Português

Manual do usuário autenticação

INC Cloud

INC Cloud

Parabéns, você acaba de adquirir um produto com a qualidade e a segurança Intelbras.

Resumo

1. Sobre a autenticação do INC Cloud

O Intelbras INC Cloud fornece métodos de autenticação abundantes para usuários de acesso, como funcionários, convidados e terminais IoT. Quando um cliente deseja acessar a Internet ou os recursos específicos da rede, o dispositivo de acesso redireciona o cliente para o INC Cloud para autenticação do portal.

A Intelbras INC Cloud oferece os seguintes benefícios: " Nenhum limite superior para clientes de autenticação. " Diversas políticas de autenticação.

" Serviços de envio de anúncios personalizados.

O Intelbras INC Cloud fornece os métodos de autenticação listados na *Tabela Métodos de autenticação.*

Métodos de autenticação:

Método de autenticação	Cenário aplicável	Observações	Combinado autenticação
Uma tecla	Baixos requisitos de auditoria e coleta de estatísticas operacionais, restaurantes e lojas.	Autenticação baseada em MAC. Os usuários podem concluir a autenticação simplesmente clicando em um botão na página de autenticação do portal.	Com suporte
Conta fixa	Os usuários da rede são fixos, como áreas de campus e escritórios.	Autenticação baseada em nome de usuário e senha. As seguintes funções são : LDAP Importação e exportação de contas Vinculação de uma conta a vários endereços MAC Limite de clientes simultâneos	Com suporte
Autenticação do Google	As operadoras usam o Google para coletar estatísticas sobre os usuários da rede.	Os usuários devem fazer login no Google para conceder acesso ao INC Cloud. Esse método está disponível somente em https://oasiscloud.intelbras.com.	Com suporte
Autenticação do Twitter	As operadoras usam o Twitter para coletar estatísticas sobre os usuários da rede.	Os usuários devem fazer login no Twitter para conceder acesso ao INC Cloud. Esse método está disponível somente em https://oasiscloud.intelbras.com.	Com suporte
Autenticação de convidados	Empresas ou lojas em que é necessário o acesso temporário de convidados.	Um convidado pode acessar a rede depois que um aprovador escaneia o código QR no terminal do convidado e autoriza o terminal.	Não suportado
Autenticação de terminal burro	Dispositivos IoT, impressoras sem fio e terminais POS.	Autenticação automatizada em terminais sem fio.	Não suportado
Autenticação do Facebook	As operadoras usam o Facebook para coletar estatísticas sobre os usuários da rede.	Os usuários devem fazer login no Facebook para conceder acesso ao INC Cloud. Esse método está disponível somente em https://oasiscloud.intelbras.com.	Com suporte

Método de autenticação e compatibilidade de rede

	Compatibilidade com redes com diferentes autenticadores		
Método de autenticação	CA	Roteador Wireless	Roteador com fio
Autenticação de uma chave	Sim	Sim	Sim
Autenticação de conta fixa	Sim	Sim	Sim
Autenticação de convidados	Sim	Sim	Sim
Autenticação do Facebook	Sim	Não	Não
Autenticação combinada	Sim	Sim	Sim
Autenticação de terminal burro	Sim	Sim	Não
Autenticação em massa	Sim	Sim	Não
Página de autenticação personalizada	Sim	Sim	Sim

Observação:

Um roteador Wireless pode atuar como um AC ou fat AP para fornecer autenticação sem fio. Um roteador com fio se conecta aos terminais diretamente ou se conecta aos terminais por meio de um switch ou de um AP fat para autenticação.

2. Configurar a autenticação do INC Cloud com um AC como o autenticador

2.1. Configurar as definições básicas

Pré-requisitos

Antes de configurar a autenticação do INC Cloud, conclua as seguintes tarefas:

- **" Conecte o dispositivo ao INC Cloud.**
  Para obter mais informações, consulte o *Guia de implantação do Intelbras INC Cloud*.
- **" Conclua as configurações de VLAN e DHCP.**
- **" Configure os serviços Wireless e certifique-se de que os APs possam ficar on-line.**

Configurar as definições no dispositivo

Restrições e diretrizes

Somente a versão de software 5405 ou superior suporta a implementação automática das configurações de autenticação. Para outras versões de software, defina manualmente as seguintes configurações no dispositivo.

Para uma implementação rápida dos seguintes métodos de autenticação, consulte *o Apêndice A. de autenticação para o dispositivo.*

- **" Autenticação de uma chave. " Autenticação de conta fixa. " Autenticação do Facebook.**
- **" Autenticação de terminal burra.**
- **" Autenticação de convidados.**

Configurar as definições gerais

1. **Configure um domínio de autenticação de portal.**
   # Adicione um domínio ISP chamado Cloud e insira sua visualização.
   <Sysname> visão do sistema
   [Sysname] domain cloud
   # Especifique os métodos de autenticação, autorização e contabilidade como nenhum.
   [Sysname-isp-cloud] authentication portal
   none [Sysname-isp-cloud] authorization portal
   none [Sysname-isp-cloud] accounting portal
   none [Sysname-isp-cloud] quit
2. **Configure a autenticação do portal Cloud.**
   # Adicione um servidor Web de portal chamado Cloud e especifique seu URL e tipo. (Se o administrador configurar o serviço Wireless no INC Cloud, a configuração será implantada no dispositivo automaticamente).
   [portal web-server cloud
   [Sysname-portal-websvr-cloud] url http://oasisauth.intelbras.com/portal/protocol
   [Sysname- portal-websvr-cloud] server-type oauth

 # Configure uma regra de correspondência para redirecionar solicitações HTTP que contenham a string de agente de usuário Captive NetworkSupport para o URL http://oasisauth.intelbras.com/generate_404.

[Sysname-portal-websvr-cloud] if-match user-agent CaptiveNetworkSupport redirect-url http:// oasisauth.intelbras.com/generate_404

 # Configure uma regra de correspondência para redirecionar solicitações HTTP que contenham a string de agente de usuário Dalvik /2.1.0(Linux;U;Android7.0;HUAWEI para o URL http://oasisauth.intelbras.com/generate_404.

[Sysname-portal-websvr-cloud] if-match user-agent Dalvik/2.1.0(Linux;U;Android7.0;HUAWEI redirect-url http://oasisauth.intelbras.com/generate_404

 # Configure uma regra de aprovação temporária para permitir a aprovação de pacotes de usuários que contenham informações do agente do usuário Mozilla e, em seguida, redirecione os pacotes destinados ao URL http://captive.apple.com para o URL http://oasisauth.intelbras.com/portal/protocol.

[Sysname-portal-websvr-cloud] if-match original-url http://captive.apple.com user-agent Mo- zilla temp-pass redirect-url http://oasisauth.intelbras.com/portal/protocol

 # Configure uma regra de aprovação temporária para permitir a aprovação de pacotes de usuários que contenham informações do agente do usuário Mozilla e, em seguida, redirecione os pacotes destinados ao URL http://www.apple.com para o URL http://oasisauth.intelbras.com/portal/protocol.

[Sysname-portal-websvr-cloud] if-match original-url http://www.apple.com user-agent Mozilla temp-pass redirect-url http://oasisauth.intelbras.com/portal/protocol

[Sysname-portal-websvr-cloud] quit

 # Configure uma regra de aprovação temporária para permitir temporariamente a aprovação de pacotes de usuários que acessam o URL http://10.168.168.168.

[portal web-server cloud

[Sysname-portal-websvr-cloud] if-match original-url http://10.168.168.168 temp-pass

 # Habilite o recurso de desvio cativo otimizado para usuários do

iOS. [Sysname-portal-websvr-cloud] captive-bypass ios optimize

enable [Sysname-portal-websvr-cloud] quit

 # Habilite a autenticação direta do portal no modelo de serviço Cloud.

[Sysname] wlan service-template Cloud

[Sysname-wlan-st-cloud] portal enable method direct

 # Configure o domínio de autenticação como Cloud e especifique o servidor Web do portal Cloud como o servidor Web do portal Cloud para autenticação do portal.

[Sysname-wlan-st-cloud] portal domain cloud

[Sysname- wlan-st-cloud] portal apply web-server cloud

[Sysname- wlan-st-cloud] quit

 # Habilite o passe temporário do portal e defina o período do passe temporário para 20 segundos.

[Sysname] wlan service-template Cloud

[Sysname-wlan-st-cloud] portal temp-pass period 20

enable [Sysname-wlan-st-cloud] quit

 # Adicione um serviço da Web de portal local baseado em HTTP e insira sua visualização.

[Sysname] portal local-web-server

http [Sysname-portal-local-websvr-

http] quit

 # Adicione um serviço da Web de portal local baseado em HTTPS e insira sua visualização.

[Sysname] portal local-web-server

https [Sysname-portal-local-websvr-

https] quit

 # Habilite os serviços HTTP e

HTTPS. [Sysname] ip http enable

[Sysname] ip https enable

 # Habilite a verificação de validade nos clientes do portal Wireless.

[Sysname] portal host-check enable

 # Habilite o registro de logins e logouts de usuários do portal.

[Sysname] portal user log enable

 # Configure a regra livre de portal baseada em destino1 para permitir que os usuários do portal acessem o serviço DNS sem autenticação. (Este exemplo usa a regra 114.114.114.114 255.255.255.255.)

[Sysname] portal free-rule 1 destination ip 114.114.114.114 255.255.255.255

 # Configure as regras 2 e 4 de portal livre baseado em destino para permitir que os usuários do portal acessem o serviço DNS sem autenticação.

[Sysname] portal free-rule 2 destination ip any udp 53

[Sysname] portal free-rule 3 destination ip any tcp 53

[Sysname] portal free-rule 4 destination ip any tcp 5223

 # Configure a regra 5 livre de portal baseada em destino para permitir que os usuários do portal acessem o servidor de autenticação do INC Cloud sem autenticação.

[Sysname] portal free-rule 5 destination oasisauth.intelbras.com

 # Configure as regras 10 a 22 de portal-free baseadas em destino para permitir que os usuários do portal acessem o servidor de autenticação do INC Cloud sem autenticação.

[Sysname] portal free-rule 10 destination short.weixin.qq.com [Sysname]

portal free-rule 11 destination mp.weixin.qq.com [Sysname] portal free-

rule 12 destination long.weixin.qq.com [Sysname] portal free-rule

13 destination dns.weixin.qq.com [Sysname] portal free-rule 14

destination minorshort.weixin.qq.com [Sysname] portal free-rule 15

destination extshort.weixin.qq.com [Sysname] portal free-rule 16

destination szshort.weixin.qq.com [Sysname] portal free-rule 17

destination szlong.weixin.qq.com [Sysname] portal free-rule 18

destination szextshort.weixin.qq.com [Sysname] portal free-rule 19

destination isdspeed.qq.com [Sysname] portal free-rule 20 destination

wx.qlogo.cn

[Sysname] portal free-rule 21 destination wifi.weixin.qq.com

[Sysname] portal free-rule 22 destination open.weixin.qq.com #

Habilite o redirecionamento seguro do portal.

[Sysname] portal safe-redirect enable

 # Especifique os métodos de solicitação HTTP permitidos pelo safe-redirect do portal.

[Sysname] portal safe-redirect method get post

 # Especifique os tipos de navegador permitidos pelo portal safe-redirect. [Sysname] portal safe-redirect user-agent Android

[Sysname] portal safe-redirect user-agent CFNetwork

[Portal safe-redirect user-agent CaptiveNetworkSupport [Sysname]

Portal safe-redirect user-agent MicroMessenger [Sysname] Portal safe-redirect user-agent Mozilla

[Sysname] portal safe-redirect user-agent iPhone [Sysname]

portal safe-redirect user-agent micromessenger

Configurar a autenticação do Facebook

Importante:

" **Execute os comandos desta seção depois de concluir as configurações em** *Configurar configurações gerais* **ou**
Apêndice A Comandos de autenticação para o dispositivo.

" **A regra livre 38 pode desativar a exibição de imagens pelo aplicativo. Configure essa regra conforme necessário ou entre em contato com o suporte técnico.**

 # Configure regras sem portal baseadas em destino para permitir que os usuários do portal que enviarem uma solicitação HTTP/HT-TPS com nomes de host relacionados ao Facebook acessem os recursos da rede sem autenticação.

<Sysname> visão do sistema

[Sysname] portal free-rule 31 destination facebook.com [Sysname]

portal free-rule 32 destination m.facebook.com [Sysname] portal free-rule 33 destination www.facebook.com [Sysname] portal free-rule

34 destination graph.facebook.com [Sysname] portal free-rule

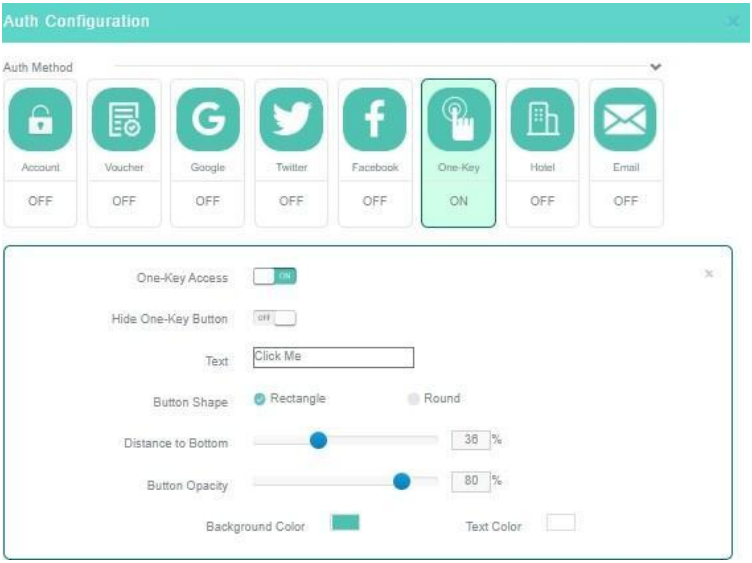
35 destination connect.facebook.net [Sysname] portal free-rule

36 destination static.xx.fbcdn.net [Sysname] portal free-rule 37 destination staticxx.fbcdn.com

[Sysname] portal free-rule 38 destination scontent-hkg-3-1.xx.fbcdn.net

Configurar a autenticação de uma chave

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Settings (Configurações>ACs> Authentication (Autenticação)* **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Para adicionar um modelo de autenticação, clique em** *Add (Adicionar)* **na guia Authentication Templates (Modelos de autenticação).**
5. **Para editar um modelo de autenticação, clique no ícone** *Edit (Editar)* **para esse modelo de autenticação.**
6. **Para vincular um modelo de autenticação a um serviço wireless, clique no ícone** *Edit (Editar)* **para esse modelo de autenticação, selecione** *Yes (Sim)* **no campo** *Bind to Wireless Service (Vincular ao serviço wireless)* **e clique em** *Apply (Aplicar).* **Se o modelo tiver sido vinculado ao serviço Wireless, pule esta etapa.**
7. **Clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**
8. **Clique na caixa** *One-Key* **na área** *Configuração de Autenticação***, ative a autenticação de uma chave e confirme a autenticação de uma chave.**
   Defina outras configurações conforme necessário.
9. **Clique em** *OK* **ou em** *Liberar* **no canto superior direito da página.**



Configuração da autenticação de uma chave

Configurar a autenticação de conta fixa

Restrições e diretrizes

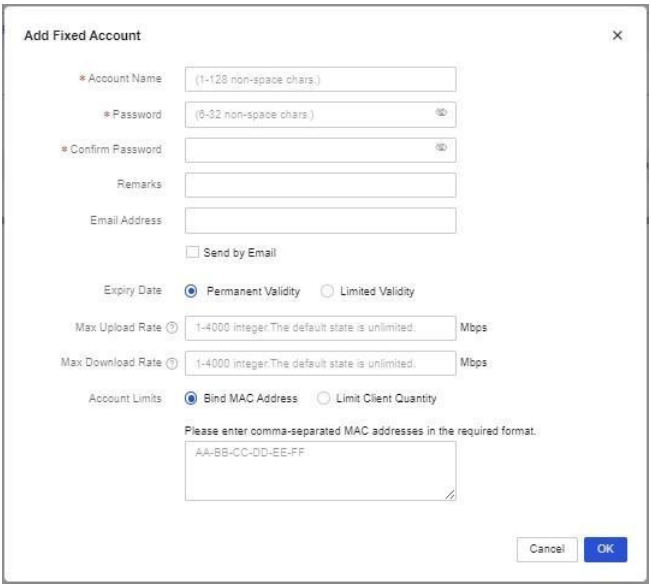
Se você não configurar o período de validade ou configurá-lo como 0, a conta nunca expirará.

Se você selecionar *Bind MAC Address (Vincular endereço* **MAC***)* **e não inserir nenhum endereço MAC, os clientes que usam o endereço MAC fixo poderão ser excluídos.**
A conta não é limitada.

Se você selecionar Enviado por e-mail, o sistema enviará o nome da conta e a senha para o endereço de e-mail especificado. O número de endereços de e-mail não pode exceder 10 e deve ser separado por vírgulas.

Procedimento

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Settings (Configurações>ACs> Users (Usuários*) **no painel de navegação.**
3. **Clique na guia** *Fixed Accounts (Contas fixas*) **na guia Portal Users (Usuários do portal).**
4. **Clique em** *Adicionar.*
5. **Configure as informações da conta fixa conforme necessário.**

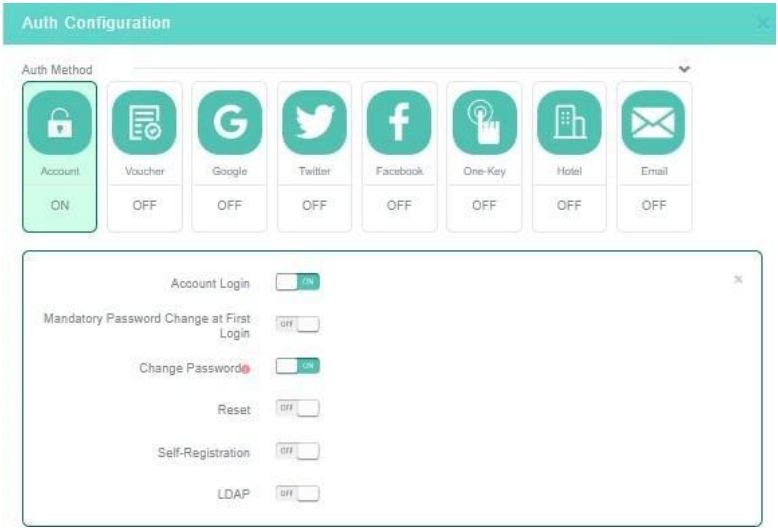


Adição de uma conta fixa

1. **Para adicionar ou editar um modelo de autenticação, selecione** *Configurações > ACs > Authentication* **no painel de navegação e, em seguida, selecione uma filial, um site e um dispositivo na parte superior da página. Para adicionar um modelo, clique em** *Add (Adicionar*) **na guia** *Authentication Templates (Modelos de autenticação*)**.**

   Para editar um modelo, clique no ícone *Edit (Editar*) **para esse modelo de autenticação.**
2. **Para vincular um modelo de autenticação a um serviço wireless, clique no ícone** *Edit (Editar*) **para esse modelo de autenticação, selecione** *Yes (Sim*) **no campo** *Bind to Wireless Service (Vincular ao serviço wireless)* **e clique em** *Apply (Aplicar).* **Se o modelo tiver sido vinculado ao serviço Wireless, pule esta etapa.**
3. **Clique no ícone** *Draw (Desenhar*) **para o modelo de autenticação de destino.**
4. **Clique na caixa** *Account (Conta*) **na área** *Auth Configuration (Configuração de autenticação*)**, ative a autenticação de conta fixa e defina outras configurações conforme necessário.**
5. **Desative outros métodos de autenticação.**

6. **Clique em** *OK* **ou em** *Liberar* **no canto superior direito da página.**

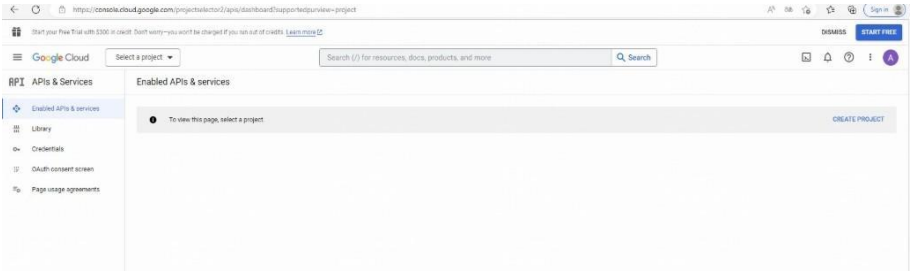


Configuração da autenticação de conta fixa

Configurar a autenticação do Google

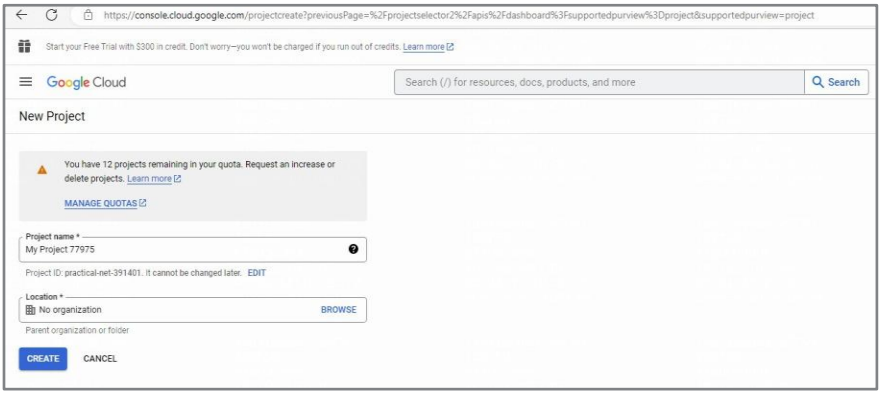
Criando um aplicativo do Google

1. **Faça login no Google Cloud Platform em** *https://console.cloud.google.com/apis*.
2. **Clique em** *CREATE PROJECT* **para criar um projeto.**



Criação de um projeto

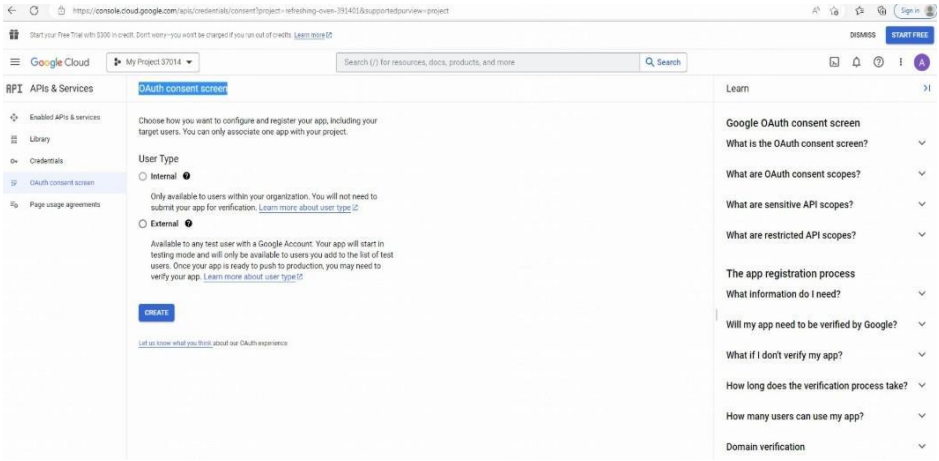
3. Defina as configurações básicas do projeto e clique em *Create (Criar).*



Configurações básicas do projeto

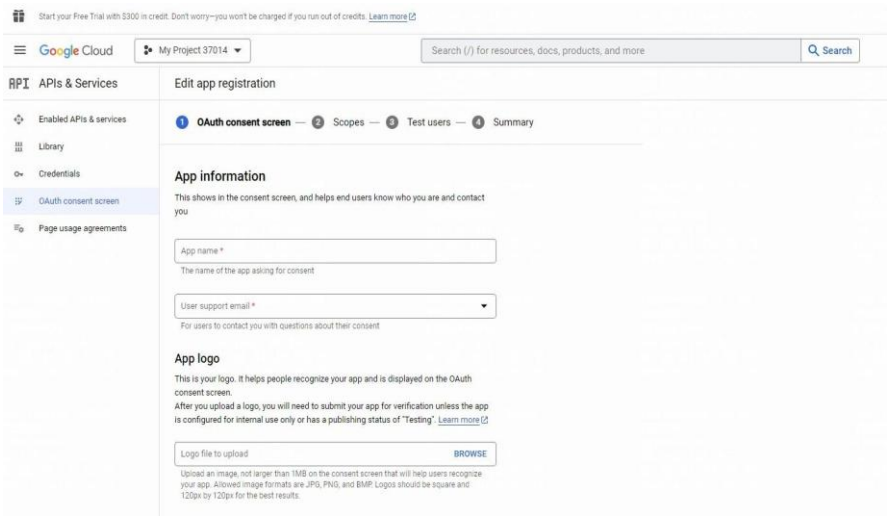
4. Defina as configurações da tela de consentimento do OAuth.

" Selecione *Externo* **como o tipo de usuário.**

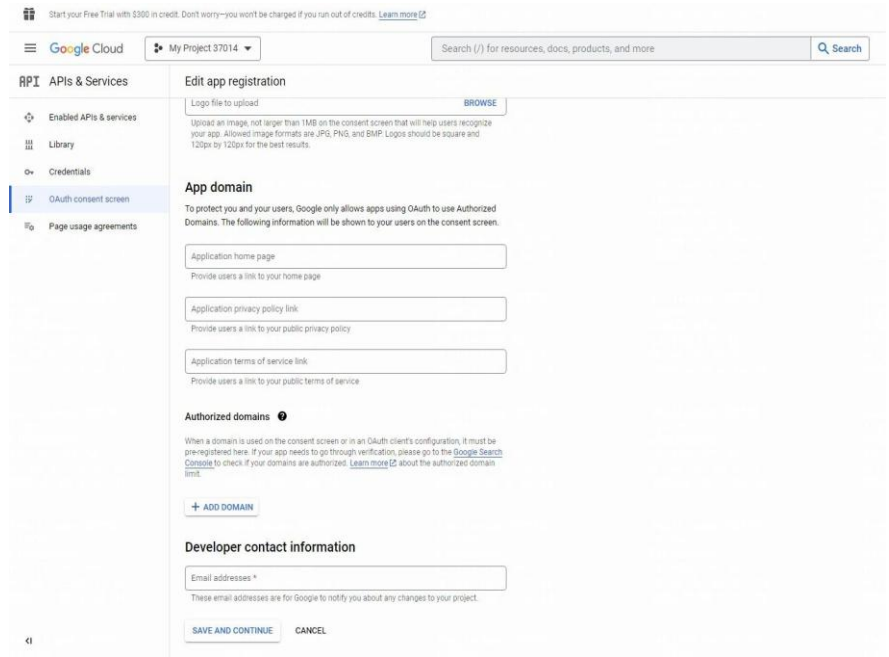


Seleção de um tipo de usuário

" Editar configurações de registro do aplicativo



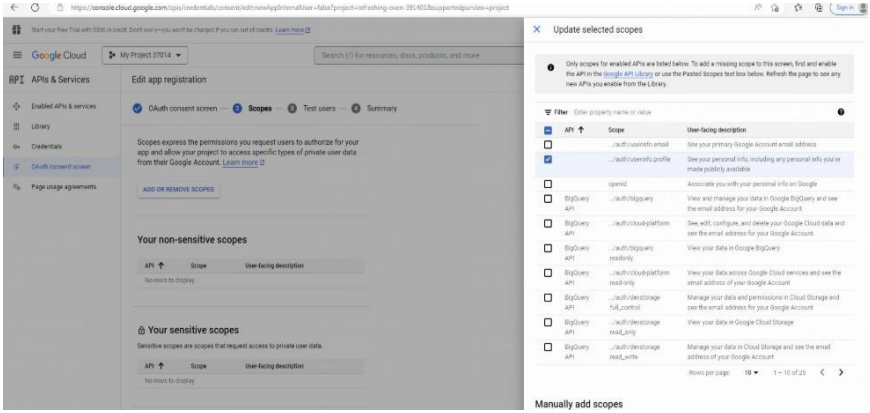
Edição das configurações de registro do aplicativo 1



Edição das configurações de registro do aplicativo 2

" **Configurar escopos.**

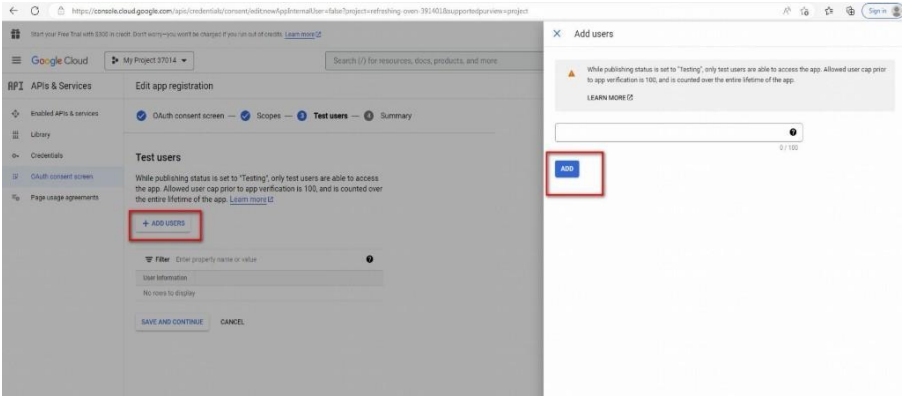
Você só precisa selecionar *userinfo.profile.*



Atualização de escopos

" **Configure os usuários de teste.**

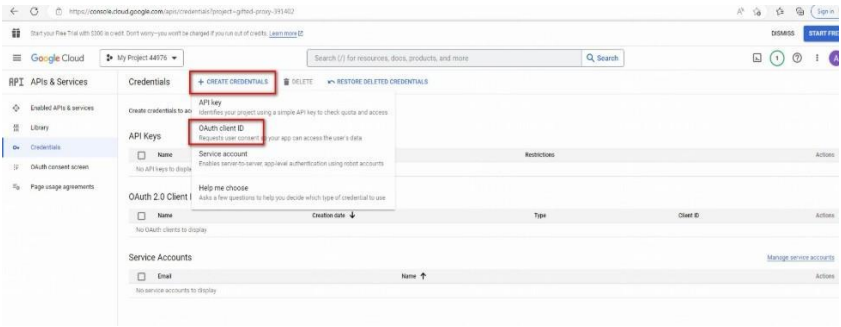
Clique em *Add Users* **(***Adicionar usuários***) para adicionar usuários de teste. Somente usuários de teste podem fazer login em um aplicativo do Google no estado Testing (Teste).**



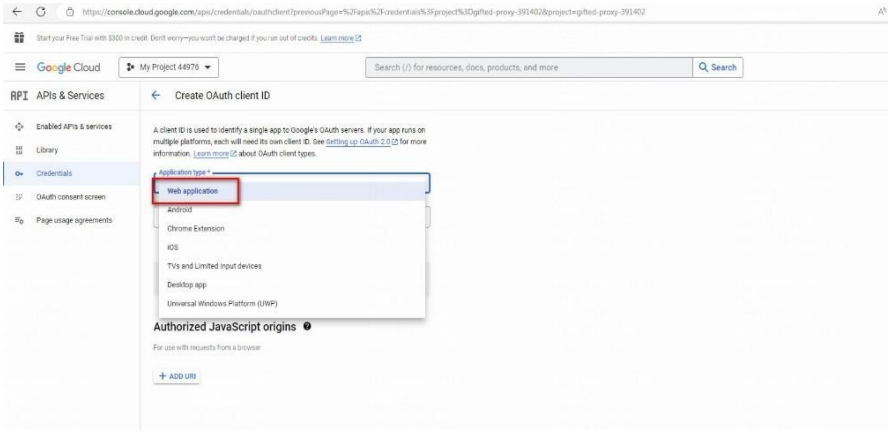
Adição de usuários de teste

" **Criar credenciais.**

" **Clique em** *CREATE CREDENTIALS* **e, em seguida, clique em** *OAuth client ID.*

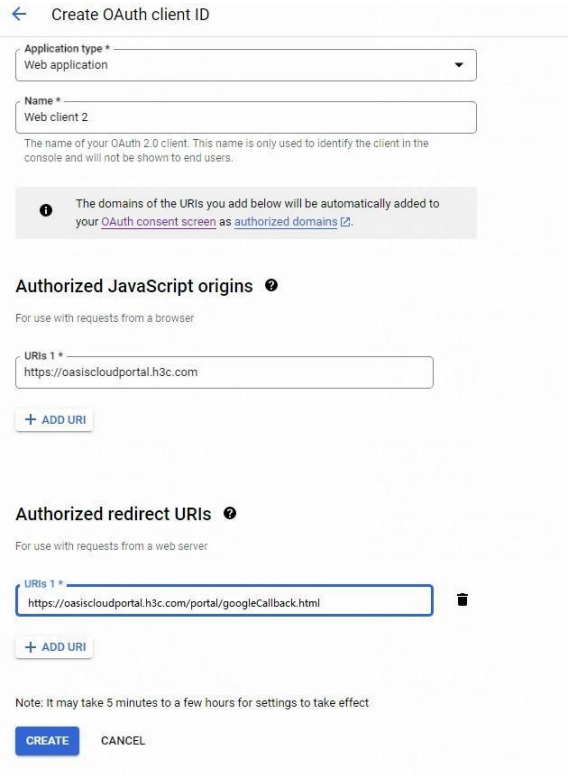


" **Selecione aplicativo da Web como o tipo de aplicativo.**



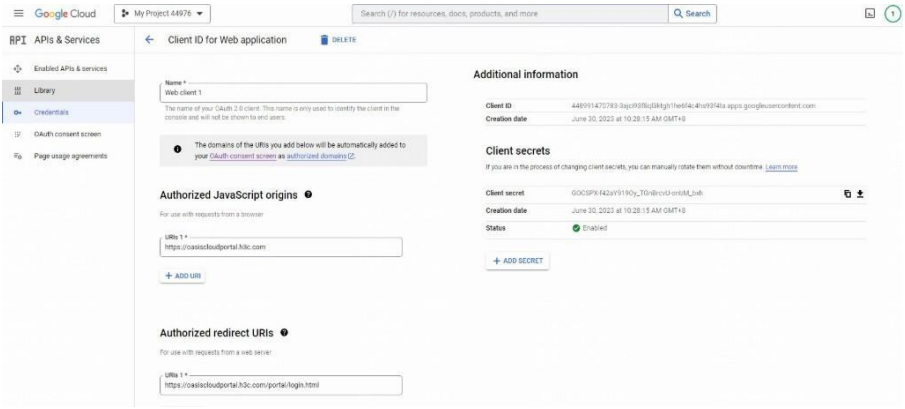
Seleção de um tipo de aplicativo

" **Adicione origens de JavaScript autorizadas e URIs de redirecionamento autorizados.**
O URI de redirecionamento autorizado é *https://oasiscloudportal.intelbras.com/portal/googleCallback.html.*
As origens JavaScript especificadas devem começar com *https.*



Origens de JavaScript autorizadas e URIs de redirecionamento autorizados

5. **Depois que a credencial for criada, clique em** *Credenciais* **no painel de navegação esquerdo. Na lista** *IDs de cliente OAuth 2.0*, **clique em** *Editar cliente OAuth* **na coluna** *Ações* **da credencial. Na página que se abre, você pode visualizar o ID e a chave secreta do cliente.**



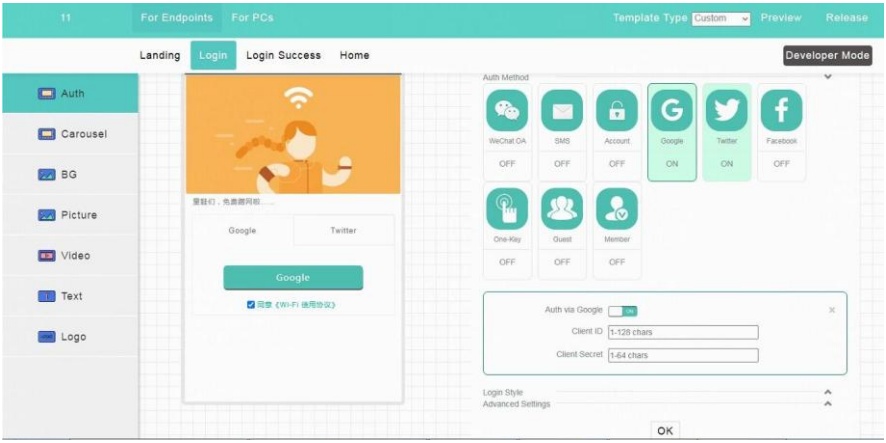
Informações sobre o cliente

Definir as configurações de autenticação do Google no INC Cloud

O método de autenticação do Google pode ser usado em conjunto com:

- **Autenticação por SMS.**
- **Autenticação de conta.**
- **Autenticação de membros.**
- **Autenticação do Facebook.**
- **Autenticação do Twitter.**

Você pode usar até três métodos de autenticação simultaneamente.



Autenticação do Google

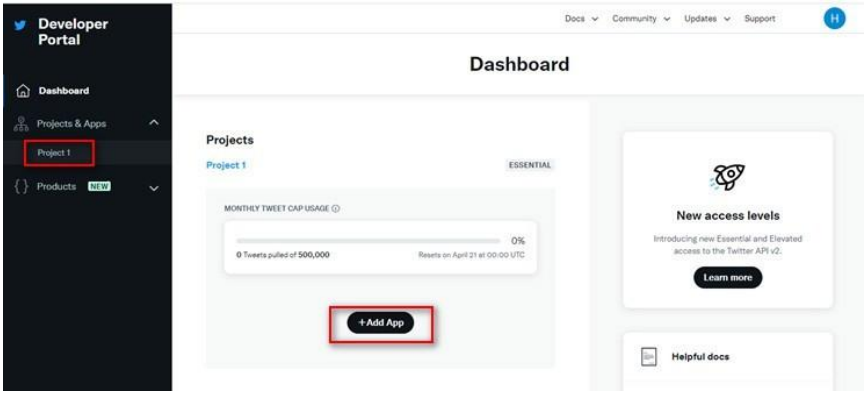
Configurar a autenticação do Twitter

Criando um aplicativo do Twitter

" **Entre na Plataforma de Desenvolvedores do Twitter em** *https://developer.twitter.com.*

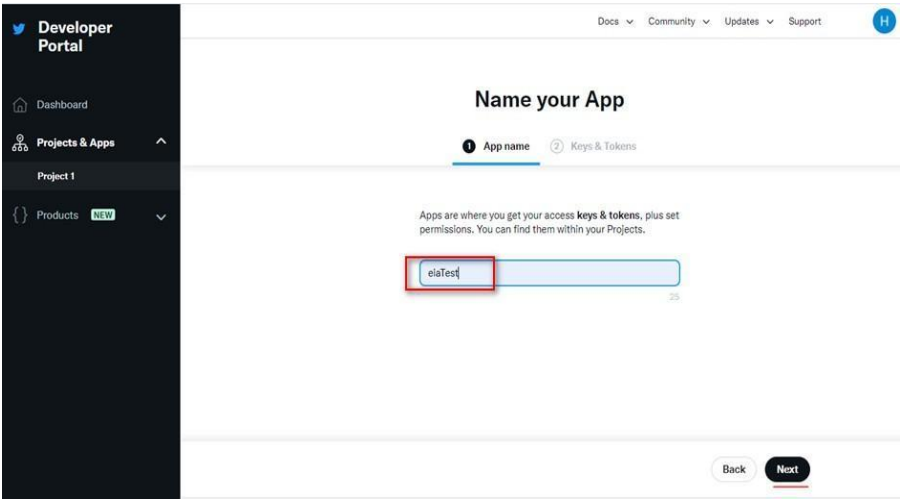
Página inicial

" **Registre-se para obter uma conta de desenvolvedor.**



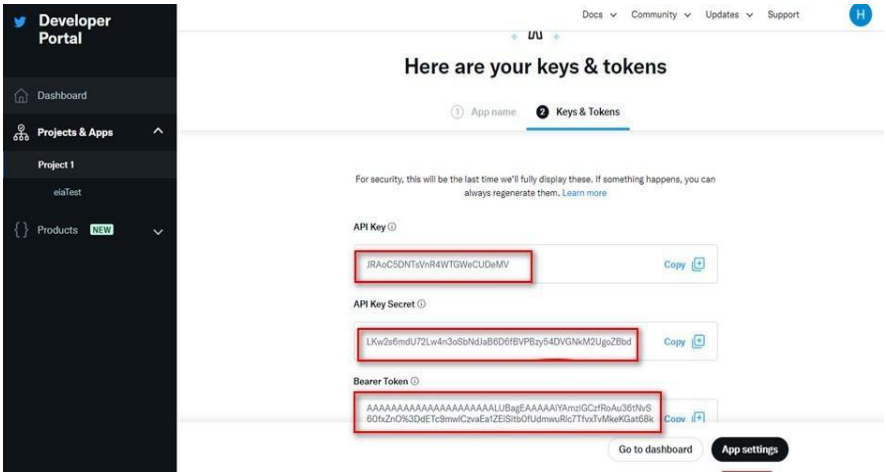
Página para registro de conta

" **Clique em Portal do desenvolvedor para criar um aplicativo em segundo plano.**



Nomeação de aplicativos

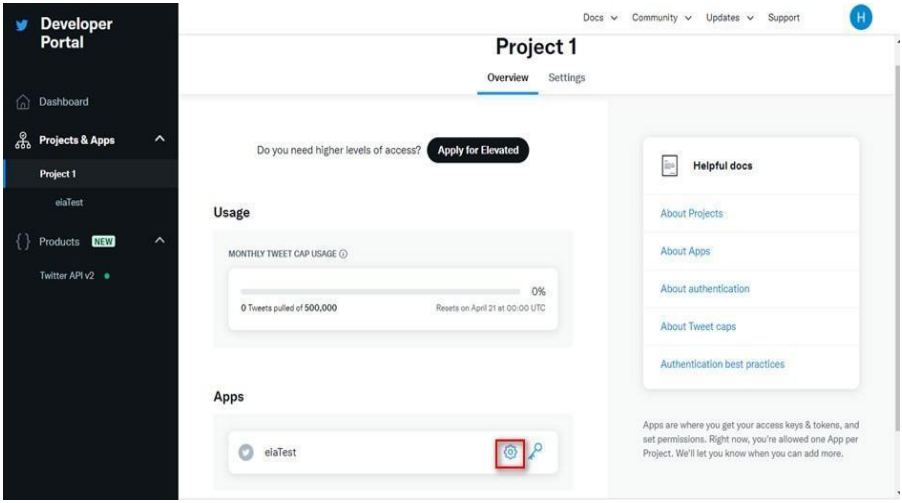
" **Registre a chave da API e o segredo da chave da API. Elas serão usadas posteriormente.**



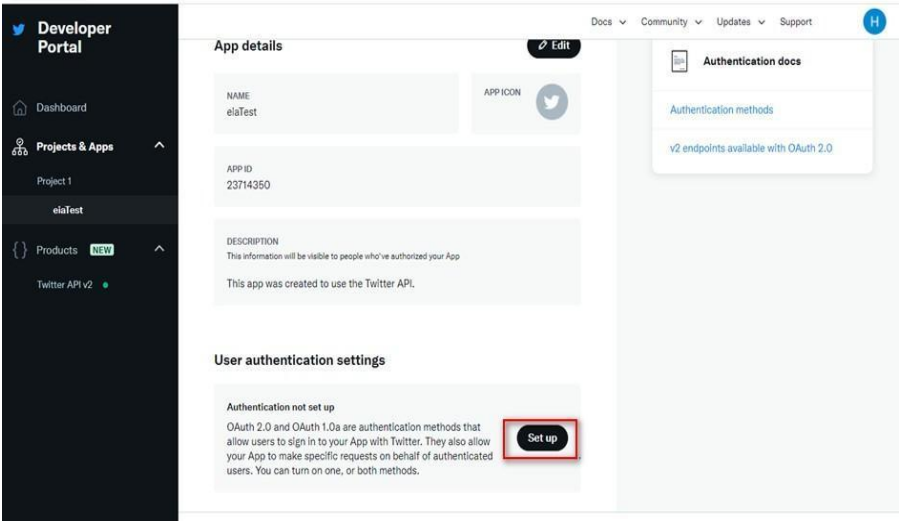
Senha

" **Configurar as definições do aplicativo.**

" **Clique no ícone** *Configurações* **na área** *Aplicativos*.

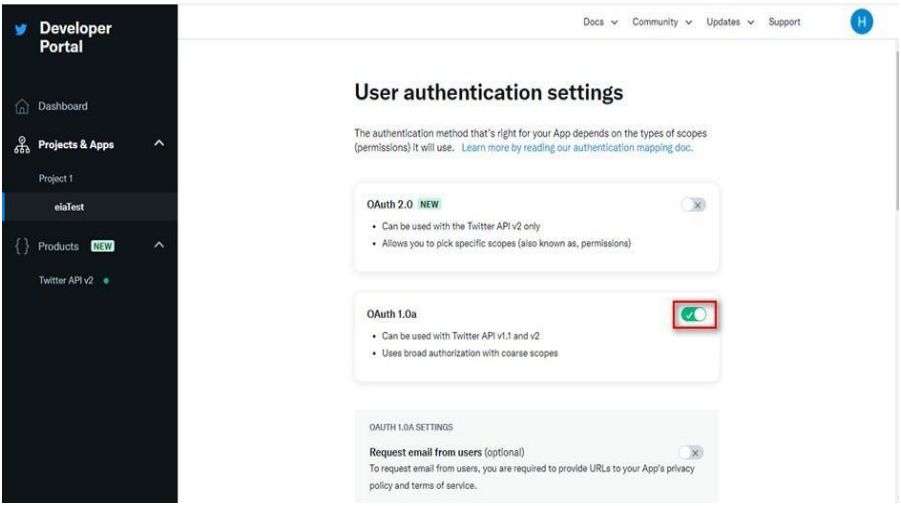


" **Clique no botão Set up (Configurar) na área User authentication settings (Configurações de autenticação do usuário).**



Configuração de autenticação do usuário

" **Ativar o Oauth 1.0a.**

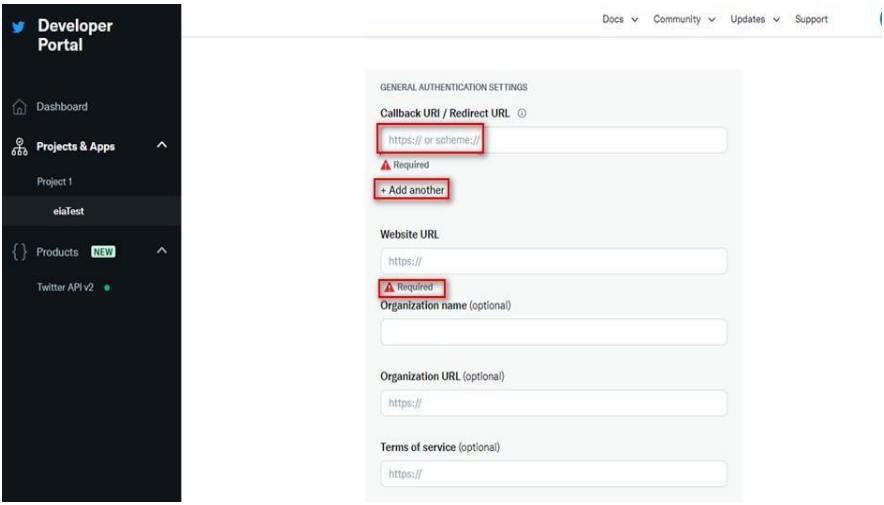


Ativação do Oauth 1.0a.

" **Especifique um URL de redirecionamento e um URL de site.**

" **URL de redirecionamento:** *https://oasiscloudportal/portal/twitterCallback.html.*

" **URL do site: insira um URL no formato de nome de domínio.**



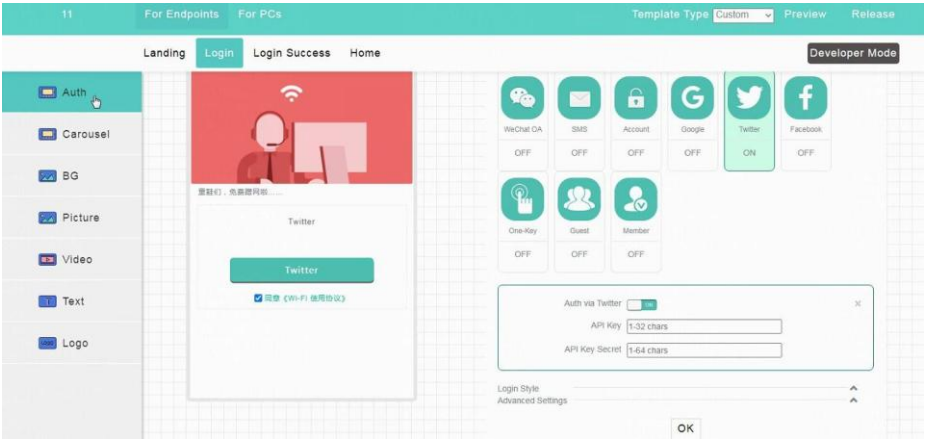
URL de redirecionamento e URL do site

Configurar as definições de autenticação do Twitter no INC Cloud

O método de autenticação do Google pode ser usado em conjunto com:

- **" Autenticação por SMS.**
- **" Autenticação de conta.**
- **" Autenticação de membros.**
- **" Autenticação do Facebook.**
- **" Autenticação do Google.**

Você pode usar até três métodos de autenticação simultaneamente.



Autenticação do Twitter

Configurar a autenticação de convidados

Restrições e diretrizes

Após a configuração, um convidado só poderá acessar a rede depois que o aprovador escanear o código QR no cliente e autorizar o cliente. O código QR é válido por cinco minutos. Quando o código QR expirar, o convidado deverá atualizar o código QR.

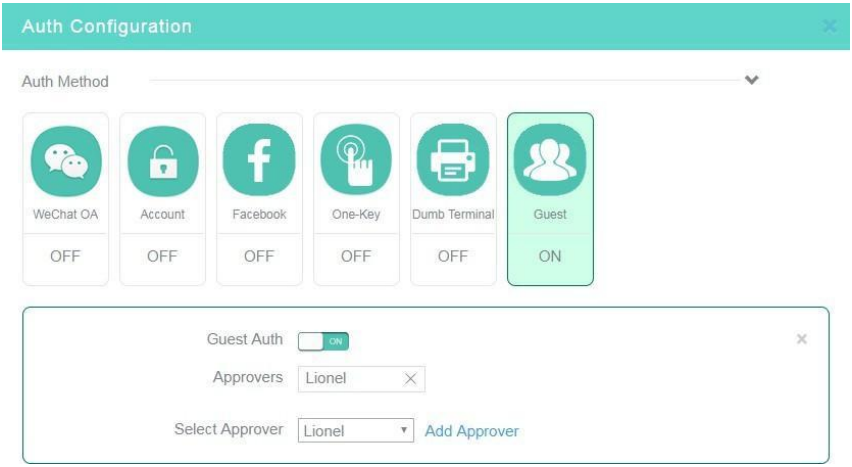
Procedimento

1. **Na barra de navegação superior, clique em** *Service (Serviço)*.
2. **Selecione** *Authentication (Autenticação)* **no painel de navegação e clique na guia** *Accounts (Contas)*.
3. **Clique na guia** *Contas de convidado* **e clique em** *Adicionar*.
   Um aprovador é adicionado depois que o aprovador escaneia o código QR e, em seguida, insere o código de verificação. Se o aprovador for excluído, o INC Cloud removerá automaticamente a permissão do aprovador.

Adição de um aprovador

4. **Selecione** *Settings (Configurações>ACs> Authentication (Autenticação)* **no painel de navegação e, em seguida, selecione uma filial, um site e um dispositivo na parte superior da página.**
5. **Para adicionar um modelo de autenticação, clique em** *Add (Adicionar)* **na guia** *Authentication Templates (Modelos de autenticação)*. **Para editar um modelo de autenticação, clique no ícone** *Edit (Editar)* **para esse modelo de autenticação.**

6. **Para vincular um modelo de autenticação a um serviço wireless, clique no ícone** *Edit (Editar)* **para esse modelo de autenticação, selecione** *Yes (Sim)* **no campo** *Bind to Wireless Service (Vincular ao serviço wireless)* **e clique em** *Apply (Aplicar)*. **Se o modelo tiver sido vinculado ao serviço Wireless, pule esta etapa.**
7. **Clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**
8. **Clique na caixa** *Convidado* **na área** *Configuração de Autenticação* **e ative a autenticação de convidado.**
9. **Selecione os aprovadores.**
   O campo *Aprovadores* **exibe apenas os aprovadores autorizados por essa conta e todas as suas subcontas. Para locatários, o campo** *Aprovadores* **exibe os aprovadores autorizados por todas as suas subcontas.**
10. **Desative outros métodos de autenticação.**
11. **Clique em** *OK* **ou em** *Liberar* **no canto superior direito da página.**



Configuração da autenticação de convidados

Configurar a autenticação do Facebook

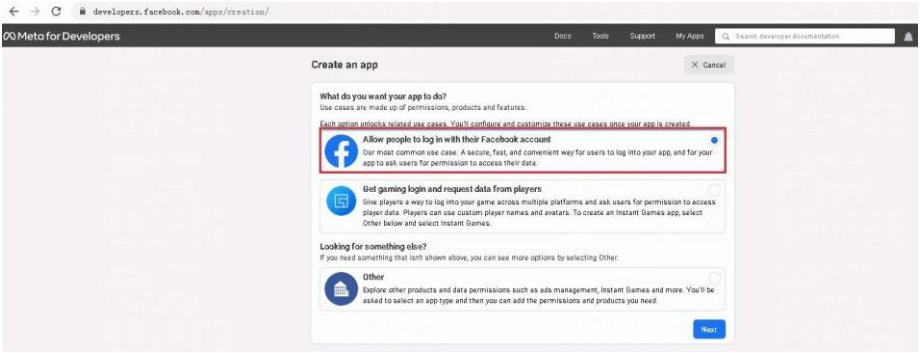
Com a autenticação do Facebook ativada, os usuários serão redirecionados para a página de login do Facebook para autenticação. Eles poderão acessar a rede somente depois de conceder ao INC Cloud a obtenção de suas informações do Facebook (apelido, perfil e informações de e-mail) do Facebook.

Criação de um aplicativo do Facebook

1. **Faça login no Meta for Developers em** *https://developers.facebook.com.*
2. **Clique em** *Criar aplicativo* **para criar um aplicativo do Facebook.**

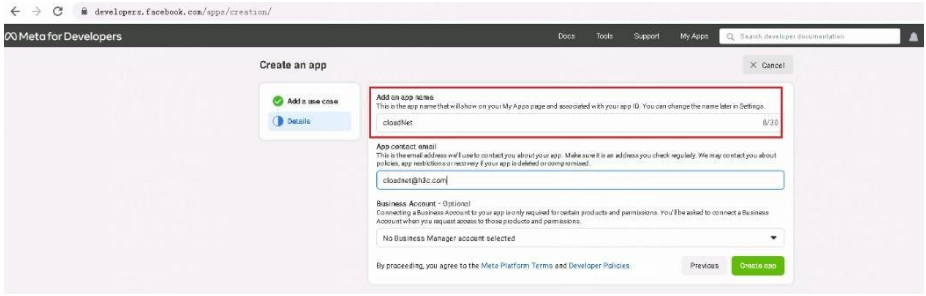
Criando um aplicativo

3. Selecione *Permitir que as pessoas façam login com suas contas do Facebook.*



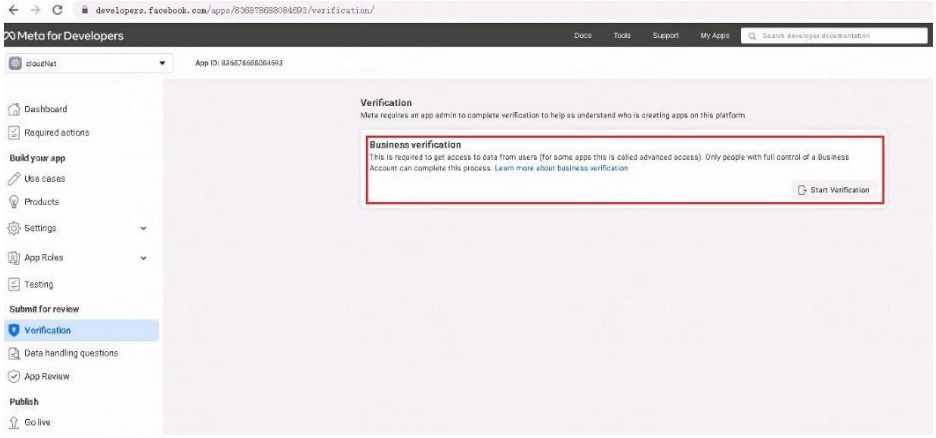
Seleção de um caso de uso

4. Especifique o nome do aplicativo.



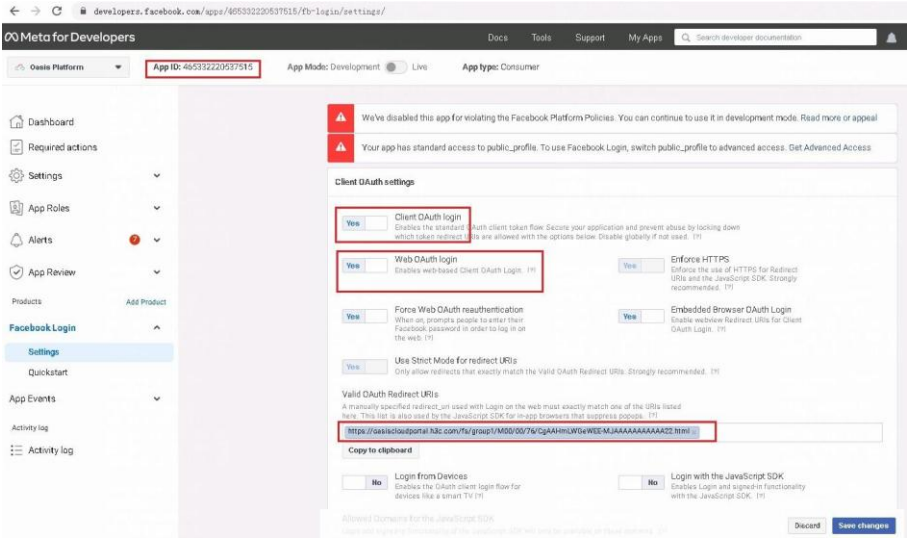
Especificando o nome do aplicativo

5. Iniciar a verificação de negócios.

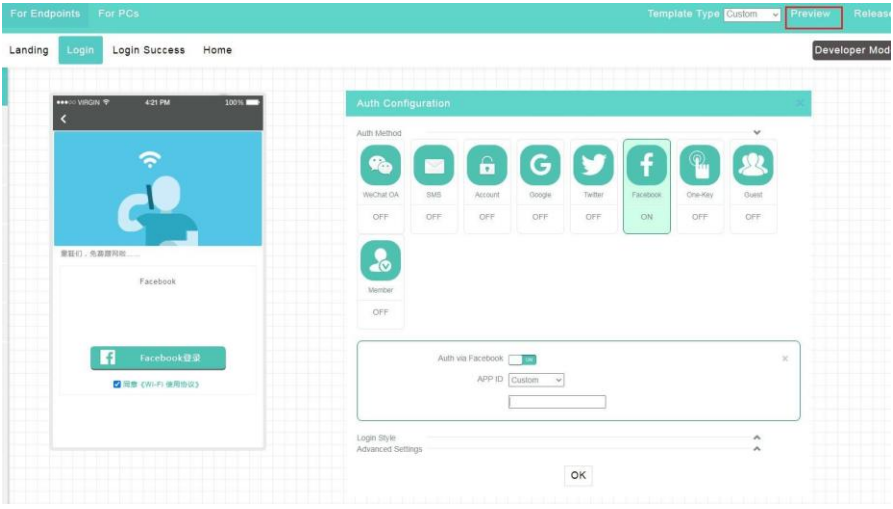


Verificação de negócios

6. **No Meta para Desenvolvedores, ative o login do cliente OAuth e o login do Web OAuth e insira o URI da página de login de autenticação como um URI de redirecionamento OAuth válido. Para obter o URI da página de login de autenticação, acesse a página** *Auth Configuration (Configuração de autenticação*) **do INC Cloud e clique em** *Preview (Visualizar)*.



*Configura**ç**ões do OAuth*



*P**á**gina de configura**ç**ão de autentica**ç**ão*

Página de login de autenticação

Definição das configurações de autenticação do Facebook no INC Cloud

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Settings (Configurações >ACs > Authentication (Autenticação*) **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Para adicionar um modelo de autenticação, clique em** *Add (Adicionar*) **na guia Authentication Templates (Modelos de autenticação).**
5. **Para editar um modelo de autenticação, clique no ícone** *Edit (Editar*) **para esse modelo de autenticação.**
6. **Para vincular um modelo de autenticação a um serviço sem fio, clique no ícone** *Edit (Editar*) **do modelo de autenticação, selecione** *Yes (Sim*) **no campo** *Bind to Wireless Service (Vincular ao serviço sem fio*) **e clique em** *Apply (Aplicar).* **Se o modelo tiver sido vinculado a um serviço Wireless, pule esta etapa.**
7. **Clique no ícone** *Draw (Desenhar*) **para o modelo de autenticação de destino.**
8. **Clique na caixa** *Facebook* **na área** *Configuração de Autenticação*, **ative a autenticação via Facebook, digite o código App ID e desative todos os outros métodos de autenticação.**
9. **Clique em** *OK* **ou em** *Liberar* **no canto superior direito da página.**

Configuração da autenticação do Facebook

Configurar a autenticação combinada

Restrições e diretrizes

Somente os seguintes métodos de autenticação podem ser usados em conjunto:

- **Autenticação de conta fixa.**
- **Autenticação do Facebook.**

Um usuário pode acessar a rede desde que seja aprovado em uma autenticação.

Procedimento

1. *Configure as Configure as definições no dispositivo* **definições no dispositivo conforme descrito em se o dispositivo**
   a versão do software é inferior a 5405.
2. **Configure no mínimo dois métodos de autenticação (Detalhes não mostrados).**

Configurar a autenticação do terminal burro

Restrições e diretrizes

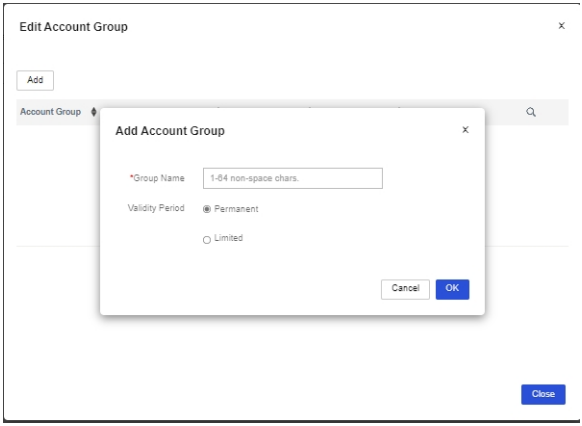
Se um grupo de contas contiver contas que tenham sido autenticadas, a alteração do período de validade do grupo de contas alterará o período de validade de todas as contas do grupo.

Se você configurar o período de validade como 0, a conta nunca expirará.

Você pode inserir os três primeiros bytes para adicionar endereços MAC em massa. A configuração do período de validade de um endereço MAC completo e a de um endereço MAC de três bytes não são mutuamente exclusivas. Suponha que você adicione endereços MAC que comecem com AA-BB-CC e especifique um período de validade de 5 dias e, em seguida, adicione o endereço MAC *AA-BB-CC-11-22-33* **e especifique um período de validade de 10 dias. Os períodos de validade dos terminais burros com um endereço MAC de** *AA-BB-CC-11-22-33* **e um endereço MAC que começa com** *AA-BB-CC* **são de 10 e 5 dias, respectivamente.**

Procedimento

1. **Na barra de navegação superior, clique em** *Service (Serviço).*
2. **Selecione** *Authentication (Autenticação*) **no painel de navegação e clique na guia** *Accounts (Contas*).
3. **Na guia** *Contas de terminal burro*, **clique em** *Editar grupo de contas.*
4. **Clique em** *Adicionar.*
5. **Digite as informações necessárias e clique em** *OK.*

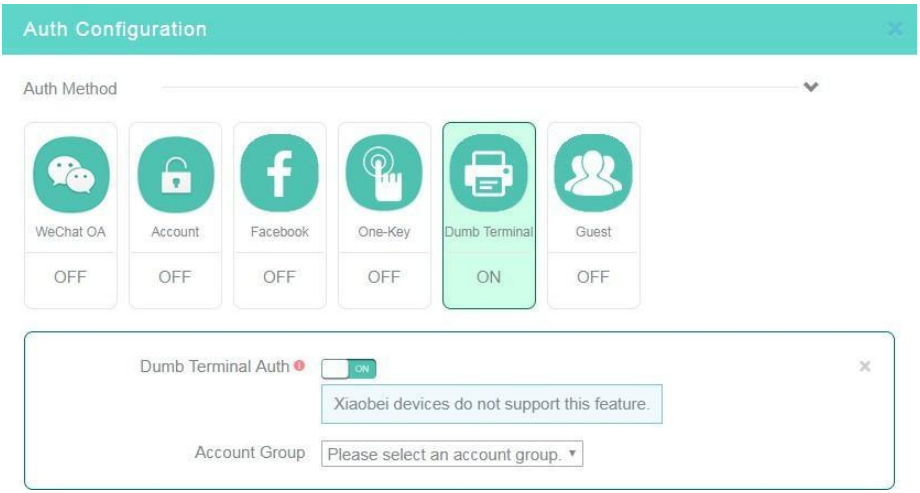


Adição de um grupo de contas

6. **Selecione um grupo de contas e clique em** *Add (Adicionar)*.
7. **Digite um endereço MAC no formato necessário.**

Adição de um endereço MAC

8. **Clique na guia** *Authentication Templates (Modelos de autenticação)*.
9. **Para adicionar um modelo de autenticação, clique em** *Add (Adicionar)*. **Para editar um modelo de autenticação, clique no ícone** *Edit (Editar* **para esse modelo de autenticação.**
10. **Clique no ícone** *de desenho* **para o modelo de autenticação de destino. Você será colocado na guia** *Login*.
11. **Clique na caixa** *Terminal burro* **na área** *Auth Configuration* **e, em seguida, ative a autenticação de terminal burro.**
12. **Selecione um grupo de contas.**
13. **Clique em** *OK* **ou em** *Liberar* **no canto superior direito da página.**



Configuração da autenticação do terminal burro

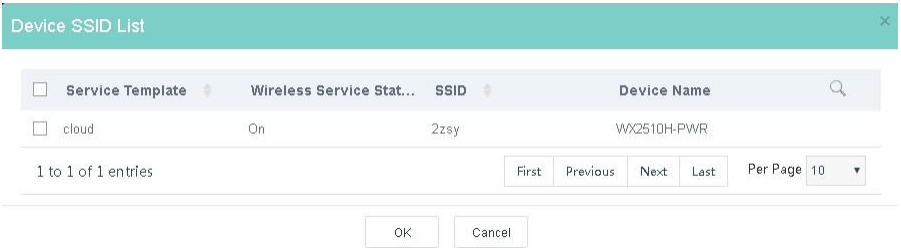
14. **Para implementar um modelo, execute as etapas a seguir:**

- **Clique no ícone** *Implantar Modelo* **para esse modelo de autenticação.**
- **Clique na guia** *ACs*.
- **Selecione uma filial ou local.**
- **Selecione um CA e clique em** *Aplicar.*

  Se nenhum dispositivo for exibido, verifique a versão do dispositivo.

Implementação de um modelo

- **Selecione um modelo de serviço ou um SSID e clique em** *OK.*



Seleção de um modelo de serviço

15. **Ative a autenticação acionada por MAC no dispositivo. Para obter mais informações, consulte** *Configurar autenticação acionada por MAC no dispositivo.*
    -ativar a autenticação.

Configurar a autenticação em massa

Execute esta tarefa para implementar configurações de autenticação em massa.

Restrições e diretrizes

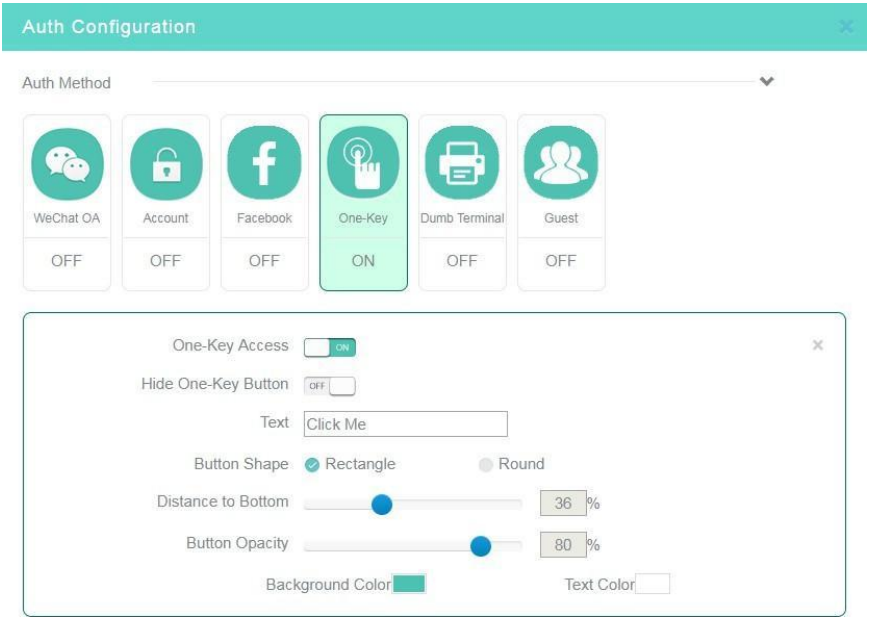
A configuração de um modelo de autenticação em massa tem precedência sobre a de um modelo de autenticação que não seja em massa. Para que o modelo de autenticação não em massa tenha efeito, clique no ícone *Editar* **para esse modelo de autenticação e, em seguida, clique em** *Aplicar.*

Antes de implementar a configuração em massa, certifique-se de que os seguintes requisitos sejam :

- **Os dispositivos em que a autenticação em massa é implantada estão on-line. Se um dispositivo estiver off-line, a implementação falhará. O dispositivo carregará as configurações implantadas mais recentes na .**
- **A versão do software deve ser 5405 ou superior.**
- **O nome do serviço sem fio é o mesmo do servidor da Web do portal.**

Procedimento

1. **Na barra de navegação superior, clique em** *Service (Serviço)*.
2. **Selecione** *Authentication (Autenticação)* **no painel de navegação.**
3. **Na guia** *Authentication Templates (Modelos de autenticação)***, clique em** *Add (Adicionar)*.
4. **Clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino. Para obter o processo de configuração detalhado, clique em**
   procedimentos de diferentes métodos de autenticação, consulte *Definir configurações básicas*.



Configuração da autenticação em massa

5. **Para implementar um modelo, execute as etapas a seguir:**

   " **Clique no ícone** *Implantar Modelo* **para esse modelo de autenticação.**
   " **Clique na guia** *ACs*.
   " **Selecione uma filial ou local.**
   " **Selecione um CA e clique em** *Aplicar*.
   Se nenhum dispositivo for exibido, verifique a versão do dispositivo.

Implementação de um modelo

Personalizar uma página de autenticação

Você pode configurar a página de destino, a página de login, a página de sucesso do login e a página inicial, e pode enviar
ou desative a página de destino ou a página de login bem-sucedido, conforme necessário.

Restrições e diretrizes

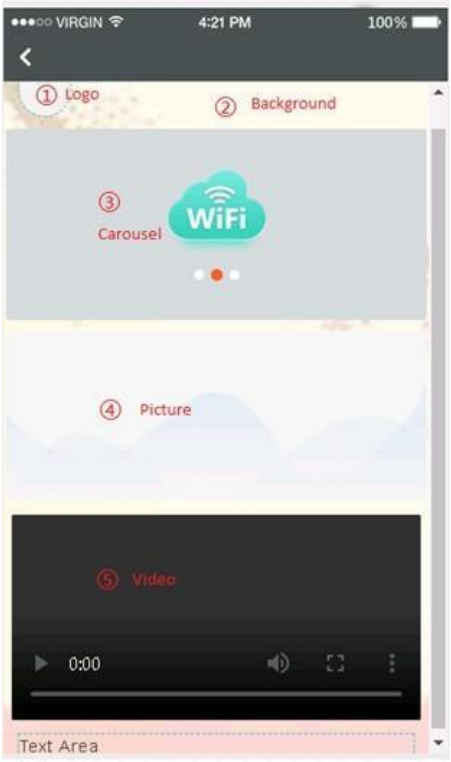
O tamanho da imagem não pode exceder 1 M. Como prática recomendada, defina o tamanho da imagem entre

100 KB e 200 KB. Somente os formatos JPG, JPEG, BMP, PNG, GIF e SVG são permitidos.

Como prática recomendada para não afetar a velocidade de carregamento da página, não adicione muitos controles.

Procedimento

1. **Na barra de navegação superior, clique em** *Service (Serviço).*
2. **Selecione** *Authentication (Autenticação)* **no painel de navegação.**
3. **Na guia** *Authentication Templates (Modelos de autenticação)***, clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**
4. **Defina as seguintes configurações, conforme mostrado na** *Figura Visualização da alteração da configuração:*
   - **Logotipo: a relação de aspecto deve ser 1:1. A imagem será automaticamente cortada em um círculo. Você pode inserir um nome de loja com comprimento inferior a 12 caracteres.**
   - **Plano de fundo: a proporção deve ser de 3:5.**
   - **Carrossel: a proporção deve ser de 11:5. São necessárias duas ou três imagens com a mesma altura.**
   - **Imagem: a relação de aspecto deve ser 11:5. A descrição da imagem não pode exceder 48 caracteres.**
   - **Vídeo: o tamanho do vídeo não pode exceder 5 M. Somente os formatos MP4, WEBM e OGG são permitidos.**
   - **Texto: você pode editar a fonte, o tamanho da fonte, o negrito e a cor da fonte.**

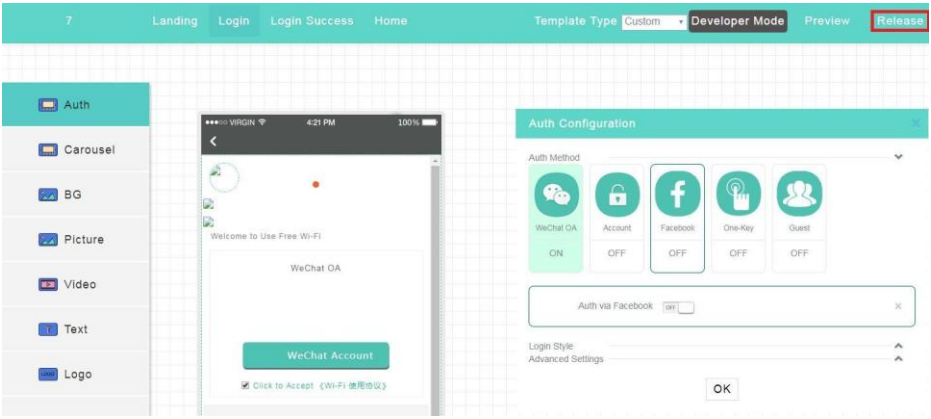


Descrição do modelo personalizado

5. **Para configurar a página inicial, clique na guia Home e selecione** *Usar link personalizado*.
6. **Digite um link personalizado e clique em Upload.**
7. **Para visualizar o link, clique em** *Preview (Visualizar)* **no canto superior direito da página.**

Pré-visualização da alteração da configuração

8. **Clique em** *Liberar* **no canto superior direito da página.**
   A página inicial enviada aos usuários durante a autenticação do portal será substituída pela página redirecionada por esse link personalizado.



Configuração do modelo personalizado

2.2. Configurar definições avançadas

O INC Cloud fornece configurações avançadas de autenticação para simplificar o gerenciamento de autenticação, reduzir custos e otimizar a promoção no mercado. *A tabela Recursos avançados de autenticação do INC Cloud* **descreve os recursos avançados disponíveis para cada método de autenticação. Você pode definir essas configurações conforme necessário.**

Recursos avançados de autenticação do INC Cloud:

Métodos de autenticação:

Método de autenticação	Cenário aplicável	Observações	Combinado autenticação
Uma tecla	Baixos requisitos de auditoria e coleta de estatísticas operacionais, restaurantes e lojas.	Autenticação baseada em MAC. Os usuários podem concluir a autenticação simplesmente clicando em um botão na página de autenticação do portal.	Com suporte
Conta fixa	Os usuários da rede são fixos, como áreas de campus e escritórios.	Autenticação baseada em nome de usuário e senha. As seguintes funções são : LDAP Importação e exportação de contas Vinculação de uma conta a vários endereços MAC Limite de clientes simultâneos	Com suporte
Autenticação do Google	As operadoras usam o Google para coletar estatísticas sobre os usuários da rede.	Os usuários devem fazer login no Google para conceder acesso ao INC Cloud. Esse método está disponível somente em https://oasiscloud.intelbras.com.	Com suporte
Autenticação do Twitter	As operadoras usam o Twitter para coletar estatísticas sobre os usuários da rede.	Os usuários devem fazer login no Twitter para conceder acesso ao INC Cloud. Esse método está disponível somente em https://oasiscloud.intelbras.com.	Com suporte
Autenticação de convidados	Empresas ou lojas em que é necessário o acesso temporário de convidados.	Um convidado pode acessar a rede depois que um aprovador escaneia o código QR no terminal do convidado e autoriza o terminal.	Não suportado
Autenticação de terminal burro	Dispositivos IoT, impressoras sem fio e terminais POS.	Autenticação automatizada em terminais sem fio.	Não suportado
Autenticação do Facebook	As operadoras usam o Facebook para coletar estatísticas sobre os usuários da rede.	Os usuários devem fazer login no Facebook para conceder acesso ao INC Cloud. Esse método está disponível somente em https://oasiscloud.intelbras.com.	Com suporte

Método de autenticação e compatibilidade de rede

	Compatibilidade com redes com diferentes autenticadores		
Método de autenticação	CA	Roteador Wireless	Roteador com fio
Autenticação de uma chave	Sim	Sim	Sim
Autenticação de conta fixa	Sim	Sim	Sim
Autenticação de convidados	Sim	Sim	Sim
Autenticação do Facebook	Sim	Não	Não
Autenticação combinada	Sim	Sim	Sim
Autenticação de terminal burro	Sim	Sim	Não
Autenticação em massa	Sim	Sim	Não
Página de autenticação personalizada	Sim	Sim	Sim

Ativar o recurso captive-bypass

Normalmente, o dispositivo envia a página de autenticação para um cliente automaticamente quando o cliente tenta acessar uma rede de autenticação de portal. O recurso captive-bypass permite que o dispositivo envie a página de autenticação do portal para o cliente somente quando o usuário iniciar um navegador.

Para ativar o recurso captive-bypass, você deve executar as seguintes etapas no dispositivo:

1. **Entre na visualização do sistema.**
   visão do sistema
2. **Entre na visualização do servidor da Web do portal da Cloud do servidor da Web.**
   Portal web-server Cloud
3. **Habilite o recurso captive-pass.**
   Ativação do captive-bypass

Ocultar ou personalizar o botão de autenticação de uma chave

Execute esta tarefa para ocultar o botão de autenticação de uma chave ou alterar o estilo do botão. Se o botão estiver oculto, os usuários passarão pela autenticação automaticamente após a expiração do cronômetro de contagem regressiva na página de login.

Restrições e diretrizes

Você pode alterar o estilo do botão somente quando o botão não estiver oculto.

Procedimento

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações >ACs > Authentication (Autenticação*) **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique no ícone** *Draw (Desenhar*) **para o modelo de autenticação de destino.**
5. **Clique na caixa** *One-Key* **na área** *Configurações de Autenticação* **e, em seguida, oculte ou personalize o botão conforme necessário.**

Gerenciar contas fixas

Execute esta tarefa para excluir, importar ou exportar contas fixas em

massa. Para gerenciar contas fixas:

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações >ACs > Users (Usuários*) **no painel de navegação.**
3. **Clique na guia** *Fixed Accounts (Contas fixas*)**.**
4. **Para excluir contas fixas, selecione as contas fixas de destino e clique em** *Excluir.*
5. **Para importar contas fixas, clique em** *Importar,* **faça o download do arquivo de modelo e preencha o arquivo conforme necessário e, em seguida, carregue o arquivo de modelo.**
6. **Para exportar contas fixas, clique em** *Exportar.*

Ativar a alteração de senha por autoatendimento

Esse recurso permite que os usuários alterem as senhas no login. Com esse recurso desativado, somente os administradores podem alterar as senhas de contas fixas.

Para ativar a alteração de senha por autoatendimento:

1. **Na barra de navegação superior, clique em** *Network.*
2. **Selecione** *Configurações (Configurações>ACs> Authentication (Autenticação*) **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique no ícone** *Draw (Desenhar*) **para o modelo de autenticação de destino.**
5. **Clique na caixa** *Account (Conta)* **na área** *Auth Configuration (Configuração de autenticação*)**.**
6. **Ativar** *alterar senha.*

Permitir a colaboração com um servidor LDAP para verificação de conta fixa

Execute esta tarefa para permitir que o INC Cloud informe nomes de usuário e senhas ao servidor LDAP para verificação quando os usuários tentarem acessar a WLAN usando contas fixas. Isso libera os administradores de rede da importação de informações de conta do servidor LDAP para o INC Cloud.

Restrições e diretrizes

Para usar esse recurso, certifique-se de que o servidor LDAP tenha sido configurado.

Procedimento

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações >ACs > Authentication (Autenticação*) **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique no ícone** *Draw (Desenhar*) **para o modelo de autenticação de destino.**
5. **Clique na caixa** *Account (Conta)* **na área** *Auth Configuration (Configuração de autenticação*)**.**
6. **Habilite** *o LDAP* **e defina as configurações do LDAP conforme necessário.**
7. **Clique em** *LDAP Config Verification (Verificação de configuração* **LDAP) para verificar as configurações LDAP.**

Alterar as configurações de efeito visual da página de login

Execute esta tarefa para personalizar a cor do plano de fundo, a opacidade do plano de fundo e a cor do texto no login
página.

Restrições e diretrizes

Cuidado:

A restauração das configurações padrão removerá todas as configurações de efeitos visuais definidas pelo usuário e a operação de restauração é
irreversível. Use esse recurso com cautela.

As configurações de efeito visual dos métodos de autenticação só têm efeito quando vários métodos de autenticação são usados.
estão ativados.

Procedimento

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações >ACs > Authentication (Autenticação*) **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique no ícone** *Draw (Desenhar*) **para o modelo de autenticação de destino.**
5. **Clique para expandir o menu** *Login Style (Estilo de login)* **na área** *Auth Configuration (Configuração de autenticação*)**.**
6. **Configure a cor do plano de fundo, a opacidade do plano de fundo e a cor do texto, conforme necessário.**
7. **O ajuste será exibido na área de visualização em tempo real. Para restaurar as configurações padrão do efeito visual, clique em** *Restore Default (Restaurar padrão).*

Configurar as definições de acesso à Internet

Procedimento

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações >ACs > Authentication (Autenticação*) **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique no ícone** *Draw (Desenhar*) **para o modelo de autenticação de destino.**
5. **Clique para expandir o menu** *Advanced Settings (Configurações avançadas)* **na área** *Auth Configuration (Configuração de autenticação*)**.**
6. **Defina as configurações de acesso à Internet conforme necessário.**

Parâmetros

- **Tempo limite da sessão: duração máxima contínua on-line de um cliente após uma autenticação. Um cliente será desconectado quando sua duração contínua on-line exceder o tempo limite. O tempo limite da sessão não pode ser maior do que a duração on-line diária.**
- **Duração diária on-line: duração máxima on-line de um cliente em um dia. Um cliente será desconectado quando sua duração on-line por um dia exceder o limite. A duração on-line diária não pode ser menor que o tempo limite da sessão.**
- **Tráfego mínimo e temporizador de inatividade: faz o logoff de um cliente se o tráfego dentro de um temporizador de inatividade não atingir o limite mínimo de tráfego. A configuração do temporizador de inatividade como 0 desativa o recurso de temporizador de inatividade.**

Observação:

Como prática recomendada, defina o timer ocioso para um valor não maior que a metade da concessão do endereço IP dos clientes, permitindo entradas de clientes off-line a serem excluídos a tempo.

- **Client Rate Limit: taxa limitada de tráfego de clientes de uplink e downlink. Esse recurso é compatível com versões superiores a 5417P01.**
- **HTTPS para Landing e Login: use sessões HTTPS para a página Landing e Login.**
- **Permitir PC: Permitir que os PCs acessem a WLAN. A autenticação do Facebook não é compatível com esse recurso.**

Gerenciar grupos de contas de terminais burros

Execute esta tarefa para criar, Excluir ou editar grupos de contas de terminal burro e importar ou exportar grupos de contas de terminal burro.
contas terminais.

Se você ativar a autenticação de terminal burro e especificar um grupo de contas, somente os terminais burros em
o grupo pode acessar a WLAN.

Para gerenciar grupos de contas de terminais burros:

1. **Na barra de navegação superior, clique em** *Service (Serviço).*
2. **Selecione** *Authentication (Autenticação)* **no painel de navegação Clique na guia** *Accounts (Contas)***.**
3. **Na guia** *Dumb Terminal Accounts (Contas de terminal burro)***, configure os grupos de contas de terminal burro.**

Configurar a autenticação automatizada do portal

Esse recurso permite que os usuários que foram autenticados acessem a rede sem nova autenticação dentro do período livre de autenticação. Os seguintes modos estão disponíveis:

- **Redirecionamento de portal: nesse modo, os usuários devem executar um navegador para acionar a autenticação automática do portal. Esse modo suporta o envio de anúncios para os clientes.**
- **MAC-trigger: nesse modo, os usuários podem acessar a WLAN sem executar um navegador. Esse modo não não suporta o envio de anúncios para os clientes.**

Configurar a autenticação de redirecionamento do portal

1. **Na barra de navegação superior, clique em** *Network*
2. **Selecione** *Configurações (Configurações >ACs > Authentication (Autenticação)* **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**
5. **Clique para expandir o menu** *Advanced Settings (Configurações avançadas)* **na área** *Auth Configuration (Configuração de autenticação)***.**
6. **Clique na guia** *Livre de Autenticação* **e configure o recurso** *Autenticação Gratuita***.**

Configurar a autenticação de acionamento de MAC

1. **Configurar a autenticação de redirecionamento do portal. Para obter mais informações, consulte** *Configurar o redirecionamento do portal autenticação.*
2. **Configure a autenticação de acionamento de MAC no dispositivo:**

   " **Configure o servidor de vinculação de MAC.**

Observação:

Execute essa etapa somente nas versões anteriores à 5405. A versão 5405 e posteriores suportam a implementação automática da configuração de autenticação nos dispositivos e não precisam da configuração manual dos comandos nesta etapa.

 # Crie um servidor de vinculação de MAC e entre em sua exibição.

<Sysname> visão do sistema

[portal mac-trigger-server cloud

 # Habilite a autenticação de acionamento de MAC da Cloud. Defina o número máximo de tentativas de consulta de vinculação de MAC como 2 e o intervalo de consulta como 3 segundos.

[Sysname-portal-mac-trigger-server-cloud] cloud-binding enable

[Sysname- portal-mac-trigger-server-cloud] binding-retry 2 interval 3

[Sysname-portal- mac-trigger-server-cloud] quit

" **Aplique a nuvem do servidor de vinculação MAC à nuvem do modelo de serviço. [Sysname] wlan service-template Cloud**

[Sysname-wlan-st-cloud] portal apply mac-trigger-server cloud

Configurar a reautenticação entre sites e entre SSIDs

Esse recurso permite que os clientes que foram autenticados façam roaming entre serviços Wireless associados a diferentes sites ou diferentes SSIDs para o mesmo site sem reautenticação. Esses serviços sem fio devem usar o mesmo modelo de autenticação ou ter o mesmo SSID.

Restrições e diretrizes

Esse recurso está disponível somente para modelos de autenticação configurados no App Center.

Procedimento

1. **Na barra de navegação superior, clique em** *Service (Serviço).*
2. **Selecione** *Authentication (Autenticação*) **no painel de navegação.**
3. **Clique no ícone** *Draw (Desenhar*) **para o modelo de autenticação de destino.**
4. **Clique para expandir o menu** *Advanced Settings (Configurações avançadas)* **na área** *Auth Configuration (Configuração de autenticação*)**.**
5. **Clique na guia** *Livre de Autenticação* **e ative** *a Autenticação gratuita.*
6. **Configure a reautenticação entre sites e entre SSIDs.**

Configurar o controle de acesso à Internet

Execute esta tarefa para especificar os intervalos de tempo durante os quais os usuários têm permissão para acessar a WLAN.

Restrições e diretrizes

O controle de acesso à Internet é feito hora. É possível especificar um máximo de cinco intervalos de tempo para um dia. Para especificar um intervalo de tempo que termine às 24 horas, defina o horário de término como 00. Se você definir um intervalo de tempo de 00 a 00 para um dia, os usuários poderão acessar a Internet a qualquer momento nesse dia.

Procedimento

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações >ACs > Authentication (Autenticação*) **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique no ícone** *Draw (Desenhar*) **para o modelo de autenticação de destino.**
5. **Clique para expandir o menu** *Advanced Settings (Configurações avançadas)* **na área** *Auth Configuration (Configuração de autenticação*)**.**
6. **Clique na guia** *Internet Access Control (Controle de acesso à Internet*) **e especifique os intervalos de tempo.**

Configurar o modo de desenvolvedor

Cuidado:

A edição dos códigos das funções existentes pode desativar a autenticação do INC Cloud. Use esse recurso com cuidado.

O modo de desenvolvedor permite que os usuários modifiquem os códigos -fonte de um modelo de autenticação para
para fins de personalização.

Procedimento

1. Na barra de navegação superior, clique em *Rede*.
2. Selecione *Configurações (Configurações >ACs > Authentication (Autenticação)* no painel de navegação.
3. Selecione uma filial, um site e um dispositivo na parte superior da página.
4. Clique no ícone *Draw (Desenhar)* para o modelo de autenticação de destino.
5. Clique em *Developer Mode (Modo de desenvolvedor)*

no canto superior direito. **Configurar a lista branca e a**

lista negra de nomes de domínio *Restrições e*

diretrizes

Esse recurso entra em vigor somente quando a autenticação sem fio está configurada.

Procedimento

1. Na barra de navegação superior, clique em *Rede*.
2. Selecione *Configurações (Configurações>ACs> Authentication (Autenticação)* no painel de navegação.
3. Clique na guia *Domain Name Whitelist (Lista branca de nomes de domínio) ou Domain Name Blacklist (Lista negra de nomes de domínio)* para configurar a lista branca ou a lista negra.

Exibir ou exportar o histórico da implantação do modelo de autenticação

Execute esta tarefa para visualizar o histórico de todas as implantações de modelos de autenticação ou implantações no
dia atual, últimos 7 dias ou últimos 30 dias.

Para exibir ou exportar o histórico da implementação do modelo de autenticação:

1. Na barra de navegação superior, clique em *Service (Serviço)*.
2. Selecione *Authentication (Autenticação)* no painel de navegação.
3. Na guia *Authentication Templates (Modelos de autenticação)*, clique no ícone *Apply (Aplicar)* para o modelo de autenticação de destino.
4. Clique na guia *ACs* para visualizar o histórico de implementação de um AC.

3. Configurar a autenticação do INC Cloud com um roteador Wireless como autenticador

Importante:

O captive portal interno da plataforma ainda não oferece suporte ao protocolo IPv6, sendo compatível apenas com o padrão IPv4. Dessa forma, para a operação correta da funcionalidade, é indicado configurar a LAN de autenticação captive para operar apenas com o padrão IPv4.

3.1. Configurar as definições básicas

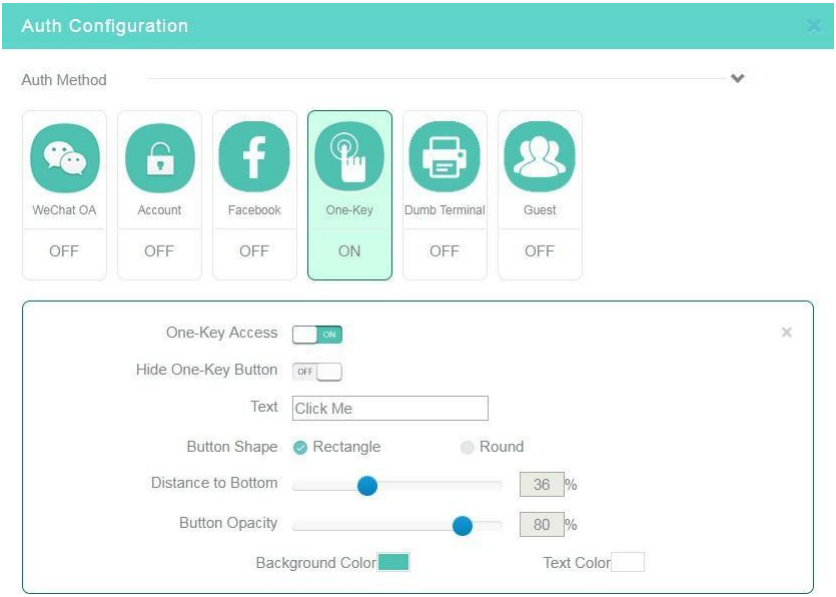
Pré-requisitos

Antes de configurar a autenticação do INC Cloud, conclua as seguintes tarefas:

- **Conecte o dispositivo ao INC Cloud.**
  Para obter mais informações, consulte o *Guia de implantação do Intelbras INC Cloud*.
- **Conclua as configurações de VLAN e DHCP.**
- **Configure os serviços Wireless e certifique-se de que os APs possam ficar on-line.**

Configurar a autenticação de uma chave

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações >Routers (Roteadores >Authentication (Autenticação)* **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Para adicionar um modelo de autenticação, clique em** *Add* **(***Adicionar***) na guia** *Wireless* **Authentication Templates (Modelos de autenticação** *Wireless***).**
5. **Para editar um modelo de autenticação, clique no ícone** *Edit (Editar)* **para esse modelo de autenticação.**
6. **Para vincular um modelo de autenticação a um serviço wireless, clique no ícone** *Edit (Editar)* **para esse modelo de autenticação, selecione** *Yes (Sim)* **no campo** *Bind to Wireless Service (Vincular ao serviço wireless)* **e clique em** *Apply (Aplicar).* **Se o modelo tiver sido vinculado ao serviço Wireless, pule esta etapa.**
7. **Clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**
8. **Clique na caixa** *One-Key* **na área** *Configurações de Autenticação***, ative a autenticação de uma chave e confirme a autenticação de uma chave.**
   Defina outras configurações conforme necessário.
9. **Clique em** *OK* **ou em** *Liberar* **no canto superior direito da página.**



Configuração da autenticação de uma chave

Configurar a autenticação de conta fixa

Restrições e diretrizes

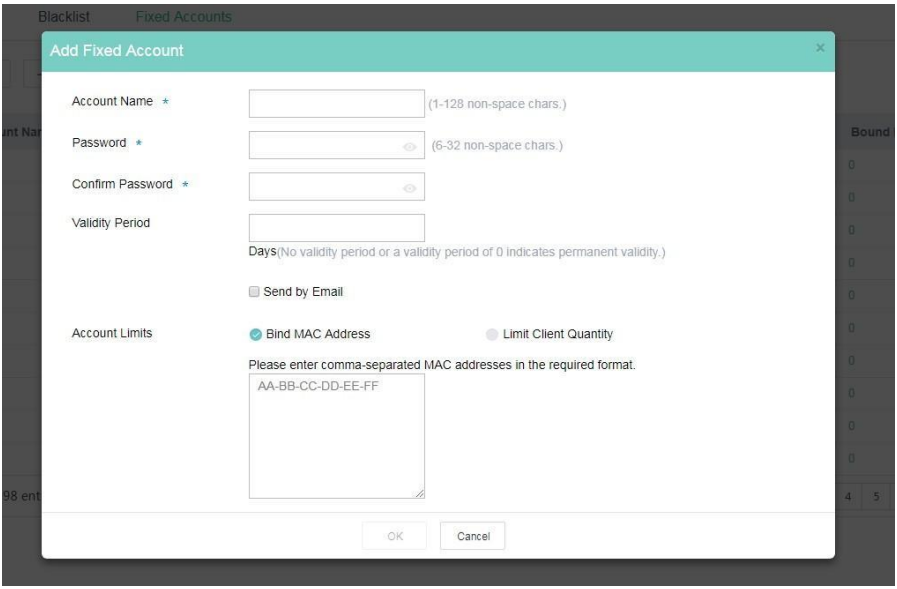
Se você não configurar o período de validade ou configurá-lo como 0, a conta nunca expirará.

Se você selecionar *Bind MAC Address (Vincular endereço* **MAC***)* **e não inserir nenhum endereço MAC, os clientes que usam o endereço MAC fixo poderão ser excluídos.**
A conta não é limitada.

Se você selecionar *Enviado por e-mail,* **o sistema enviará o nome da conta e a senha para o endereço de e- mail especificado. O número de endereços de e-mail não pode exceder 10 e deve ser separado por vírgulas.**

Procedimento

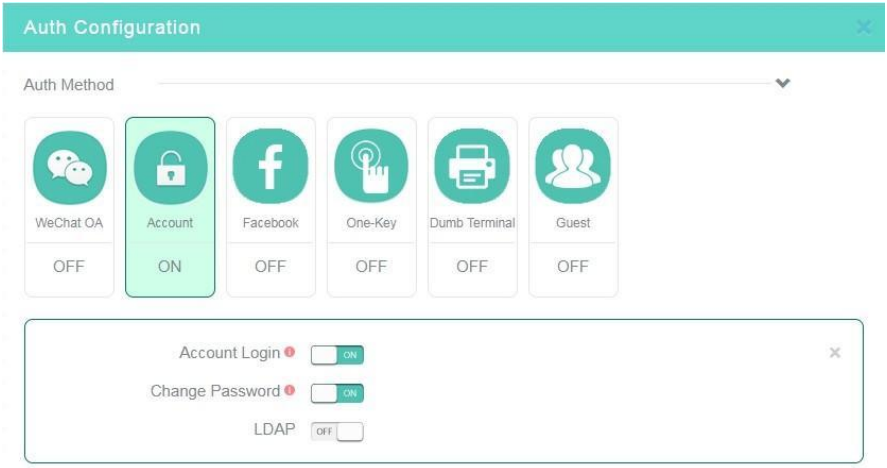
1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações>Routers (Roteadores>Users (Usuários*) **no painel de navegação.**
3. **Clique na guia** *Fixed Accounts (Contas fixas*)**.**
4. **Clique em** *Adicionar.*
5. **Configure as informações da conta fixa conforme necessário.**



Adição de uma conta fixa

6. **Para adicionar ou editar um modelo de autenticação, selecione** *Configurações (Configurações >Routers (Roteadores >Authentication (Autenticação* **sem fio) no painel de navegação e, em seguida, selecione uma filial, um site e um dispositivo na parte superior da página. Para adicionar um modelo, clique em** *Add (Adicionar*) **na guia** *Wireless Authentication Templates (Modelos de autenticação Wireless*)**. Para editar um modelo, clique no ícone** *Edit (Editar*) **para esse modelo de autenticação.**
7. **Para vincular um modelo de autenticação a um serviço wireless, clique no ícone** *Edit (Editar*) **para esse modelo de autenticação, selecione** *Yes (Sim*) **no campo** *Bind to Wireless Service (Vincular ao serviço wireless*) **e clique em** *Apply (Aplicar).* **Se o modelo tiver sido vinculado ao serviço Wireless, pule esta etapa.**
8. **Clique no ícone** *Draw (Desenhar*) **para o modelo de autenticação de destino.**
9. **Clique na caixa** *Account (Conta*) **na área** *Auth Configuration (Configuração de autenticação*)**, ative a autenticação de conta fixa e defina outras configurações conforme necessário.**
10. **Desative outros métodos de autenticação.**

11. **Clique em** *OK* **ou em** *Liberar* **no canto superior direito da página.**



Configuração da autenticação de conta fixa

Configurar a autenticação de convidados

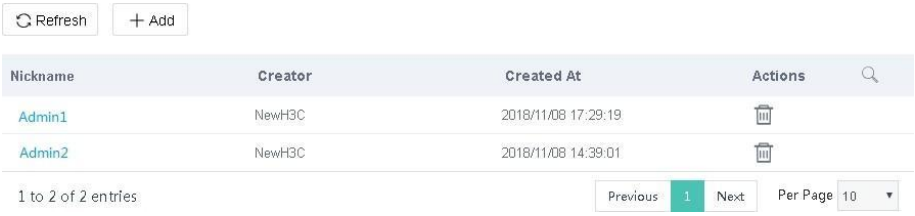
Restrições e diretrizes

Após a configuração, um convidado só poderá acessar a rede depois que o aprovador escanear o código QR no cliente e autorizar o cliente. O código QR é válido por cinco minutos. Quando o código QR expirar, o convidado deverá atualizar o código QR.

Procedimento

1. **Na barra de navegação superior, clique em** *Service (Serviço)*.
2. **Selecione** *Authentication (Autenticação)* **no painel de navegação Clique na guia** *Accounts (Contas)*
3. **Clique na guia** *Contas de convidado* **e clique em** *Adicionar.*

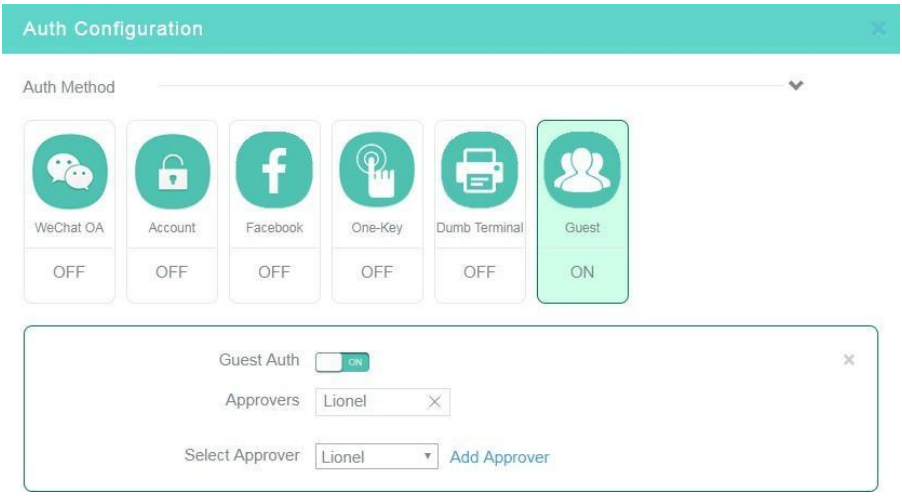
   Um aprovador é adicionado depois que o aprovador escaneia o código QR e, em seguida, insere o código de verificação. Se o aprovador for excluído, o INC Cloud removerá automaticamente a permissão do aprovador.



Adição de um aprovador

4. **Selecione** *Configurações (Configurações >Routers (Roteadores >Authentication (Autenticação)* **no painel de navegação e, em seguida, selecione uma filial, um site e um dispositivo na parte superior da página.**
5. **Para adicionar um modelo de autenticação, clique em** *Add (Adicionar)* **na guia** *Wireless Authentication Templates (Modelos de autenticação Wireless)*. **Para editar um modelo de autenticação, clique no ícone** *Edit (Editar)* **para esse modelo de autenticação.**
6. **Para vincular um modelo de autenticação a um serviço wireless, clique no ícone** *Edit (Editar)* **para esse modelo de autenticação, selecione** *Yes (Sim)* **no campo** *Bind to Wireless Service (Vincular ao serviço wireless)* **e clique em** *Apply (Aplicar)*. **Se o modelo já tiver sido vinculado ao serviço Wireless, pule esta etapa.**
7. **Clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**

8. **Clique na caixa *Convidado* na área *Configuração de Autenticação* e ative a autenticação de convidado.**
9. **Selecione os aprovadores.**
10. **O campo *Aprovadores* exibe apenas os aprovadores autorizados por essa conta e todas as suas subcontas. Para locatários, o campo *Aprovadores* exibe os aprovadores autorizados por todas as suas subcontas.**
11. **Desative outros métodos de autenticação.**
12. **Clique em *OK* ou em *Liberar* no canto superior direito da página.**



Configuração da autenticação de convidados

Configurar a autenticação combinada

Restrições e diretrizes

Somente os seguintes métodos de autenticação podem ser usados em conjunto:

- **Autenticação de conta fixa.**
- **Autenticação do Facebook.**

Um usuário pode acessar a rede desde que seja aprovado em uma autenticação.

Procedimento

Configure um mínimo de dois métodos de autenticação. (Detalhes não mostrados).

Configurar a autenticação do terminal burro

Restrições e diretrizes

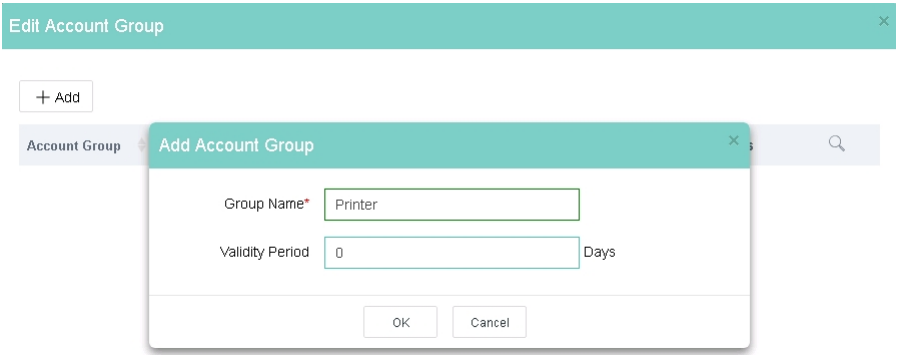
Se um grupo de contas contiver contas que tenham sido autenticadas, a alteração do período de validade do grupo de contas alterará o período de validade de todas as contas do grupo.

Se você configurar o período de validade como 0, a conta nunca expirará.

Você pode inserir os três primeiros bytes para adicionar endereços MAC em massa. A configuração do período de validade de um endereço MAC completo e a de um endereço MAC de três bytes não são mutuamente exclusivas. Suponha que você adicione endereços MAC que comecem *com AA-BB-CC* e especifique um período de validade de 5 dias e, em seguida, adicione o endereço MAC *AA-BB-CC-11-22-33* e especifique um período de validade de 10 dias. Os períodos de validade dos terminais burros com um endereço MAC de *AA-BB-CC-11-22-33* e um endereço MAC que começa com *AA-BB-CC* são de 10 e 5 dias, respectivamente.

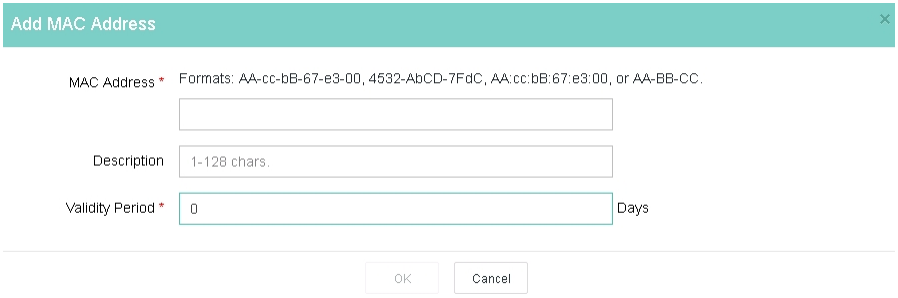
Procedimento

1. **Na barra de navegação superior, clique em** *Service (Serviço)*.
2. **Selecione** *Authentication (Autenticação)* **no painel de navegação e clique na guia** *Accounts (Contas)*
3. **Na guia** *Contas de terminal burro*, **clique em** *Editar grupo de contas*.
4. **Clique em** *Adicionar*.
5. **Digite as informações necessárias e clique em** *OK*.



Adição de um grupo de contas

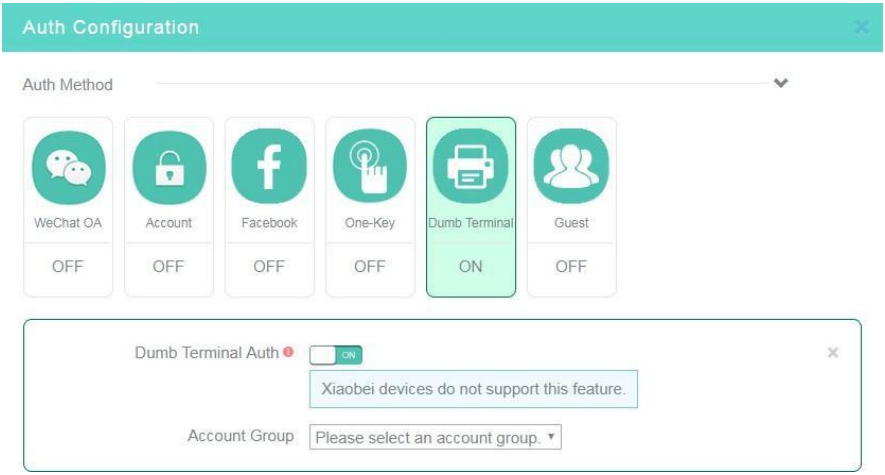
6. **Selecione um grupo de contas e clique em** *Add (Adicionar)*.
7. **Digite um endereço MAC no formato necessário.**



Adição de um endereço MAC

1. **Clique na guia** *Authentication Templates (Modelos de autenticação)*.
2. **Para adicionar um modelo de autenticação, clique em** *Add (Adicionar)*. **Para editar um modelo de autenticação, clique no ícone** *Edit (Editar* **para esse modelo de autenticação.**
3. **Clique no ícone** *de desenho* **para o modelo de autenticação de destino. Você será colocado na guia Login.**
4. **Clique na caixa** *Terminal burro* **na área** *Configuração de Autenticação* **e ative a autenticação do terminal burro.**
5. **Selecione um grupo de contas.**

6. Clique em *OK* ou em *Liberar* no canto superior direito da página.

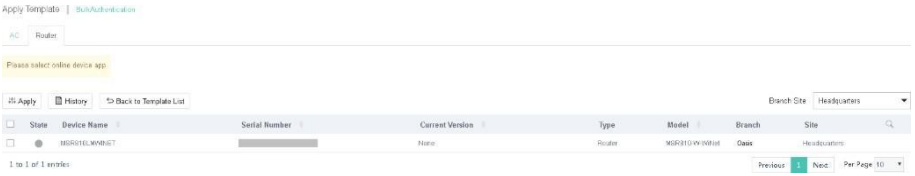


Configuração da autenticação do terminal burro

7. Para implementar um modelo, execute as etapas a seguir:

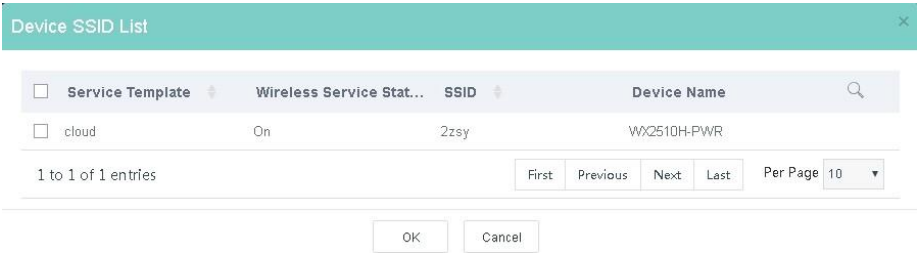
- **Clique no ícone *Deploy Template* para esse modelo de autenticação.**
- **Clique na guia *Roteador*.**
- **Selecione uma filial ou local.**
- **Selecione um dispositivo e clique em *Apply (Aplicar)*.**

  Se nenhum dispositivo for exibido, verifique a versão do dispositivo.



Implementação de um modelo

- **Selecione um modelo de serviço ou um SSID e clique em *OK*.**



Seleção de um modelo de serviço

8. Habilite a autenticação acionada por MAC no dispositivo. Para obter mais informações, consulte *Configurar autenticação acionada por MAC no dispositivo.*
-ativar a autenticação.

Configurar a autenticação em massa

Execute esta tarefa para implementar configurações de autenticação em massa.

Restrições e diretrizes

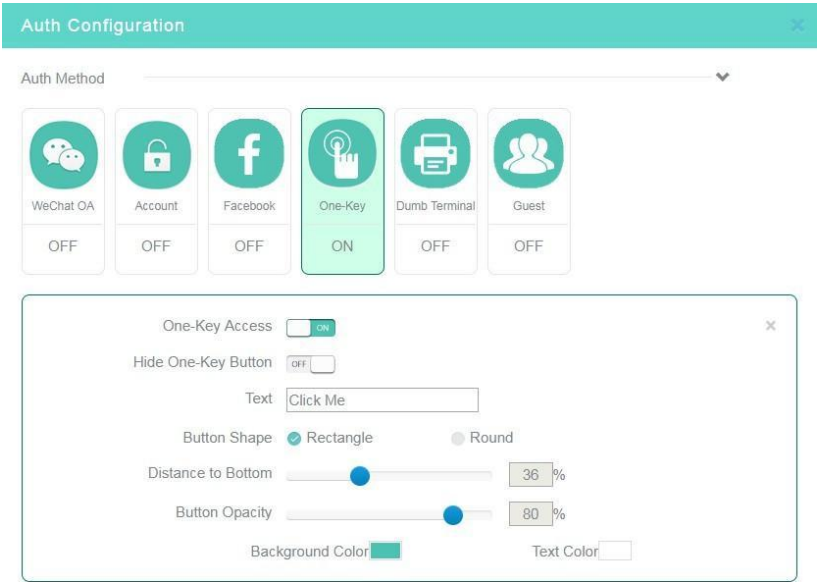
A configuração de um modelo de autenticação em massa tem precedência sobre a de um modelo de autenticação que não seja em massa. Para que o modelo de autenticação não em massa tenha efeito, clique no ícone *Editar* para esse modelo de autenticação e, em seguida, clique em *Aplicar*.

Antes de implementar a configuração em massa, certifique-se de que os seguintes requisitos sejam :

- **Os dispositivos em que a autenticação em massa é implantada estão on-line. Se um estiver off-line, a implementação falhará para ele. O dispositivo carregará as configurações implantadas mais recentes na .**
- **O nome do serviço sem fio é o mesmo do servidor da Web do portal.**

Procedimento

1. **Na barra de navegação superior, clique em *Service (Serviço)*.**
2. **Selecione *Authentication (Autenticação)* no painel de navegação,**
3. **Clique no ícone *Draw (Desenhar)* para o modelo de autenticação de destino. Para obter o processo de configuração detalhado, clique em procedimentos de diferentes métodos de autenticação, consulte *Definir configurações básicas*.**

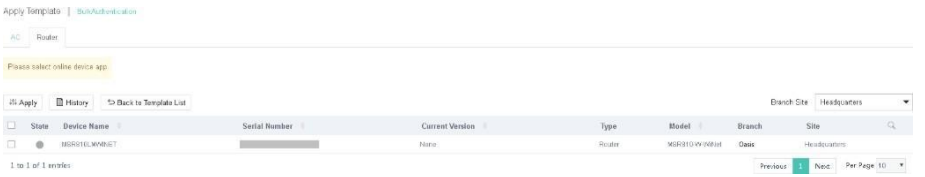


Configuração da autenticação em massa

4. **Para implementar um modelo, execute as etapas a seguir:**

   - **Clique no ícone *Deploy Template* para esse modelo de autenticação.**
   - **Clique na guia *Roteador*.**
   - **Selecione uma filial ou local.**
   - **Selecione um dispositivo e clique em *Apply (Aplicar)*.**

   Se nenhum dispositivo for exibido, verifique a versão do dispositivo.



Implementação de um modelo

Personalizar uma página de autenticação

Você pode configurar a página de destino, a página de login, a página de sucesso do login e a página inicial, e pode enviar
ou desative a página de destino ou a página de login bem-sucedido, conforme necessário.

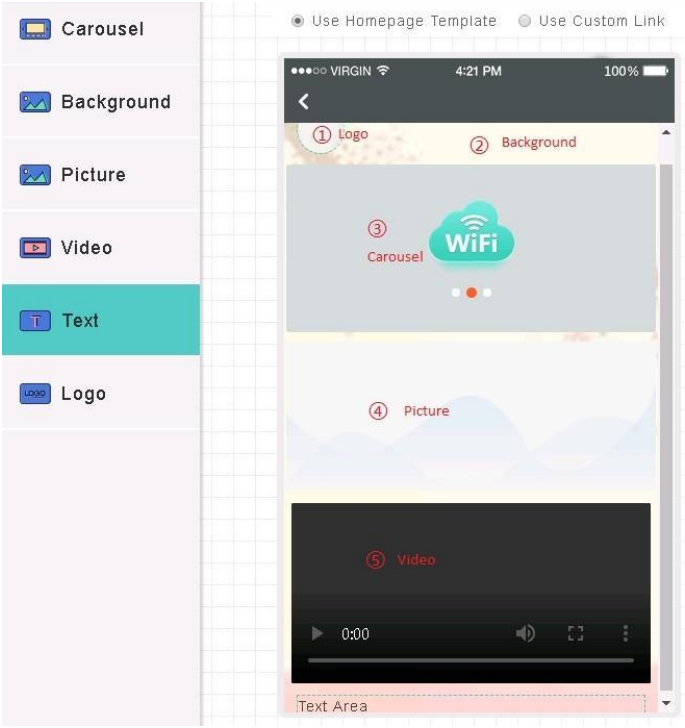
Restrições e diretrizes

O tamanho da imagem não pode exceder 1 M. Como prática recomendada, defina o tamanho da imagem entre 100 KB e 200 KB. Somente os formatos JPG, JPEG, BMP, PNG, GIF e SVG são permitidos.

Como prática recomendada para não afetar a velocidade de carregamento da página, não adicione muitos controles.

Procedimento

1. **Na barra de navegação superior, clique em** *Service (Serviço).*
2. **Selecione** *Authentication (Autenticação)* **no painel de navegação.**
3. **Na guia** *Authentication Templates (Modelos de autenticação)***, clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**
4. **Defina as seguintes configurações, conforme mostrado na** *Figura Visualização da alteração da configuração:*
   - **Logotipo: a relação de aspecto deve ser 1:1. A imagem será automaticamente cortada em um círculo. Você pode insira um nome de loja com comprimento inferior a 12 caracteres.**
   - **Plano de fundo: a proporção deve ser de 3:5.**
   - **Carrossel: a proporção deve ser de 11:5. São necessárias duas ou três imagens com a mesma altura.**
   - **Imagem: a relação de aspecto deve ser 11:5. A descrição da imagem não pode exceder 48 caracteres.**
   - **Vídeo: o tamanho do vídeo não pode exceder 5 M. Somente os formatos MP4, WEBM e OGG são permitidos.**
   - **Texto: você pode editar a fonte, o tamanho da fonte, o negrito e a cor da fonte.**



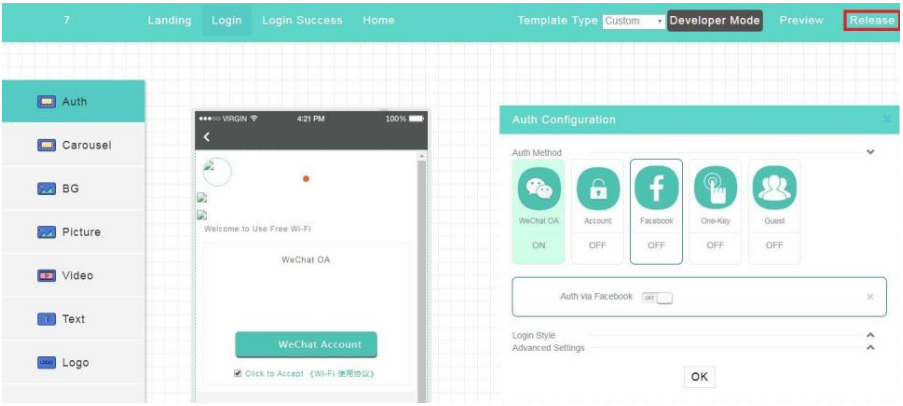
Descrição do modelo personalizado

Para configurar a página inicial, clique na guia Home e selecione *Use Custom Link (Usar link personalizado).*

5. **Digite um link personalizado e clique em** *Upload*.
6. **Para visualizar o link, clique em** *Preview (Visualizar)* **no canto superior direito da página.**

Pré-visualização da alteração da configuração

7. **Clique em** *Liberar* **no canto superior direito da página.**
   A página inicial enviada aos usuários durante a autenticação do portal será substituída pela página redirecionada por esse link personalizado.



Configuração do modelo personalizado

3.2. Configurar definições avançadas

O INC Cloud fornece configurações avançadas de autenticação para simplificar o gerenciamento de autenticação, reduzir custos e otimizar a promoção no mercado. *A tabela Recursos avançados de autenticação do INC Cloud* **descreve os recursos avançados disponíveis para cada método de autenticação. Você pode definir essas configurações conforme necessário.**

Recursos avançados de autenticação do INC Cloud:

Método de autenticação	Recursos avançados
Autenticação de uma chave	Bypass cativo Ocultar e personalizar o botão de autenticação de uma chave Configurações de acesso à Internet Autenticação gratuita Reautenticação entre sites e entre SSIDs Controle de acesso à Internet Modo de desenvolvedor Lista branca e lista negra de nomes de domínio Visualização e exportação do histórico da implementação da configuração de autenticação
Autenticação de conta fixa	Bypass cativo Gerenciamento em massa de contas fixas Alteração de senha por autoatendimento Colaboração com o servidor LDAP Alteração dos efeitos visuais da página de login Configurações de acesso à Internet Autenticação gratuita Reautenticação entre sites e entre SSIDs Controle de acesso à Internet Modo de desenvolvedor Lista branca e lista negra de nomes de domínio Visualização e exportação do histórico da implementação da configuração de autenticação
Autenticação de convidados	Bypass cativo Configurações de acesso à Internet Autenticação gratuita Reautenticação entre sites e entre SSIDs Controle de acesso à Internet Modo de desenvolvedor Lista branca e lista negra de nomes de domínio Visualização e exportação do histórico da implementação da configuração de autenticação
Autenticação de terminal burro	Bypass cativo Gerenciamento de grupos de contas de terminais burros Controle de acesso à Internet Modo de desenvolvedor Lista branca e lista negra de nomes de domínio Visualização e exportação do histórico da implementação da configuração de autenticação

Ativar o recurso captive-bypass

Normalmente, o dispositivo envia a página de autenticação para um cliente automaticamente quando o cliente tenta acessar uma rede de autenticação de portal. O recurso captive-bypass permite que o dispositivo envie a página de autenticação do portal para o cliente somente quando o usuário iniciar um navegador.

Para ativar o recurso captive-bypass, você deve executar as seguintes etapas no dispositivo:

1. **Entre na visualização do sistema.**
   visão do sistema
2. **Entre na visualização do servidor da Web do portal da Cloud do servidor da Web.**
   Portal web-server Cloud
3. **Ativar o recurso captive-pass.**
   captive-bypass enable

Ocultar ou personalizar o botão de autenticação de uma tecla

Execute esta tarefa para ocultar o botão de autenticação de uma chave ou alterar o estilo do botão. Se o botão estiver oculto, os usuários passarão pela autenticação automaticamente após a expiração do cronômetro de contagem regressiva na página de login.

Restrições e diretrizes

Você pode alterar o estilo do botão somente quando o botão não estiver oculto.

Procedimento

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações>Routers (Roteadores>Authentication (Autenticação)* **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique na guia** *Wireless Authentication Templates (Modelos de autenticação Wireless)***.**
5. **Clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**
6. **Clique no bloco** *One-Key* **na área** *Configurações de Autorização* **e, em seguida, oculte ou personalize o botão conforme necessário.**

Gerenciar contas fixas

Execute esta tarefa para excluir, importar ou exportar contas fixas em

massa. Para gerenciar contas fixas:

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações>Routers (Roteadores>Users (Usuários)* **no painel de navegação.**
3. **Clique na guia** *Fixed Accounts (Contas fixas)***.**
4. **Para excluir contas fixas, selecione as contas fixas de destino e clique em** *Excluir.*
5. **Para importar contas fixas, clique em** *Importar,* **faça o download do arquivo de modelo e preencha o arquivo conforme necessário e, em seguida, carregue o arquivo de modelo.**
6. **Para exportar contas fixas, clique em** *Exportar.*

Ativar a alteração de senha por autoatendimento

Esse recurso permite que os usuários alterem as senhas no login. Com esse recurso desativado, somente os administradores podem alterar as senhas de contas fixas.

Para ativar a alteração de senha por autoatendimento:

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações>Routers (Roteadores>Authentication (Autenticação)* **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique na guia** *Wireless Authentication Templates (Modelos de autenticação Wireless)***.**
5. **Clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**
6. **Clique na caixa** *Account (Conta)* **na área** *Auth Configuration (Configuração de autenticação)***.**
7. **Ativar** *alterar senha.*

Permitir a colaboração com um servidor LDAP para verificação de conta fixa

Execute esta tarefa para permitir que o INC Cloud informe nomes de usuário e senhas ao servidor LDAP para verificação quando os usuários tentarem acessar a WLAN usando contas fixas. Isso libera os administradores de rede da importação de informações de conta do servidor LDAP para o INC Cloud.

Restrições e diretrizes

Para usar esse recurso, certifique-se de que o servidor LDAP tenha sido configurado.

Procedimento

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações >Routers (Roteadores >Authentication (Autenticação)* **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique na guia** *Wireless Authentication Templates (Modelos de autenticação Wireless)***.**
5. **Clique no ícone** *Draw (Desenhar)*  **para o modelo de autenticação de destino.**
6. **Clique na caixa** *Account (Conta)* **na área** *Auth Configuration (Configuração de autenticação)***.**
7. **Habilite** *o LDAP* **e defina as configurações do LDAP conforme necessário.**
8. **Clique em** *LDAP Config Verification (Verificação de configuração* **LDAP) para verificar as configurações LDAP.**

Alterar as configurações de efeito visual da página de login

Execute esta tarefa para personalizar a cor do plano de fundo, a opacidade do plano de fundo e a cor do texto no login
página.

Restrições e diretrizes

Cuidado:

A restauração das configurações padrão removerá todas as configurações de efeitos visuais definidas pelo usuário e a operação de restauração é
irreversível. Use esse recurso com cautela.

As configurações de efeito visual dos métodos de autenticação só têm efeito quando vários métodos de autenticação são usados.
estão ativados.

Procedimento

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações>Routers (Roteadores>Authentication (Autenticação)* **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique na guia** *Wireless Authentication Templates (Modelos de autenticação Wireless)***.**
5. **Clique no ícone** *Draw (Desenhar)*  **para o modelo de autenticação de destino.**
6. **Clique para expandir o menu** *Login Style (Estilo de login)* **na área** *Auth Configuration (Configuração de autenticação)***.**
7. **Configure a cor do plano de fundo, a opacidade do plano de fundo e a cor do texto, conforme necessário. O ajuste será exibido na área de visualização em tempo real. Para restaurar as configurações padrão do efeito visual, clique em** *Restore Default (Restaurar padrão).*

Configurar as definições de acesso à Internet

Procedimento

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações >Routers (Roteadores >Authentication (Autenticação)* **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique na guia** *Wireless Authentication Templates (Modelos de autenticação Wireless)***.**
5. **Clique no ícone** *Draw (Desenhar)*  **para o modelo de autenticação de destino.**
6. **Clique para expandir o menu** *Advanced Settings (Configurações avançadas)* **na área** *Auth Configuration (Configuração de autenticação)***.**
7. **Defina as configurações de acesso à Internet conforme necessário.**

Parâmetros

- **Tempo limite da sessão: duração máxima contínua on-line de um cliente após uma autenticação. Um cliente será desconectado quando sua duração contínua on-line exceder o tempo limite. O tempo limite da sessão não pode ser maior do que a duração on-line diária.**
- **Duração diária on-line: duração máxima on-line de um cliente em um dia. Um cliente será desconectado quando sua duração on-line por um dia exceder o limite. A duração on-line diária não pode ser menor que o tempo limite da sessão.**

" **Tráfego mínimo e temporizador de inatividade: faz o logoff de um cliente se o tráfego dentro de um temporizador de inatividade não atingir o limite mínimo de tráfego. A configuração do temporizador de inatividade como 0 desativa o recurso de temporizador de inatividade.**

Observação:

Como prática recomendada, defina o timer ocioso para um valor não maior que a metade da concessão do endereço IP dos clientes, permitindo entradas de clientes off-line a serem excluídos a tempo.

- **Client Rate Limit: taxa limitada de tráfego de clientes de uplink e downlink. Esse recurso é compatível com versões superiores a 5417P01.**
- **HTTPS para aterrissagem e login: use sessões HTTPS para a página de aterrissagem e login.**
- **Permitir PC: Permitir que os PCs acessem a WLAN. A autenticação do Facebook não é compatível com esse recurso.**

Gerenciar grupos de contas de terminais burros

Execute esta tarefa para criar, Excluir ou editar grupos de contas de terminal burro e importar ou exportar grupos de contas de terminal burro.
contas terminais.

Se você ativar a autenticação de terminal burro e especificar um grupo de contas, somente os terminais burros em
o grupo pode acessar a WLAN.

Para gerenciar grupos de contas de terminais burros:

1. **Na barra de navegação superior, clique em** *Service (Serviço).*
2. **Selecione** *Authentication (Autenticação)* **no painel de navegação.**
3. **Clique na guia** *Accounts (Contas)***.**
4. **Na guia** *Dumb Terminal Accounts (Contas de terminal burro)***, configure os grupos de contas de terminal burro.**

Configurar a autenticação automatizada do portal

Esse recurso permite que os usuários que foram autenticados acessem a rede sem nova autenticação dentro do período livre de autenticação. Os seguintes modos estão disponíveis:

- **Redirecionamento de portal: nesse modo, os usuários devem executar um navegador para acionar a autenticação automática do portal. Esse modo suporta o envio de anúncios para os clientes.**
- **MAC-trigger: nesse modo, os usuários podem acessar a WLAN sem executar um navegador. Esse modo não não suporta o envio de anúncios para os clientes.**

Configurar a autenticação de redirecionamento do portal

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações>Routers (Roteadores>Authentication (Autenticação)* **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique na guia** *Wireless Authentication Templates (Modelos de autenticação Wireless)***.**
5. **Clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**
6. **Clique para expandir o menu** *Advanced Settings (Configurações avançadas)* **na área** *Auth Configuration (Configuração de autenticação)***.**
7. **Clique na guia** *Livre de Autenticação* **e configure o recurso** *Autenticação Gratuita***.**

Configurar a autenticação de acionamento de MAC

1. **Configure a autenticação de redirecionamento do portal. Para obter mais informações, consulte** *Configurar o redirecionamento do portal autenticação.*
2. **Aplique** *a nuvem* **do servidor de vinculação MAC à** *nuvem* **do modelo de serviço**. **[Sysname] wlan service-template Cloud**

   [Sysname-wlan-st-cloud] portal apply mac-trigger-server cloud

Configurar a reautenticação entre sites e entre SSIDs

Esse recurso permite que os clientes que foram autenticados façam roaming entre serviços Wireless associados a diferentes sites ou diferentes SSIDs para o mesmo site sem reautenticação. Esses serviços sem fio devem usar o mesmo modelo de autenticação ou ter o mesmo SSID.

Restrições e diretrizes

Esse recurso está disponível somente para modelos de autenticação configurados no App Center.

Procedimento

1. **Na barra de navegação superior, clique em** *Service (Serviço).*
2. **Selecione** *Authentication (Autenticação)* **no painel de navegação.**
3. **Clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**
4. **Clique para expandir o menu** *Advanced Settings (Configurações avançadas)* **na área** *Auth Configuration (Configuração de autenticação).*
5. **Clique na guia** *Livre de Autenticação* **e ative** *a Autenticação gratuita.*
6. **Configure a reautenticação entre sites e entre SSIDs.**

Configurar o controle de acesso à Internet

Execute esta tarefa para especificar os intervalos de tempo durante os quais os usuários têm permissão para acessar a WLAN.

Restrições e diretrizes

O controle de acesso à Internet é feito hora. É possível especificar um máximo de cinco intervalos de tempo para um dia. Para especificar um intervalo de tempo que termine às 24 horas, defina o horário de término como 00. Se você definir um intervalo de tempo de 00 a 00 para um dia, os usuários poderão acessar a Internet a qualquer momento nesse dia.

Procedimento

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações>Routers (Roteadores>Authentication (Autenticação)* **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique na guia** *Wireless Authentication Templates (Modelos de autenticação Wireless).*
5. **Clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**
6. **Clique para expandir o menu** *Advanced Settings (Configurações avançadas)* **na área** *Auth Configuration (Configuração de autenticação).*
7. **Clique na guia** *Internet Access Control (Controle de acesso à Internet)* **e especifique os intervalos de tempo.**

Configurar o modo de desenvolvedor

Cuidado:

A edição dos códigos das funções existentes pode desativar a autenticação do INC Cloud. Use esse recurso com cuidado.

O modo de desenvolvedor permite que os usuários modifiquem os códigos-fonte de um modelo de autenticação para
para fins de personalização.

Procedimento

1. **Na barra de navegação superior, clique em** *Rede .*
2. **Selecione** *Configurações (Configurações>Routers (Roteadores>Authentication (Autenticação)* **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique na guia** *Wireless Authentication Templates (Modelos de autenticação Wireless).*
5. **Clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**
6. **Clique em** *Developer Mode (Modo de desenvolvedor)*

no canto superior direito. Configurar a lista branca e a

lista negra de nomes de domínio *Restrições e*

diretrizes

Esse recurso entra em vigor somente quando a autenticação sem fio está configurada.

Procedimento

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações>Routers (Roteadores>Authentication (Autenticação)* **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique na guia** *Domain Name Whitelist (Lista* **branca** *de nomes de domínio) ou Domain Name Blacklist*

(Lista **negra** *de nomes de domínio*) **para configurar a lista branca ou negra.**

Exibir ou exportar o histórico da implantação do modelo de autenticação

Execute esta tarefa para visualizar o histórico de todas as implantações de modelos de autenticação ou implantações no dia atual, últimos 7 dias ou últimos 30 dias.

Para exibir ou exportar o histórico da implementação do modelo de autenticação:

1. **Na barra de navegação superior, clique em** *Service (Serviço).*
2. **Selecione** *Authentication (Autenticação*) **no painel de navegação.**
3. **Na guia** *Authentication Templates (Modelos de autenticação*)**, clique no ícone** *Apply (Aplicar*) **para o modelo de autenticação de destino.**
4. **Clique na guia ACs para visualizar o histórico de implementação de um AC.**

4. Gerenciar usuários do INC Cloud

4.1. Configurar a lista negra de clientes

Execute esta tarefa para proibir o acesso de clientes específicos à WLAN.

Restrições e diretrizes

Esse recurso tem efeito apenas em clientes off-line. Se você adicionar um cliente on-line à lista negra, ele será rejeitado na próxima tentativa de acesso.

Procedimento

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações> Categoria do dispositivo> Usuários* **no painel de navegação.**
3. **Execute uma das seguintes tarefas para adicionar usuários à lista negra:**
   - **Na guia** *Guests (Convidados*)**, clique no ícone** *Add to Blacklist Adicionar à lista negra* **para o usuário-alvo.**
   - **Na guia** *Blacklist (Lista negra*)**, clique em** *Add (Adicionar).*

4.2. Fazer logoff de usuários on-line

Execute essa tarefa para fazer logoff de usuários on-line específicos ou de todos os usuários on-line.

Restrições e diretrizes

Esse recurso não tem efeito sobre usuários sem autenticação.

Esse recurso está disponível somente em cenários com um roteador CA ou com fio como autenticador.

Procedimento

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Rede> Clientes> Detalhes do convidado* **no painel de navegação.**
3. **Selecione uma filial e um local na parte superior da página.**
4. **Na guia** *Clientes on-line***, clique em** *Clientes autenticados.*
5. **Para fazer logoff de clientes específicos, selecione os clientes e clique em** *Log Off Selected Users (Fazer logoff de usuários selecionados).* **Para fazer logoff de todos os clientes, clique em** *Log Off All Users (Fazer logoff de todos os usuários).*

5. Configurar o portal fail-permit

Esse recurso está disponível somente em cenários com um roteador AC ou Wireless como autenticador.

A permissão de falha do portal permite que os usuários tenham acesso à rede sem autenticação do portal quando o dispositivo de acesso detecta que o servidor de autenticação do portal ou o servidor da Web do portal está inacessível.

Depois que a autenticação do portal for retomada, os usuários não autenticados deverão ser aprovados na autenticação do portal para acessar a rede. Os usuários que foram aprovados na autenticação do portal antes do evento de permissão de falha podem continuar acessando a rede.

5.1. Restrições e diretrizes

Para que esse recurso entre em vigor, certifique-se de ter definido as configurações básicas no dispositivo. Para obter mais informações
informações, consulte "Definir configurações no dispositivo".

Procedimento

1. Ativar a permissão de falha do portal.

   <Sysname> visão do sistema

   [Sysname] wlan service-template

   Cloud

   [Sysname-wlan-st-cloud] portal fail-permit web-

   server [Sysname-wlan-st-cloud] quit

2. Configurar a detecção do servidor Web do portal.

Cuidado:

Para evitar a oscilação do servidor do portal, siga a ordem fornecida para configurar a detecção do servidor da Web do portal.

 # Especifique o URL e o tipo de detecção do servidor Web do portal.

[portal web-server cloud

[Sysname-portal-websvr-cloud] server-detect url http://oasisauth.intelbras.com/portal/ping de- tect-type http

 # Configurar a detecção do servidor:

" Defina o intervalo de detecção para 600 segundos.

" Defina o número máximo de falhas de detecção consecutivas como 2.

" Configure o dispositivo para enviar uma mensagem de registro e uma mensagem trap após a capacidade de alcance do servidor alterações de status.

[Sysname-portal-websvr-cloud] server-detect interval 10 retry 2 log

trap [Sysname-portal-websvr-cloud] quit

6. Configure a autenticação quando um AP se registrar em um AC em uma rede pública

Esse recurso está disponível somente em cenários com um roteador AC ou Wireless como autenticador.

Por padrão, o dispositivo fornece a porta HTTP 80 para que os clientes troquem pacotes de autenticação. Com o encaminhamento local ativado, se os APs se registrarem no AC por meio da rede pública e a porta 80 não estiver disponível, execute esta tarefa para configurar o CMCC ou alterar a porta de serviço HTTP para que os clientes realizem a autenticação do INC Cloud.

6.1. Configurar CMCC

Você deve configurar a CMCC no AC e na Cloud do INC. Para configurar o

CMCC:

1. **Configurar o protocolo CMCC**
   - **Configurar o INC Cloud:**
     - **Configurar o INC Cloud em uma rede AC+fit AP**
     - **Configure o INC Cloud em uma rede Wireless**
   - **Configurar o dispositivo**
2. **(Opcional) Configure a autenticação de redirecionamento do portal CMCC**
   - **Configurar o**
   - **Configurar o dispositivo**

6.2. Restrições e diretrizes

Com o CMCC configurado, o tempo limite da sessão, a duração diária on-line, o tráfego mínimo e o temporizador de inatividade
As configurações ficam indisponíveis.

Configurar o protocolo CMCC

Configure o INC Cloud em uma *rede AC+fit AP*

1. **Na barra de navegação superior, clique em** *Rede*
2. **Selecione** *Configurações (Configurações>ACs> Authentication (Autenticação)* **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**
5. **Clique para expandir o menu** *Advanced Settings (Configurações avançadas)* **na área** *Auth Configuration (Configuração de autenticação)*.
6. **Clique na guia** *CMCC*.
7. **Habilite** *o protocolo CMCC* **e selecione um protocolo conforme necessário.**

Configure o INC Cloud em uma rede Wireless com um roteador como autenticador

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações>Routers (Roteadores>Authentication (Autenticação)* **no painel de navegação.**
3. **Selecione uma filial, um site e um dispositivo na parte superior da página.**
4. **Clique no ícone** *Draw (Desenhar)* **para o modelo de autenticação de destino.**
5. **Clique para expandir o menu** *Advanced Settings (Configurações avançadas)* **na área** *Auth Configuration (Configuração de autenticação)*.
6. **Clique na guia** *CMCC*.
7. **Habilite** *o protocolo CMCC* **e selecione um protocolo conforme necessário.**

Configurar o dispositivo

 # Crie a nuvem do servidor de autenticação do portal e insira sua visualização.

<Sysname> visão do sistema

[Portal server Cloud

 # Especifique 139.217.11.74 como o endereço IPv4 do servidor de autenticação do portal.

[Sysname-portal-server-cloud] ip 139.217.11.74

 # Especifique o tipo do servidor de autenticação do portal como cmcc.

[Sysname-portal-server-cloud] server-type cmcc

 # Configure o dispositivo para enviar pacotes de registro para o servidor de autenticação do portal em intervalos de 60 segundos.

[Sysname-portal-server-cloud] server-register

interval 60 [Sysname-portal-server-cloud] quit

6.3. Configurar a autenticação de redirecionamento do portal CMCC

Configurar a Cloud do INC

 # Habilite a autenticação de redirecionamento de portal. Para obter mais informações, consulte *Configurar redirecionamento de portal a autenticação de* **para redes AC+fit AP e** *Configurar a autenticação de redirecionamento de portal* **para redes sem fio com um roteador sem fio como autenticador.**

Configurar o dispositivo

Certifique-se de ter definido as configurações básicas no dispositivo. Para obter mais informações, consulte *Configurar as definições no dispositivo.*

Para configurar o dispositivo:

1. **Configure o servidor de vinculação de MAC.**

Cuidado:

Para não afetar os serviços Wireless, é necessário especificar um servidor de vinculação de MAC dedicado para CMCC, mesmo que um servidor de vinculação de MAC
O servidor de vinculação foi criado.

 # Crie o servidor de vinculação de MAC mts e entre em sua exibição.

<Sysname> visão do sistema

[Sysname] portal mac-trigger-server

mts
 # Especifique o endereço IP do servidor de vinculação de MAC como 139.217.11.74.

[Sysname-portal-mac-trigger-server-mts] ip 139.217.11.74 #

Especifique o tipo do servidor de vinculação de MAC como

cmcc. [Sysname-portal-mac-trigger-server-mts] server-type

cmcc

 # (Opcional.) Defina o limite de tráfego livre para usuários do portal,

em bytes. [Sysname-portal-mac-trigger-server-mts] free-traffic

threshold 1 [Sysname-portal-mac-trigger-server-mts] quit

 # Vincular o servidor de vinculação MAC mts ao modelo de serviço Cloud.

[Sysname] wlan service-template Cloud

[Sysname-wlan-st-cloud] portal apply mac-trigger-server mts

2. **Configure os atributos de autorização para usuários no domínio ISP.**
   # Crie uma nuvem de domínio ISP.
   [Sysname] domain cloud
   # Defina o cronômetro de inatividade, em
   minutos. [Sysname-isp-cloud] authorization-
   attribute idle-cut 30 # Defina o tempo limite da
   sessão, em minutos.
   [Sysname-isp-cloud] authorization-attribute session-
   timeout 360 [Sysname-isp-cloud] quit

6.4. Alterar a porta do serviço HTTP

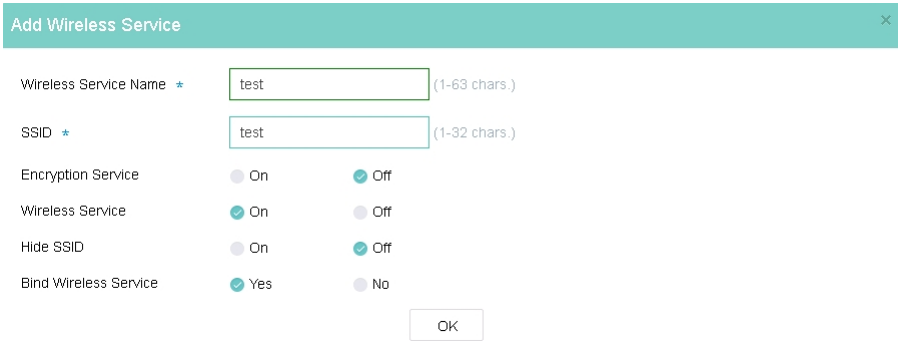
Antes de executar essa tarefa, certifique-se de ter configurado as definições básicas no dispositivo. Para obter mais informações
informações, consulte *Definir configuraçõ**es** no dispositivo.*

Para alterar a porta do serviço HTTP:

1. **Defina o número da porta do serviço HTTP. Neste exemplo, o número da porta é 8088.**
   <Sysname> visão do sistema
   [Sysname] ip http port 8088
2. **Crie um serviço da Web de portal local baseado em HTTP e defina o número da porta de escuta como 8088. [Sysname] portal local-web-server http**
   [Sysname-portal-local-websvr-http] tcp-port
   8088 [Sysname-portal-local-websvr-http] quit
3. **Configure o servidor do portal.**
   # Configure a URL do servidor da Web do portal. x.x.x.x representa o IP de saída da rede em no qual o CA reside.
   [portal web-server cloud
   [Sysname-portal-websvr-cloud] url http://oasisauth.intelbras.com/portal/protocol?redirect_ uri=http://x.x.x.x:8088/portal/cloudlogin.html
   # Configure o servidor do INC Cloud para redirecionar os usuários para x.x.x.x:8088.
   [Sysname-portal-websvr-cloud] if-match original-url http://captive.apple.com user-agent Mozilla temp-pass redirect-url http://oasisauth.intelbras.com/portal/protocol?redirect_uri=http://x-.x.x.x.x:8088/portal/cloudlogin.html
   [Sysname-portal-websvr-cloud] if-match original-url http://www.apple.com user-agent Mozilla temp-pass redirect-url http://oasisauth.intelbras.com/portal/protocol?redirect_uri=http://x-.x.x.x.x:8088/portal/cloudlogin.ht
   ml [Sysname-portal-websvr-
   cloud] quit

7. Configurar serviços Wireless

1. **Na barra de navegação superior, clique em** *Rede.*
2. **Selecione** *Configurações (Configurações>Device Category (Categoria do dispositivo>Wireless Services (Serviços Wireless)* **no painel de navegação.**
3. **Na guia** *Wireless Services (Serviços Wireless)***, clique em** *Add (Adicionar).*
4. **Para configurar um serviço de criptografia, selecione** *Ligado ou Desligado* **no campo** *Serviço de criptografia***, conforme necessário.**



Configuração de um serviço de criptografia

5. **Para sincronizar as informações de SSID, clique em** *Sync SSID Info.*
   Certifique-se de ter criado um serviço Wireless e configurado as informações de SSID no dispositivo.

Observação:
Esse recurso está disponível somente para ACs de versão anterior a 5418 e roteadores de versão anterior a 0809.

Sincronização de informações de SSID

6. **Para sincronizar as configurações do serviço Wireless nos dispositivos para a INC Cloud, clique em** *Sincronizar para a Nuvem.* **Essa operação sincroniza as configurações, como o nome do serviço Wireless, o SSID e a taxa de largura de banda garantida para o INC Cloud.**

Observação:
Esse recurso está disponível somente para ACs da versão 5418 ou posterior e roteadores da versão 0809 ou posterior.

8. PERGUNTAS FREQUENTES

8.1. Modifiquei e implementei as configurações do modelo de autenticação com êxito. Por que as configurações anteriores entram em vigor nos clientes que ficam on-line após a implementação?

Verifique se as configurações foram modificadas e implementadas com êxito. Se o problema persistir, limpe o navegador
registros de acesso e armazenamento em cache no cliente.

8.2. A página Authentication Templates (Modelos de autenticação) no App Center não exibe os dispositivos disponíveis para implantação de modelos. O que devo fazer?

Verifique se a versão do dispositivo está de acordo com o necessário. Caso contrário, atualize o dispositivo para a mais recente.

8.3. Como posso alterar o SSID de um serviço sem fio?

1. **Altere o nome do Wi-Fi no INC Cloud. Para redes AC+fit AP, você também pode alterar o nome do Wi-Fi nome no CA.**
2. **Desvincule e, em seguida, vincule novamente o modelo de serviço do serviço de autenticação.**

8.4. Como posso atualizar meu INC Cloud para usar os recursos recém-lançados?

Os recursos no INC Cloud são atualizados automaticamente e não requerem operações manuais. Para os novos do modelo de autenticação, talvez seja necessário reconfigurar e, em seguida, liberar o modelo para que os novos recursos entrem em vigor.

8.5. Por que um cliente pode ficar off-line e depois ficar on-line sem ser autenticado, mesmo que a autenticação gratuita não esteja configurada?

O sistema não remove a entrada do cliente da lista de clientes autenticados imediatamente após um evento de desassociação de cliente. A entrada não será removida até que o timer de inatividade expire ou o administrador faça o logoff do cliente. Um cliente off-line pode ficar on-line sem ser autenticado se sua entrada ainda existir.

É possível visualizar as entradas do cliente no INC Cloud ou executando o comando display portal user all.

8.6. Por que o número de clientes autenticados excede o número total de clientes on-line?

Esse sintoma ocorre quando um cliente acaba de ficar off-line. O sistema não remove a entrada do cliente da lista de clientes autenticados imediatamente após um evento de desassociação de cliente. A entrada não será removida até que o timer de inatividade expire ou o administrador faça o logoff do cliente manualmente.

8.7. Configurei as definições de autenticação no dispositivo e no INC Cloud conforme necessário. A tentativa de acesso do cliente pode acionar a autenticação do portal, mas não consegue abrir a página de redirecionamento. O que devo fazer?

Esse problema pode ocorrer se o segmento de rede do endereço IP do cliente for desconhecido para os dispositivos de uplink e os pacotes não puderem ser transmitidos de volta. Para resolver esse problema, configure o comando nat outbound na interface do dispositivo que conecta o dispositivo à rede externa ou use o IGP para anunciar o segmento de rede na rede.

8.8. Os clientes iOS não podem acionar a autenticação mesmo que o captive-bypass otimizado esteja ativado. O que devo fazer?

Execute o comando portal captive-bypass optimize delay *seconds* para definir o tempo limite de proteção do captive-bypass. O intervalo de valores é de 6 a 60 segundos e o valor padrão é 6 segundos.

Para não afetar o desempenho do dispositivo, não defina o tempo limite com um valor muito alto.

9. Apêndice A Comandos de autenticação para o dispositivo

Esta seção descreve os comandos que precisam ser executados no dispositivo para autenticação de uma chave, contagem de acesso fixo, Facebook, terminal burro e convidado.

Para as autenticações do aplicativo e do Facebook, você deve definir as configurações em *Configurar do Facebook autenticação* **e** *Configurar autenticação do Facebook,* **respectivamente, depois de concluir as configurações nesta seção.**

Para executar rapidamente esses comandos no dispositivo, edite as seções escurecidas conforme necessário e cole todos os comandos
os comandos na visualização do usuário do dispositivo.

Observação:

" Execute esses comandos somente em versões anteriores à 5405. A versão 5405 e posteriores suportam a implementação automática da configuração de autenticação nos dispositivos e não precisam da configuração manual desses comandos.

" Certifique-se de que os comandos não entrem em conflito com a configuração existente no dispositivo.

" Certifique-se de ter concluído as tarefas dos pré-requisitos de configuração. Para obter mais informações, consulte *Pré-requisitos.*

---

visão do sistema
domain cloud portal de
autenticação nenhum portal
de autorização nenhum
portal de contabilidade
nenhum quit

portal servidor web Cloud
url
http://oasisauth.intelbras.com/portal/protocol
server-type oauth
if-match user-agent CaptiveNetworkSupport redirect-url http://oasisauth.intelbras.com/ generate_404
if-match user-agent Dalvik/2.1.0(Linux;U;Android7.0;HUAWEI redirect-url http://oasisauth.intelbras.com/generate_404
if-match original-url http://captive.apple.com user-agent Mozilla temp-pass redirect-url http:// oasisauth.intelbras.com/portal/protocol
if-match original-url http://www.apple.com user-agent Mozilla temp-pass redirect-url http:// oasisauth.intelbras.com/portal/protocol
if-match original-url http://10.168.168.168 temp-
pass captive-bypass ios optimize enable
sair

wlan service-template cloud
portal enable method direct
portal domain cloud
portal apply web-server cloud portal
temp-pass period 20 enable quit

portal local-web-server
http sair
portal local-web-server
https sair

ip http enable
ip https enable
portal host-check
enable portal user log
enable
portal free-rule 1 destination ip 114.114.114.114 255.255.255.255
portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53 portal
free-rule 4 destination ip any tcp 5223
portal free-rule 5 destination oasisauth.intelbras.com
portal free-rule 10 destination short.weixin.qq.com
portal free-rule 11 destination mp.weixin.qq.com portal
free- rule 12 destination long.weixin.qq.com portal
free-rule
13 destination dns.weixin.qq.com
regra livre do portal 14 destination
minorshort.weixin.qq.com regra livre do portal 15
destination extshort.weixin.qq.com regra livre do portal
16 destination szshort.weixin.qq.com regra livre do portal
17 destination szlong.weixin.qq.com regra livre do portal
18 destination szextshort.weixin.qq.com regra livre do
portal 19 destination isdspeed.qq.com portal free-rule 20
destination wx.qlogo.cn
portal free-rule 21 destination wifi.weixin.qq.com
portal free-rule 22 destination open.weixin.qq.com

Portal safe-redirect enable
portal safe-redirect method get post portal
safe-redirect user-agent Android portal safe-
redirect user-agent CFNetwork
portal safe-redirect user-agent CaptiveNetworkSupport
portal safe-redirect user-agent MicroMessenger
portal safe-redirect user-agent Mozilla
portal safe-redirect user-agent iPhone
portal safe-redirect user-agent micromessenger

intelbras

fale com a gente

Suporte a clientes: (48) 2106 0006
Fórum: forum.intelbras.com.br
Suporte via chat: chat.apps.intelbras.com.br
Suporte via e-mail: suporte@intelbras.com.br
SAC / Onde comprar? / Quem instala? : 0800 7042767

Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – 88122-001
CNPJ 82.901.000/0014-41 – www.intelbras.com.br

01.25