Conta de usuário do Onsite 71  
 Conta do Workspace 56  
 Conta excluída 86  
 Conta registrada 86  
 Conta registrada (HTML, Texto) 101  
 Conta SIP 70, 71  
 Conta SIP principal 71  
 Contacts.csv 40  
 Contas de usuários do Onsite, 40  
 Contas Onsite 43  
 Contas SIP 71  
 CONTAS SIP 70  
 Contas SIP curinga 72  
 Contato com o suporte. 107

- Contato externo 45
- Contatos 14, 14
- Contatos externos 39, 40, 45, 47, 48, 58
- Contatos externos são públicos por padrão 58
- Contatos padrão 39
- Conteúdo 19, 73
- Contrato de licença de usuário final (EULA) 105
- Controle de domínio 21
- Controle de largura de banda 54
- Controle de versão automático 73
- Controles de permissão 73
- Controles de permissão detalhados 73
- Convidados 59
- Convidados externos 31
- Convidar um convidado externo 51
- Convite de usuário convidado (HTML, texto, SMS) 101
- Convite para convidado externo 86
- Convites para convidados externos 77
- Convites para convidados por SMS 85
- Coreano 101
- Credenciais da conta Onsign 61
- Credenciais de SSO 67
- Credenciais do Onsign 61
- Criar e excluir usuários 31
- Criar nova lista de contatos 47
- Criar novo usuário 25, 25
- Criar novos usuários 39
- Criar um novo usuário 25
- Criar um novo usuário manualmente 25
- Criar uma duplicata 46
- Criar uma lista de contatos externos 47
- Criar usuários 22
- Criptografado 91
- Criptografia SAML 69
- CSV 43, 45, 64, 89, 91, 94, 96, 96, 98
- Cube 7, 20

## D

- Dados anônimos 56, 56
- Dados anônimos não são reversíveis 56
- Dados de autenticação 62
- Dados de autorização 62
- Dados de registro temporal 57
- Dados pessoais ativos 56
- Dados Pessoais Identificáveis (PII) 56
- Data da última modificação 34
- Data de criação 34
- Data de expiração 25, 86
- Data de expiração do cliente 52
- Data de início 89, 91, 98
- Data de término 89, 91, 98
- Declaração SAML 64
- Declarações assinadas obrigatórias 63
- Departamento 16, 25
- Desabilitada 84
- Desativar conta do usuário convidado quando removido da lista de contatos 79
- Desativar o acesso ao Diretório global 78
- Descrição 23, 34, 75, 82, 86, 87, 87, 94
- Detalhes 94
- Detalhes da chamada 91
- Detalhes do grupo 34
- Direito ao esquecimento (RTBF) 56
- Diretório global 14, 34, 38, 38, 45, 45, 57, 58, 78
- Diretório global de contatos 78
- Disponibilidade do Diretório global 38
- Disponível para uso 103

- Dispositivo compatível com SIP 45
- Dispositivo móvel 20
- Dispositivos Android 54
- Distribuição de software 76
- Do endereço de e-mail 79
- Domínio 21, 22, 43
- Domínio da conta Onsign 53
- Domínio do cliente 13, 52
- Domínio do Onsign 52
- Domínio SIP 72
- Domínio SSO 62
- Domínio URI do SIP 71, 71, 72, 72
- Domínios de e-mail permitidos 60
- Download 27, 29
- Download do cliente Windows 68
- Download para iOS 28
- Download para Windows 28
- Duração 89, 91, 91, 91
- Duração da chamada 96
- Duração do bloqueio da conta 60
- Duração média 96
- Duração total 91, 96

## E

- E-mail 16, 25, 43, 65
- E-mail de boas-vindas 9, 16, 27
- E-mail de boas-vindas no local 28
- E-mail de confirmação de aprovação 43
- E-mail de convite 61
- E-mail do administrador 75
- E-mail obrigatório 60
- E-mail personalizado 55
- E-mails de boas-vindas 77
- E-mails de notificação 29
- E-mails originários do OPM 101
- Editar 19, 87
- Editar a política do cliente e as permissões 36
- Editar grupo 31, 34, 36
- Editar política do cliente 77
- Endereço 45
- Endereço (SIP) 91
- Endereço de e-mail 39, 56, 64, 65
- Endereço do servidor 72, 72
- Endereço do servidor SIP 72
- Endereço IP 89, 98
- Endereço SIP 14, 71
- Endereços de e-mail 29
- Entrada de firewall 98
- Entre 96
- Enviar e-mail de boas-vindas 16
- Enviar e-mail de boas-vindas a novos usuários 40
- Enviar e-mail de boas-vindas se o endereço de e-mail for alterado 40
- Enviar instruções 61, 69
- Enviar notificação ao usuário se a senha for alterada 40
- Equipes autorizadas 73
- Erro 94
- Escolher configurações 36, 73, 80
- Espanhol 101
- Especialistas 54
- Esqueci a senha 101
- Esquema e host do OPM 28
- Estado 89
- Estatísticas 91
- Estatísticas de chamadas 55
- Estatísticas de uso 43, 96
- Estatísticas e eventos 91

- Estilos de botão 103
- Estrutura 91
- Ethernet 10/100 9
- Europa 56
- Evento 75
- Eventos 56, 75, 94
- Excluir grupo 34
- Executar relatório 96
- Exibir dados 73
- Exibir gravações 73
- Exibir imagens 73
- Exigir declarações assinadas 63
- Exigir declarações criptografadas 63, 63
- Exigir endereço de e-mail para contas autorregistradas 29, 60, 67
- Exigir respostas assinadas 63, 63
- Expiração 79
- Expiração da conta 25, 25
- Expiração da conta de usuário 25, 25, 25
- Expiração das chaves de API 86
- Expiração de senha 59
- Expiração do usuário 53
- Exportar 40, 45, 89, 91, 94, 96, 98
- Exportar contatos externos 45
- Exportar metadados do SP 62
- Exportar usuários 43
- ExternalContacts.CSV 46

## F

- Fatal 94
- Fazer chamadas 19
- Fazer upload 40, 46, 62
- Fazer upload de arquivo 40
- Fazer upload de conteúdo 19
- Fazer upload de dados 73, 73
- Fazer upload de gravações 73
- Fazer upload de imagens 73
- Fazer upload do certificado do IdP 63, 63
- Federação da identidade do usuário 61, 64, 64, 67, 68
- Federação da identidade do USUÁRIO 64
- Federação da Identidade do usuário 65
- FEDERAÇÃO DA IDENTIDADE DO USUÁRIO 66
- Filtro do Diretório global 38, 39
- Filtros de disponibilidade do Diretório global 38
- Firewall 54, 71
- Formato URI do SIP 45, 45
- Formatos de arquivo compatíveis 45
- Francês 101
- Frequência em lotes 75
- Funcionalidade do cliente 53, 54
- Fuso horário padrão 57

## G

- Gatilho 103
- Geração de um relatório 96
- Geral 69
- Gerar chave 86
- Gerar nome de usuário automaticamente 67
- Gerar senha temporária 16
- Gerenciamento de administradores de grupo 31
- Gerenciamento de chaves de API 54, 54
- Gerenciamento de grupos de licenças 22
- Gerenciamento de grupos de licenças e políticas 21
- Gerenciamento de licenças de domínio 21
- Gerenciamento de usuários 31
- Gerenciar 19
- Gerenciar configurações de privacidade 80
- Gerenciar contatos externos 47

- Gerenciar dados 73
- Gerenciar gravações 73
- Gerenciar imagens 73
- Gerenciar licenças de usuário 21
- Gerenciar usuários 23, 34, 34, 35
- Gestão do conhecimento 73
- Google Play Store para Android 28
- GOP 91
- Gravação 104
- Gravações 19, 103
- Gravações capturadas 20
- Grupo 39, 80, 82
- Grupo de licenças 22, 23, 40
- Grupo de licenças de domínio 16, 25
- Grupo de licenças padrão 21
- Grupo de licenças para novos usuários 40
- Grupo de políticas 23, 25, 25, 25
- Grupo de políticas de domínio 16
- Grupo de políticas do cliente 25
- Grupo Todos os usuários 21
- Grupos 96, 96
- Grupos de licenças 25, 31, 53
- Grupos de licenças personalizados 22
- Grupos de políticas 25
- Guia de Webhooks do Onsignt Workspace 75
- Guias de API do Onsignt 87

## H

- Habilitação do acesso ao Workspace 73
- Habilitada 84
- Habilitado 78
- Habilitar o autorregistro 60
- Hardware 91
- Herdar 36, 77, 82, 83
- Histórico de chamadas 96
- Hora 94
- Hora de início 91, 91
- Hora do logon 89
- Host e caminho do OPM 28
- Hosts de conferência 54
- HTTPS 9, 9, 57
- Hub 7, 20

## I

- ID da entidade 62, 63, 63
- ID da sessão SIP 91
- ID de nome da entidade 64
- ID de SSO federado 16, 40, 64, 64, 66
- Idioma 16, 25
- Idioma padrão 57
- Ignorar duplicatas 46
- Ignorar duplicatas (manter registros existentes) 40
- Imagens 19
- Imagens capturadas 20
- Implantação de certificados de servidor 69
- Implantação de pacotes de atualização 77
- Importação a partir de um arquivo 46
- Importação de metadados 63
- Importação de um modelo de importação de usuários 40
- Importar 40, 45, 46, 46
- Importar arquivo 39
- Importar metadados do IdP 63
- Importar usuários 40, 46
- Importar usuários de um arquivo 25
- Impressão digital do SHA1 69
- Imprimir 98
- Incluir opção para o convidado chamar o host imediatamente 79

- Incluir registros anônimos 96
- Indivíduos 73
- Informações 94
- Informações da conta SIP 72
- Informações da conta SIP corporativa 72
- Inglês 101
- Início do fluxo 91
- Inserir modelo padrão 86
- Instalar 27, 29
- Instruções de importação de CSV 45
- Instruções habilitadas para SSO 86
- Inteligência artificial (IA) 55
- Interface de rede 91
- Interface de serviços Web 9
- Interfaces de programação de aplicativos (APIs) 54
- Internet das coisas (IoT) 56
- Internet pública 98
- Interno 71
- iOS 77, 83
- iPhone 7
- Italiano 101
- Item criado 75
- Item excluído 75
- Item modificado 75

**J**

- Japonês 101

**L**

- Lei Geral de Proteção de Dados (LGPD) 56
- Leitura 86
- Licença Connect Enterprise 16
- Licença Contributor 73
- Licença Enterprise 73
- Licença master 31
- Licença múltipla 19
- Licença única 19
- Licença Workspace Enterprise 73
- Licenças 13, 51, 52, 53, 54, 54, 60
- Licenças Connect Enterprise disponíveis 11
- Licenças de ponto de extremidade do Onsite Connect 13
- Licenças de usuário 19
- Licenças disponíveis 22
- Licenças totais e disponíveis 11
- Licenças Workspace Enterprise disponíveis 11
- Líderes potenciais 96
- Ligar para o suporte Librestream 52
- Limite 91
- Limite de 160 caracteres 78
- Limpar 77
- Link do cliente móvel 68
- Links de provisionamento de usuários 68
- Lista de contatos 58
- Lista de contatos externos 45, 46, 48
- Lista de usuários importados 64
- Lista de valores separados por vírgulas 60
- Listas de contatos 21, 45
- Localização e quantidade de chamadas/logons 98
- Logon 14, 20, 29, 51, 98, 103, 104
- Logon de administração do OPM 9
- Logon do cliente SSO 68
- Logon no Onsite Connect 28, 28
- Logon off-line 61
- Logon único 61, 61
- Lojas de aplicativos 77, 77

**M**

- Maior e menor utilização 96

- Maior ou igual 96
- Maior utilização 96, 96, 96
- Manuais e guias do OPM 83
- Mapa de calor 98
- Mapa de calor para 98
- Mapeamento de e-mail 64, 65
- Mapeamento de ID de SSO federado 64, 66
- Mapeamento de identidade 40, 64
- Mapeamento de identidade do usuário 65
- MAPEAMENTO DE IDENTIDADE DO USUÁRIO 66
- Mapeamento do nome de usuário 64, 64
- Marcação automática de imagens/vídeo 56
- Marcação de conteúdo 73
- Máximo de tentativas de logon com falha 60
- Mecanismo de notificação do Webhook 75
- Melhorar dados de relatórios 59
- Membro de 40
- Membros individuais 39
- Menor ou igual 96
- Menor utilização 96, 96, 96
- Mensagem 103
- Mensagem de boas-vindas 28
- Mensagem personalizada 103
- Mensagem SMS 78
- Mensagens personalizadas 55, 103, 104
- Mentoria/Coaching 96
- Mesclar grupos 40
- Metadados do IdP 63, 63
- Método de ativação da conta 60
- Meu perfil 13
- Microsoft Excel 40
- Mídia 54
- Mínimo de caracteres não alfabéticos 60
- Mínimo de letras maiúsculas 60
- Modelo de importação 40, 40
- Modelo de importação de usuários 40
- Modificar grupo 34, 35, 36, 73
- Modificar usuários 31
- Modo Campo 54, 79
- Modo de captura 20
- Modo de criptografia 80
- Modo de importação 40
- Modo de usuário (Especialista/Campo) 54
- Modo Especialista 54, 79
- Motivo da finalização 91, 91

**N**

- NameID 64
- Não mostrar novamente 103
- Negar 36, 82, 83
- Negar acesso de superadministrador 52
- Nenhum 86
- No local 9, 9, 11, 52, 54, 69, 75, 77
- No local — Guia de instalação 69
- Nome 16, 23, 25, 34, 39, 43, 45, 47, 67, 75, 86, 87, 87, 91
- Nome da empresa 52
- Nome de autenticação 72, 72
- Nome de autenticação exclusivo 71
- Nome de domínio do Onsite 62
- Nome de usuário 9, 16, 28, 31, 39, 43, 56, 64, 64, 67, 91
- Nome de usuário/ 75
- Nome do atributo 65, 66, 67
- Nome do campo personalizado 59
- Nome do host 89
- Nome do relatório 96
- Nome do usuário de autenticação 72
- Notificação 11, 60, 67

- Notificações de novos lançamentos 77
- Notificações do sistema 39
- Notificar os administradores por e-mail quando uma conta for registrada 67
- Notificar usuários existentes 69, 69
- Nova lista 45, 47
- Novo contato 45
- Novo grupo 23
- Novo usuário 16, 25, 25
- Número de conexões do cliente 98
- Número de licenças por tipo 53
- Número de resultados 96

## O

- O acesso à rede não está disponível 61
- O administrador deve aprovar o registro de contas usando a página de autorregistro 60
- O modo de captura não está mais disponível 20
- OamClientWebService 28, 28
- Obrigatório 61
- Onsight 5000HD 77
- Onsight Collaboration Hub 77
- Onsight Connect 43, 61
- Onsight Connect para Windows 101
- Onsight Cube 76, 77
- Onsight Platform Manager — Guia de instalação 77
- Onsight Smart Camera 83
- Onsight Workspace 73
- Opcional 29, 61
- Opções de configuração do servidor SIP 71
- Opções de licença 19
- Opções de mensagem 103
- OpenOffice Calc 40
- Operadora de celular 91
- OPM.com\user@domain 28

## P

- Padrão 78
- Padrão aberto 62
- Padrões de convite para convidados externos 79
- Página de atualizações de software 77
- Página de autorregistro 29, 43
- Página de confirmação de verificação de e-mail 43
- Página de contatos externos 46
- Página Web de autorregistro 25
- Painel 11, 13, 13, 19
- País 16, 25, 25, 96, 96
- Parâmetros 87
- Parâmetros de filtro 89, 89, 91, 94, 94, 96, 96, 98
- Participante chamado 91
- Pasta de upload 19
- PC Windows 7, 20, 83
- PCs Windows 54
- Perda de conectividade de rede 51
- Perfil 16, 25, 29, 59
- Perfil de configuração de IA 87, 87
- Perfis de configuração de IA 87
- Período de retenção de dados (DRP) 56, 96
- Permissões de administrador de grupo 31
- Permissões de cliente do grupo 83
- Permissões de usuários convidados externos 51
- Permissões do cliente 21, 23, 31, 34, 36, 55, 77, 82, 83, 83, 84
- Permissões do grupo 31
- Permissões padrão do usuário 31
- Permitir 36, 82, 83, 84
- Permitir convites por mensagens de texto 78
- Permitir definir o modo de usuário ao enviar convite para o convidado 79
- Permitir novos contatos 25
- Permitir o uso de dados de celulares/dispositivos móveis 73
- Permitir que os usuários enviem convite ao convidado externo 78
- Permitir que os usuários enviem convites 31
- Personalização 55, 86
- Personalização de e-mail 86
- Personalização de SMS 86
- Pesquisa e recuperação rápidas 73
- Pesquisar 14
- Política de cliente do grupo 83
- Política de cliente do usuário 77, 77, 77
- Política de clientes do grupo 73
- Política de grupo 31
- Política de logon 59, 60
- Política de segurança corporativa 9
- Política de senhas 59, 60
- Política do cliente 21, 21, 22, 23, 25, 31, 31, 34, 36, 51, 54, 54, 55, 58, 60, 73, 77, 80, 80, 82, 83, 84, 85, 103, 104
- POLÍTICA DO CLIENTE 80
- Política do grupo 77
- Política do grupo de administradores do cliente 25
- Ponto de extremidade 54, 87
- Ponto de extremidade de vídeo de terceiros 7
- Ponto de extremidade Onsight 45, 77
- Pontos de extremidade da API REST 87
- Pontos de extremidade de vídeo externos ou de terceiros 58
- Pontos de extremidade do Onsight 51
- Pontos de extremidade do SIP para vídeo de terceiros 45
- Pontos de extremidade remotos 9
- Pool de atribuição automática 71
- Pool SIP 71, 72
- Pool SIP de atribuição automática 25
- Pool único de licenças 21
- Portal do cliente 69
- Portas do SIP 54
- Português (Portugal e Brasil) 101
- Precedência 77
- Precedência da política 80
- Primeiro logon 9
- Privacidade de conteúdo 54, 54
- Privacidade de vídeo 84
- Privacidade de vídeo remoto 84
- Privada 47
- Privado 38, 71, 72
- Privilégios administrativos 31
- Privilégios de administrador do Onsight Platform Manager 53
- Processamento de linguagem natural (PLN) 55
- Promoção de um usuário padrão 31
- Prompt 29
- Prompt no primeiro logon 67
- Proprietário da conta 13, 13, 29, 52, 53, 53, 61
- Protocolo de início de sessão (SIP) 7, 14, 70
- Protocolo de rede HTTPS 9
- Provedor de identidade (IdP) 61, 62
- Provedor de identidade (IdP) de SSO 63
- Provedor de identidade de SSO 62, 62
- Provedor de serviços (SP) 62, 62
- Provedor de serviços local 62
- Provedor de serviços parceiro 63
- Próxima atualização 73
- Próximo logon 73
- Proxy da Web 9
- Pública 47
- Público 38, 71, 72

## Q

Qualquer 96  
Quantas chamadas 96  
Quantidades de chamadas ou logons 98

## R

Receptor da chamada 98, 98  
Recursos de auditoria 73  
Recursos de chave do Workspace 73  
Recursos de licença 53  
Recursos de passagem de firewall do TeamLink 54  
Recursos hospedados 53, 55  
Recusar 84  
Rede com fio 9  
Rede sem fio 9  
Redefinir alterações 51  
Redefinir senha 101  
Reenviar e-mail de boas-vindas 29  
Reenviar mensagem de boas-vindas 27  
Região 16, 25  
Registro de controle 54  
Registro de eventos 94, 94  
Registro do TeamLink 54  
Registro em uma conta 43, 101  
Relatório de atividades do cliente 89  
Relatório de eventos 94  
Relatório de mapa de calor 98  
Relatório do usuário exportado 59  
Relatórios 96, 96  
Relatórios avançados 55, 73  
Relatórios de chamadas 96  
Relatórios do OPM e estatísticas de chamadas 56  
Remover contato da lista 48  
Remover membros 34  
Requisitos de e-mail 29  
Requisitos de rede 9  
Requisitos de trilha de auditoria 73  
Resolução 91  
Restringir o acesso à pasta de upload ao proprietário 73  
Resultados 96  
Resultados da importação 40, 46  
Resumo da utilização da licença 96  
Resumo de convites para convidados 96  
Resumo de uso geral e licença 96  
Resumo de utilização geral 96  
Retornos de chamada HTTP 75  
Russo 101

## S

Salas de reunião do WebEx 85  
Salas de videoconferência 45  
Salvar 51  
Salvar meus dados 28  
SampleUserImport.csv 40  
Se um e-mail válido estiver configurado 29  
Seção de categoria 80  
Seção Usuários OnSight 53  
Security Assertion Markup Language (SAML) 61  
Segurança 51, 59, 60, 60, 71  
Selecionar todas as linhas 69  
Sempre usar o TeamLink 54  
Senha 9, 13, 28, 71, 75, 78  
Senha de autenticação 72, 72, 72  
Senha do usuário alterada (texto, SMS) 101  
Senha inicial 43  
Senhas 39  
serviço baseado em assinatura 7  
Serviço de mensagens curtas 85  
Serviço on-line 51

Serviço SIP hospedado 71  
Serviços de chamada 51  
Serviços de chamada OnSight 19  
Serviços de IoT 56, 87  
Servidor do Workspace 73  
Servidor privado 71, 72  
Servidor público 71, 72, 72  
Servidor SIP 71, 71, 72  
Servidor SIP corporativo 71, 71, 71  
Severidade 94  
SIP 25, 51, 54, 85  
Sistema operacional 91, 91  
Sistemas de back-office 73  
Smartphone Android 83  
Smartphones 101  
SMS 55, 55, 61, 85  
Sobregavar grupos 40  
Sobrenome 16, 25, 39, 43, 67  
Software 51  
Solicitação de redefinição de senha (texto, SMS) 101  
Solicitação para redefinir senha 86  
Solicitações de compartilhamento de vídeo remoto 84  
Solução de problemas 52  
Somente host do OPM 28  
SSO 39, 40, 55, 61, 61, 64, 64, 64, 65, 66, 67, 68, 69, 101  
SSO (Single Sign On) 16  
Status de acesso do superadministrador 52  
Status do convite 78  
Substituir 77  
Substituir a senha dos usuários existentes 40  
Sueco 101  
Superadministradores 52  
Suporte Librestream 52

## T

Tablets 101  
Tags definidas pelo cliente 86  
Taxa de bits de vídeo 91  
Taxa máxima de bits de upload (Kbps) 73  
Taxa máxima de bits de vídeo 54  
TCP 9, 71, 71, 72, 72  
TeamLink 54, 91  
Telestração 7  
Tempo reportado 91  
Tempo universal coordenado (UTC) 57  
Tendências históricas 96  
Termos de uso 103  
Tipo de associação 34  
Tipo de autenticação padrão 71  
Tipo de conta 25, 31  
Tipo de dispositivo 91  
Tipo de grupo 23  
Tipo de licença 25  
Tipo de participante 98  
Tipo de pool de atribuição 72  
Tipo de pool de contas 72  
Tipo de transporte padrão 71  
Tipo de vinculação de logon 63  
Tipos de licença 21, 40  
Tipos de licença do Workspace 19  
Tipos e permissões de conta de usuário 31  
Título 103  
TLS 71, 71, 72, 72  
Todos os contatos 47, 47  
Todos os países 96  
Todos os usuários 77, 80, 96, 96  
Torres de celular 98

- Total de licenças 34
- Total de licenças Connect Enterprise 11
- Total de licenças Workspace Contributor 11
- Total de licenças Workspace Enterprise 11
- Total de usuários 11
- Tradutor do Onsight 55
- Tratamento de duplicatas 46
- Tudo 38, 89
- Túnel de dados HTTPS 54

## U

- Um URI absoluto 28
- Upload automático 73
- Upload automático de mídia 73
- Upload manual 73
- URI 71
- URI do consumidor 75
- URI do SIP 14, 72
- URI do SIP exclusivo 72
- URL 9, 60
- URL ACS 62
- URL de autorregistro 60
- URL de logon único 63
- URL de SSO 63
- URL do Onsight Platform Manager 28
- user@domain.com 9
- user@sipdomain.com 14
- Uso de chave estendida definido 69
- Usuário 89, 94
- Usuário chamado 91
- Usuário corporativo 19
- Usuário e grupos 73
- Usuário padrão 25, 31, 31, 31
- Usuários 11, 16, 23, 25, 25, 43, 57
- USUÁRIOS 31
- Usuários aguardando aprovação de um administrador 11
- Usuários anônimos 89, 91
- Usuários ativos 11
- Usuários convidados 29
- Usuários convidados externos 11, 51, 53, 57, 58, 61, 78, 80, 86, 89, 91, 94, 96
- Usuários corporativos 40
- Usuários da API 94
- Usuários de SSO 29
- Usuários e grupos 58
- Usuários expirados 11
- Usuários Onsight 53
- Usuários padrão 61, 89, 91, 94, 96
- Usuários Windows 77

## V

- Valor 36
- Valor do campo personalizado 59
- Várias contas 71, 71, 71, 72, 72
- Várias contas de administrador 13
- Várias contas SIP 72
- Vários grupos 77
- Vários participantes 54
- Verde 78
- Verificar atualizações 77
- Verificar seu endereço de e-mail 43
- Vermelho 78
- Versão 89
- Versão específica 77
- Vinculação de SSO 63
- Visão computacional (CV) 55
- Visualização 56
- Visualização de instrumentos 56

- Visualizador do Onsight Connect 20
- Visualizar relatório 46

## W

- Webhooks do Workspace 75
- Windows 76, 77, 77, 101
- Workspace 20, 86
- Workspace Contributor 19, 19, 25, 40, 53
- Workspace Enterprise 19, 19, 25, 40, 53