English

Authentication user manual

INC Cloud

intelbras

INC Cloud

Congratulations, you have just purchased a product with Intelbras quality and safety.

Summary

1. About INC Cloud authentication

Important:
Some features in this document are restricted only to China mainland.

Intelbras INC Cloud provides abundant authentication methods for access users such as employees, guests, and IoT terminals. When a client wants to access the Internet or the specific network resources, the access device redirects the client to the INC Cloud for portal authentication.

Intelbras INC Cloud offers the following benefits:

- No upper limit for authentication clients.
- Abundant authentication policies.
- Custom ads pushing services.

Intelbras INC Cloud provides the authentication methods listed in *Table Authentication methods*.

Authentication methods:

Authentication method	Applicable scenario	Remarks	Combined authentication
One-key	Low auditing and operational statistics collection requirements, such as restaurants and shops.	MAC-based authentication. Users can complete authentication by simply clicking a button on the portal authentication page.	Supported
Fixed account	Network users are fixed, such as campus and office areas.	Username and password based authentication. The following functions are supported: LDAP Import and export of accounts Binding one account to multiple MAC addresses Concurrent client limit	Supported
Google authentication	Operators use Google to collect statistics about network users.	Users must log in to Google to grant access to the INC Cloud. This method is available only at https://oasiscloud.intelbras.com.	Supported
Twitter authentication	Operators use Twitter to collect statistics about network users.	Users must log in to Twitter to grant access to the INC Cloud. This method is available only at https://oasiscloud.intelbras.com.	Supported
Guest authentication	Enterprises or shops where temporary guest access is required.	A guest can access the network after an approver scans the QR code on the terminal of the guest and authorize the terminal.	Not supported
Dumb terminal authentication	IoT devices, wireless printers, and POS terminals.	Automated authentication on specific wireless terminals.	Not supported
Facebook authentication	Operators use Facebook to collect statistics about network users.	Users must log in to Facebook to grant access to the INC Cloud. This method is available only at https://oasiscloud.intelbras.com.	Supported

Authentication method and networking compatibility

	Compatibility with networks with different authenticators		
Authentication method	**AC**	**Wireless router**	**Wired router**
One-key authentication	Yes	Yes	Yes
Fixed account authentication	Yes	Yes	Yes
Guest authentication	Yes	Yes	Yes
Facebook authentication	Yes	No	No
Combined authentication	Yes	Yes	Yes
Dumb terminal authentication	Yes	Yes	No
Bulk authentication	Yes	Yes	No
Custom authentication page	Yes	Yes	Yes

Note:
A wireless router can act as an AC or fat AP to provide wireless authentication. A wired router connects to terminals directly or connects to terminals through a switch or fat AP for authentication.

2. Configure INC Cloud authentication with an AC as the authenticator

2.1. Configure basic settings

Prerequisites

Before configuring INC Cloud authentication, complete the following tasks:

- Connect the device to the INC Cloud.
  For more information, see *Intelbras INC Cloud Deployment Guide*.
- Complete the VLAN and DHCP settings.
- Configure wireless services and make sure the APs can come online.

Configure settings on the device

Restrictions and guidelines

Only software version 5405 or higher supports deploying authentication settings automatically. For other software versions, manually configure the following settings on the device.

For fast deployment of the following authentication methods, see *Appendix A Authentication commands for the device.*

- One-key authentication.
- Fixed account authentication.
- Facebook authentication.
- Dumb terminal authentication.
- Guest authentication.

Configure general settings

1. Configure a portal authentication domain.
   # Add an ISP domain named cloud and enter its view.
   <Sysname> system-view
   [Sysname] domain cloud
   # Specify the authentication, authorization and accounting methods as none.
   [Sysname-isp-cloud] authentication portal none
   [Sysname-isp-cloud] authorization portal none
   [Sysname-isp-cloud] accounting portal none
   [Sysname-isp-cloud] quit
2. Configure cloud portal authentication.
   # Add a portal Web server named cloud and specify its URL and type. (If the administrator configures wireless service in the INC Cloud, the configuration will be deployed to the device automatically.)
   [Sysname] portal web-server cloud
   [Sysname-portal-websvr-cloud] url http://oasisauth.intelbras.com/portal/protocol
   [Sysname-portal-websvr-cloud] server-type oauth

 # Configure a match rule to redirect HTTP requests that carry the user agent string CaptiveNetworkSupport to the 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 a match rule to redirect HTTP requests that carry the user agent string Dalvik /2.1.0(Linux;U;Android7.0;HUAWEI to the 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 a temporary pass rule to allow user packets that contain user agent information Mozilla to pass and then redirect the packets destined for the URL http://captive.apple.com to URL http://oasisauth.intelbras.com/portal/protocol.

[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

 # Configure a temporary pass rule to allow user packets that contain user agent information Mozilla to pass and then redirect the packets destined for the URL http://www.apple.com to 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 a temporary pass rule to temporarily allow user packets that access URL http://10.168.168.168 to pass.

[Sysname] portal web-server cloud

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

 # Enable the optimized captive-bypass feature for iOS users.

[Sysname-portal-websvr-cloud] captive-bypass ios optimize enable

[Sysname-portal-websvr-cloud] quit

 # Enable direct portal authentication on service template cloud.

[Sysname] wlan service-template cloud

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

 # Configure the authentication domain as cloud and specify portal Web server cloud as the cloud portal Web server for portal authentication.

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

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

[Sysname-wlan-st-cloud] quit

 # Enable portal temporary pass and set the temporary pass period to 20 seconds.

[Sysname] wlan service-template cloud

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

[Sysname-wlan-st-cloud] quit

 # Add an HTTP-based local portal Web service and enter its view.

[Sysname] portal local-web-server http

[Sysname-portal-local-websvr-http] quit

 # Add an HTTPS-based local portal Web service and enter its view.

[Sysname] portal local-web-server https

[Sysname-portal-local-websvr-https] quit

 # Enable the HTTP and HTTPS services.

[Sysname] ip http enable

[Sysname] ip https enable

 # Enable validity check on wireless portal clients.

[Sysname] portal host-check enable

 # Enable logging for portal user logins and logouts.

[Sysname] portal user log enable

 # Configure destination-based portal-free rule1 to allow portal users to access the DNS service without authentication. (This example uses the 114.114.114.114 255.255.255.255.)

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

 # Configure destination-based portal-free rules 2 and 4 to allow portal users to access the DNS service without authentication.

[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 destination-based portal-free rule 5 to allow portal users to access the INC Cloud authentication server without authentication.

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

 # Configure destination-based portal-free rules 10 to 22 to allow portal users to access the INC Cloud authentication server without authentication.

[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

 # Enable portal safe-redirect.

[Sysname] portal safe-redirect enable

 # Specify HTTP request methods permitted by portal safe-redirect.

[Sysname] portal safe-redirect method get post

 # Specify browser types permitted by portal safe-redirect.

[Sysname] portal safe-redirect user-agent Android

[Sysname] portal safe-redirect user-agent CFNetwork

[Sysname] 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

Configure Facebook authentication

Important:

- Execute commands in this section after you finish the settings in *Configure general settings* or *Appendix A Authentication commands for the device*.
- Free-rule 38 might disable the app from displaying pictures. Please configure this rule as needed or contact Technical Support.

 # Configure destination-based portal-free rules to allow portal users who send an HTTP/HTTPS request that carries Facebook-related host names to access network resources without authentication.

<Sysname> system-view

[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

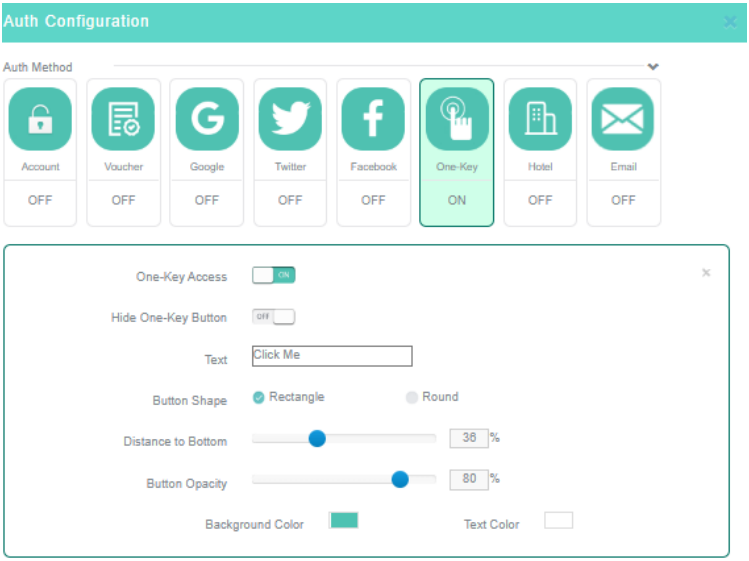
[Sysname] portal free-rule 36 destination static.xx.fbcdn.net

[Sysname] portal free-rule 37 destination staticxx.fbcdn.com

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

Configure one-key authentication

1. On the top navigation bar, click *Network.*
2. Select *Settings > ACs > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. To add an authentication template, click *Add* on the Authentication Templates tab.
5. To edit an authentication template, click the *Edit* icon for that authentication template.
6. To bind an authentication template to a wireless service, click the *Edit* icon for that authentication template, select *Yes* from the *Bind to Wireless Service* field, and then click *Apply.* If the template has been bound to wireless service, skip this step.
7. Click the *Draw* icon for the target authentication template.
8. Click the *One-Key* tile in the *Auth Configuration* area, enable one-key authentication, and then configure other settings as needed.
9. Click *OK* or click *Release* in the upper right corner of the page.



Configuring one-key authentication

Configure fixed account authentication

Restrictions and guidelines

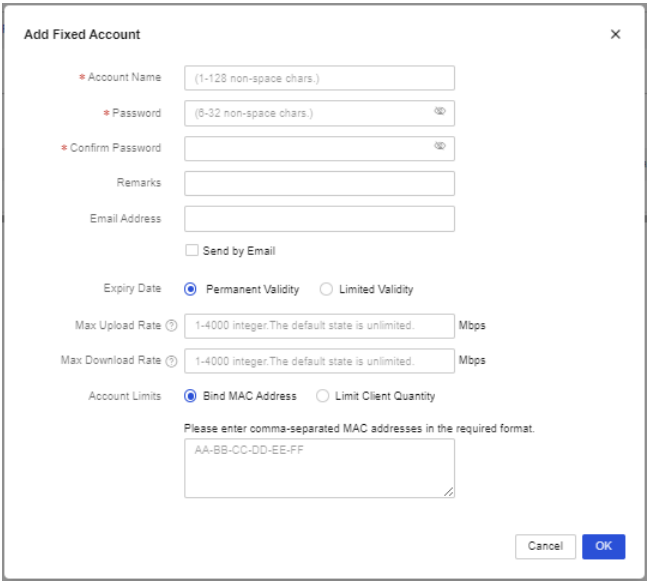
If you do not configure the validity period or configure it as 0, the account never expires.

If you select *Bind MAC Address* and do not enter any MAC addresses, clients that use the fixed account are not limited.

If you select Sent by Email, the system sends the account name and password to the specified email address. The number of email addresses cannot exceed 10 and must be separated by commas.

Procedure

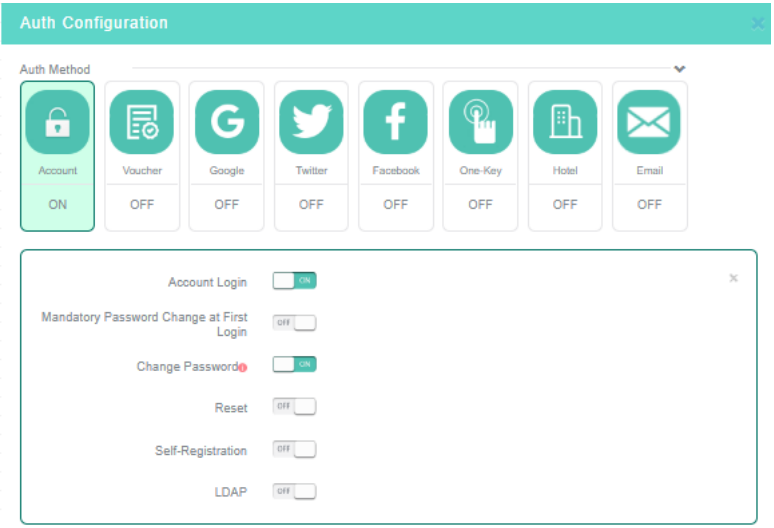
1. On the top navigation bar, click *Network*.
2. Select *Settings > ACs > Users* from the navigation pane.
3. Click the *Fixed Accounts* tab on the Portal Users tab.
4. Click *Add*.
5. Configure fixed account information as required.



Adding a fixed account

1. To add or edit an authentication template, select *Settings > ACs > Authentication* from the navigation pane, and then select a branch, a site, and a device from the top of the page. To add a template, click *Add* on the *Authentication Templates* tab. To edit a template, click the *Edit* icon for that authentication template.
2. To bind an authentication template to a wireless service, click the *Edit* icon for that authentication template, select *Yes* from the *Bind to Wireless Service* field, and then click *Apply*. If the template has been bound to wireless service, skip this step.
3. Click the *Draw* icon for the target authentication template.
4. Click the *Account* tile in the *Auth Configuration* area, enable fixed account authentication, and then configure other settings as needed.
5. Disable other authentication methods.

6. Click *OK* or click *Release* in the upper right corner of the page.

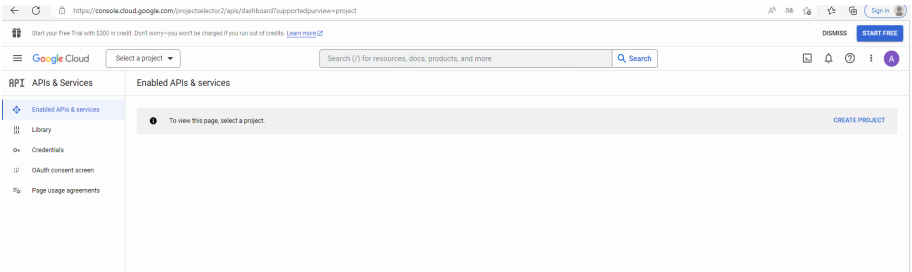


Configuring fixed account authentication

Configure Google authentication

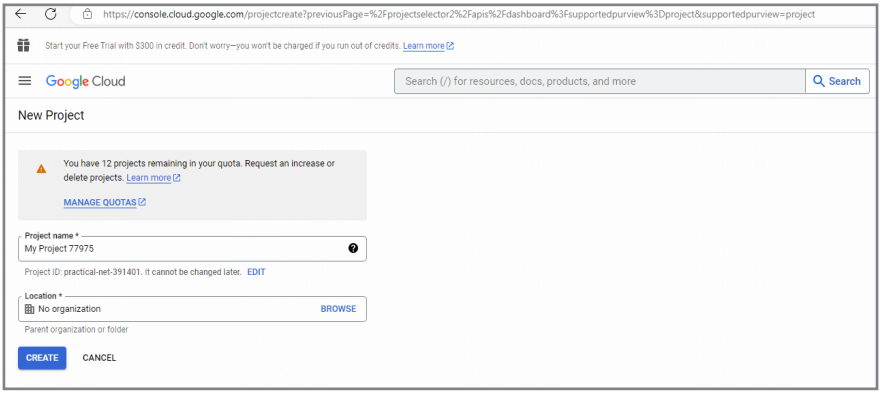
Creating a Google app

1. Log in to Google Cloud Platform at *https://console.cloud.google.com/apis*.
2. Click *CREATE PROJECT* to create a project.



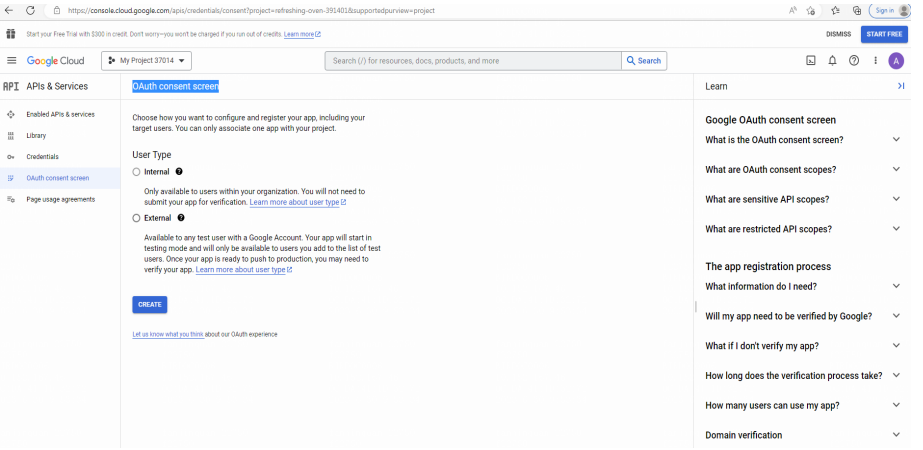
Creating a project

3. Configure the basic project settings, and then click *Create*.



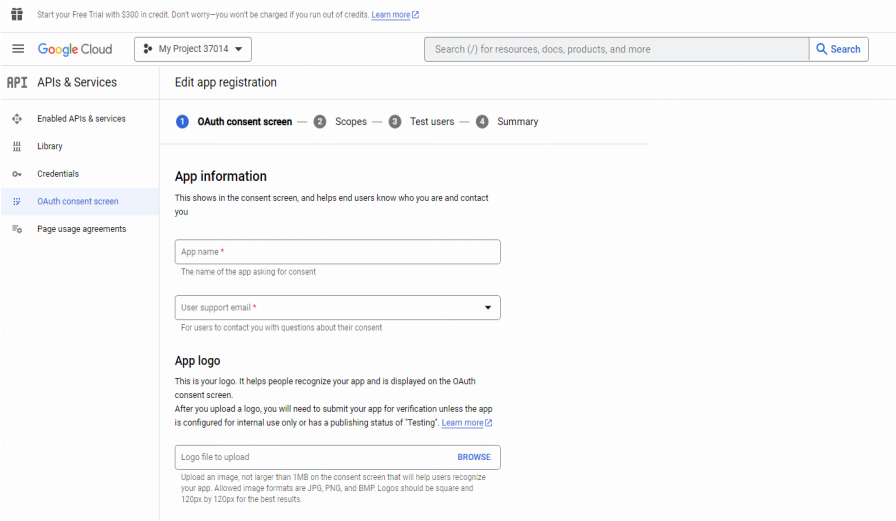
Basic project settings

4. Configure OAuth consent screen settings.
   » Select *External* as the user type.

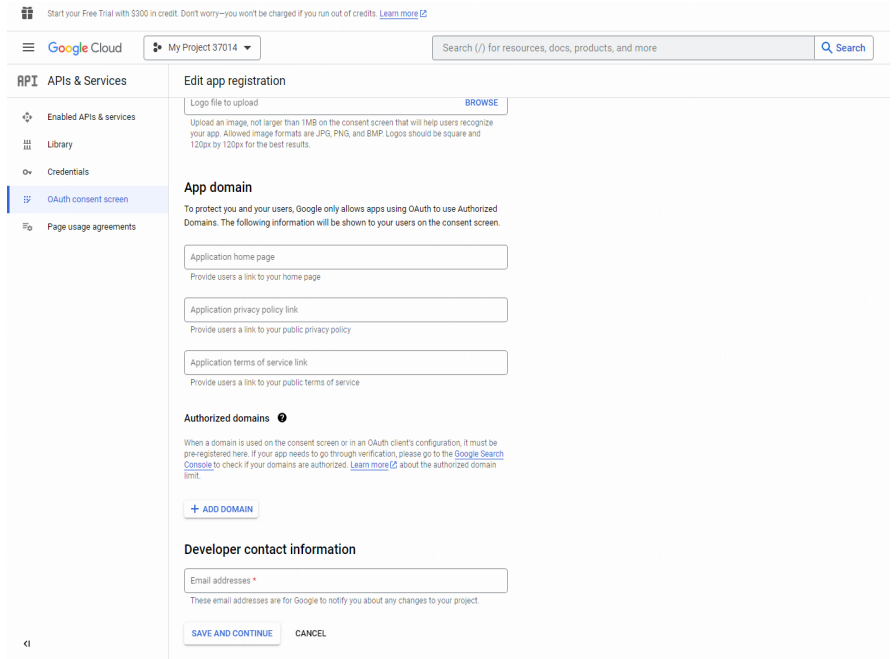


Selecting a user type

» Edit app registration settings

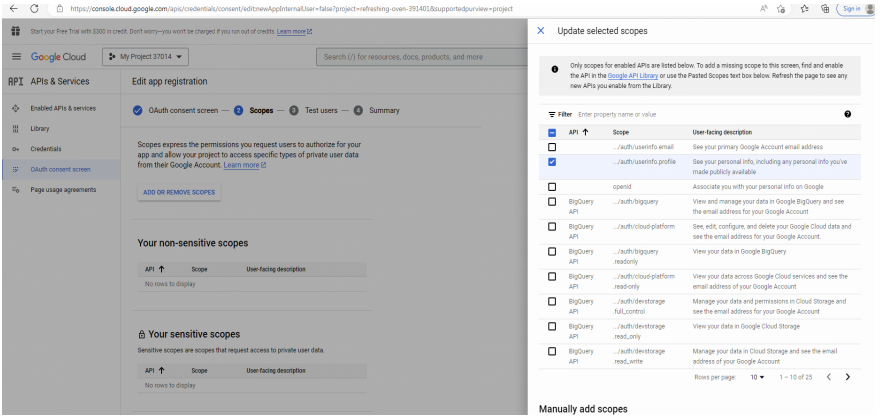


Editing app registration settings 1



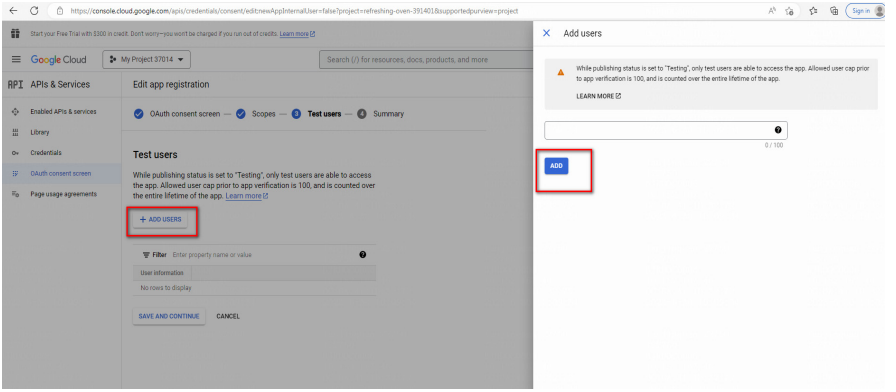
Editing app registration settings 2

» Configure scopes.
You only need to select *userinfo.profile*.



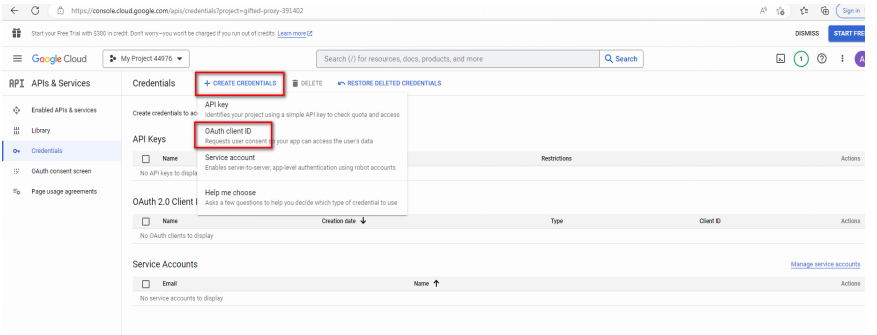
Updating scopes

» Configure test users.
Click *Add Users* to add test users. Only test users can log in to a Google app in Testing state.

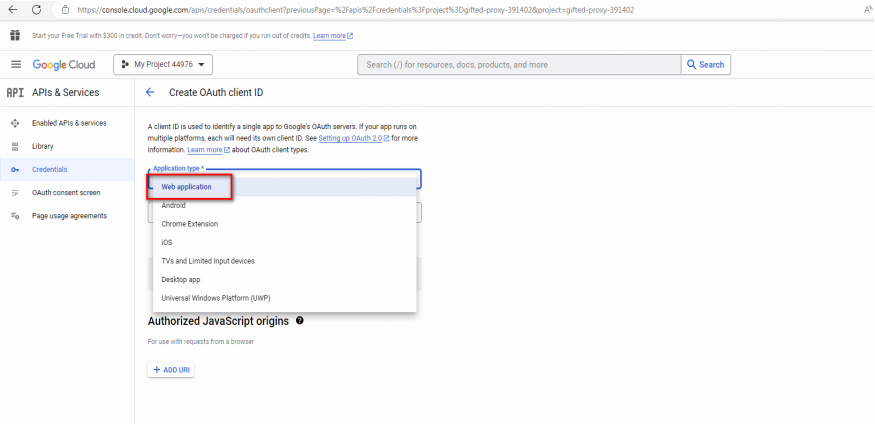


Adding test users

» Create credentials.
» Click *CREATE CREDENTIALS*, and then click *OAuth client ID*.

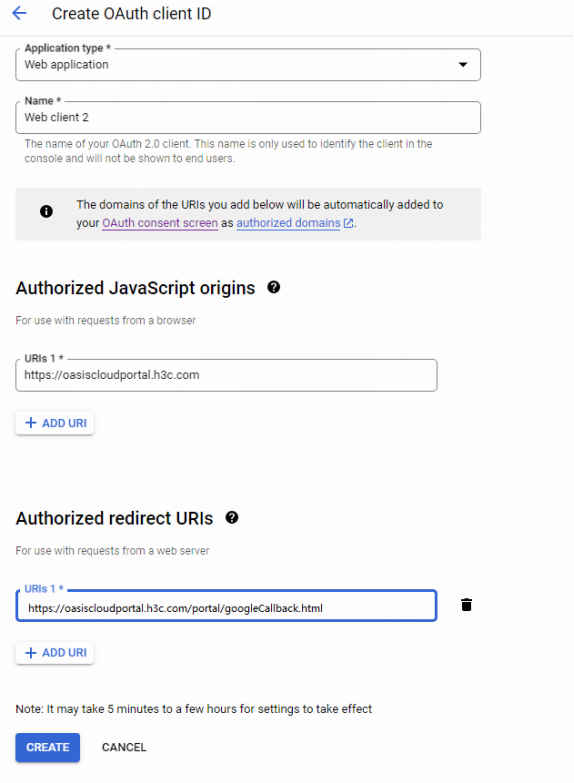


» Select web application as the application type.



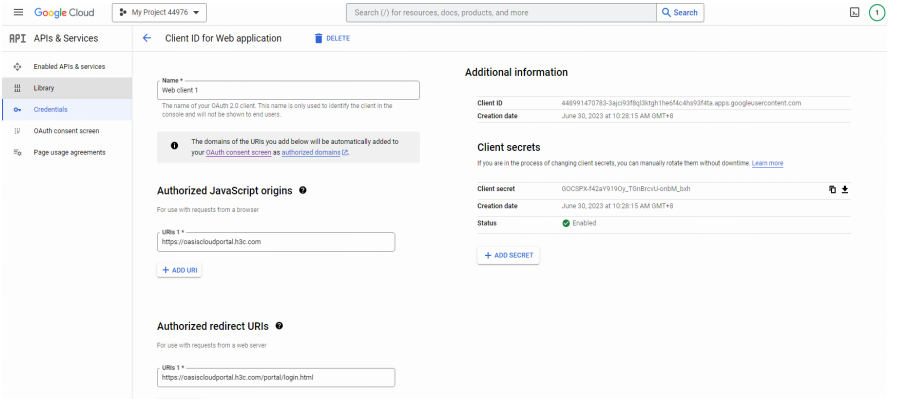
Selecting an application type

» Add authorized JavaScript origins and authorized redirect URIs.
The authorized redirect URI is *https://oasiscloudportal.intelbras.com/portal/googleCallback.html*.
The specified JavaScript origins must start with *https*.



Authorized JavaScript origins and authorized redirect URIs

5. After the credential is created, click *Credentials* on the left navigation pane. In the *OAuth 2.0 Client IDs* list, click *Edit OAuth client* in the *Actions* column for the credential. On the page that opens, you can view the ID and the secret key of the client.



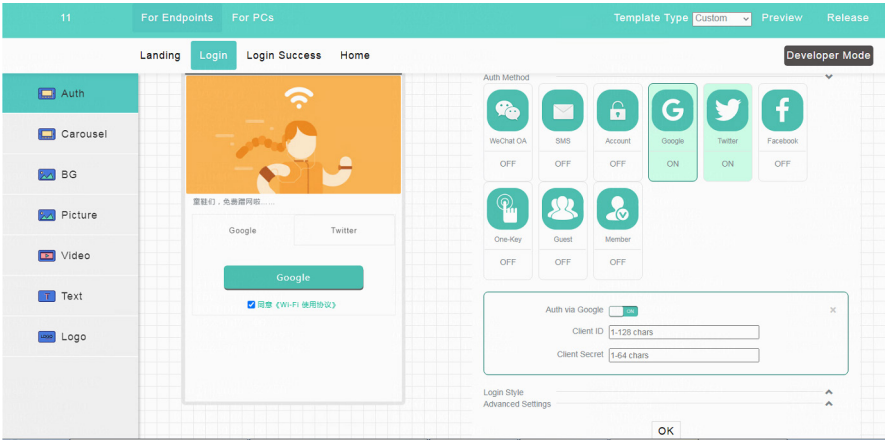
Client information

Configure Google authentication settings on INC Cloud

The Google authentication method can be used in conjunction with:

- SMS authentication.
- Account authentication.
- Member authentication.
- Facebook authentication.
- Twitter authentication.

You can use up to three authentication methods simultaneously.

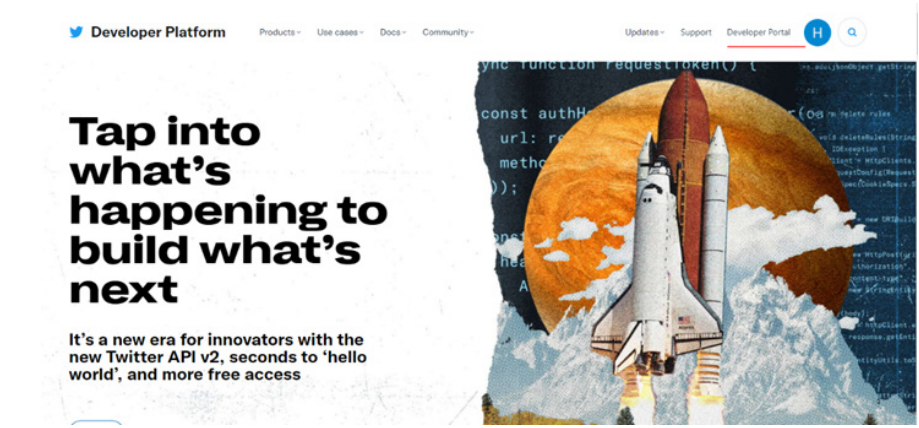


Google authentication

Configure Twitter authentication

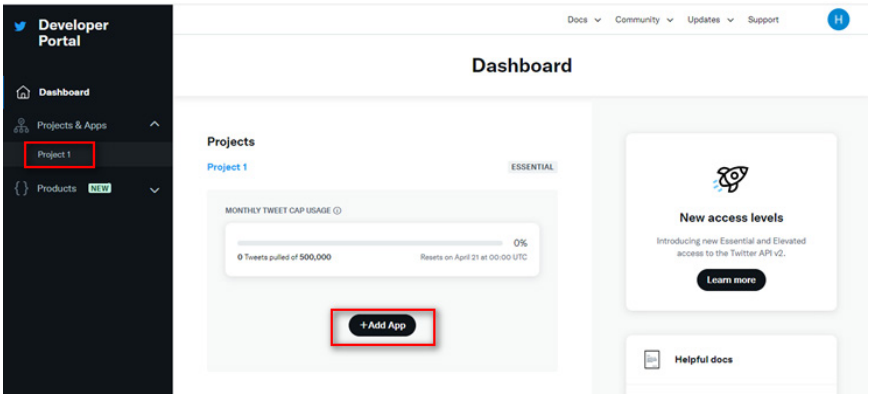
Creating a Twitter app

» Log in to Twitter Developer Platform at *https://developer.twitter.com*.



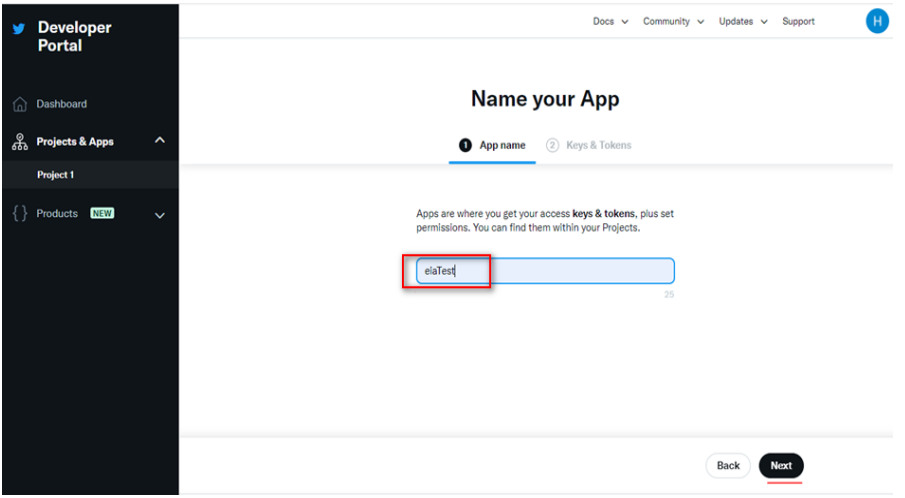
Homepage

» Register for a developer account.



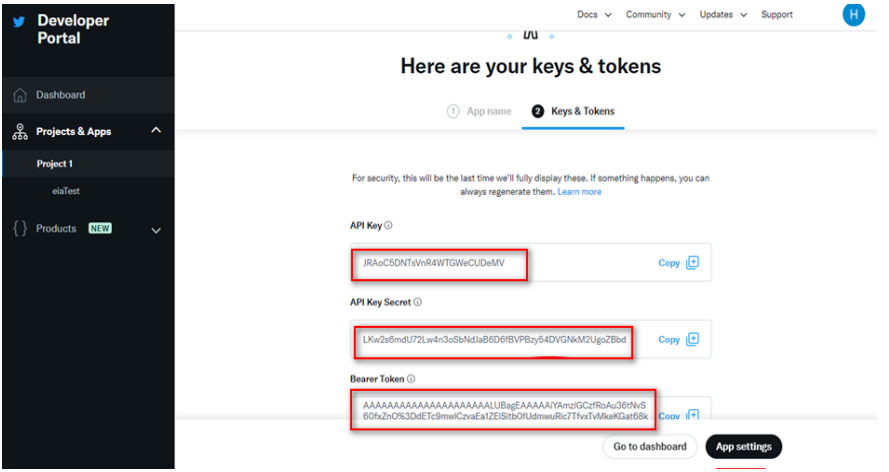
Page for account registration

» Click Developer Portal to create an app on the background.



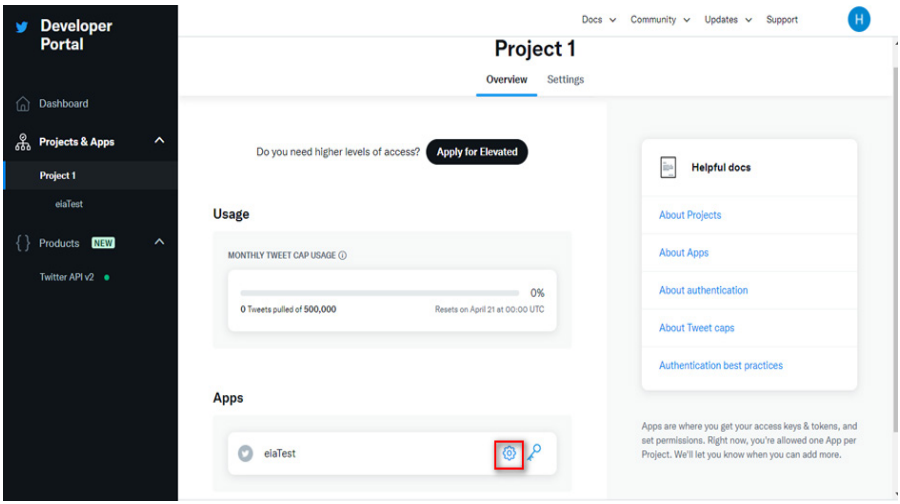
Application naming

» Record the API key, and the API key secret. They will be used later.

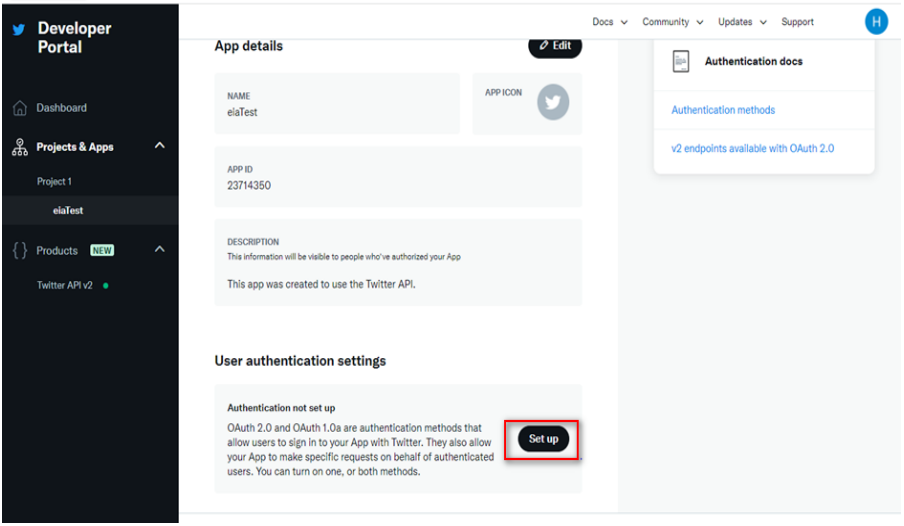


Password

» Configure application settings.
  » Click the *Settings* icon in the *Apps* area.

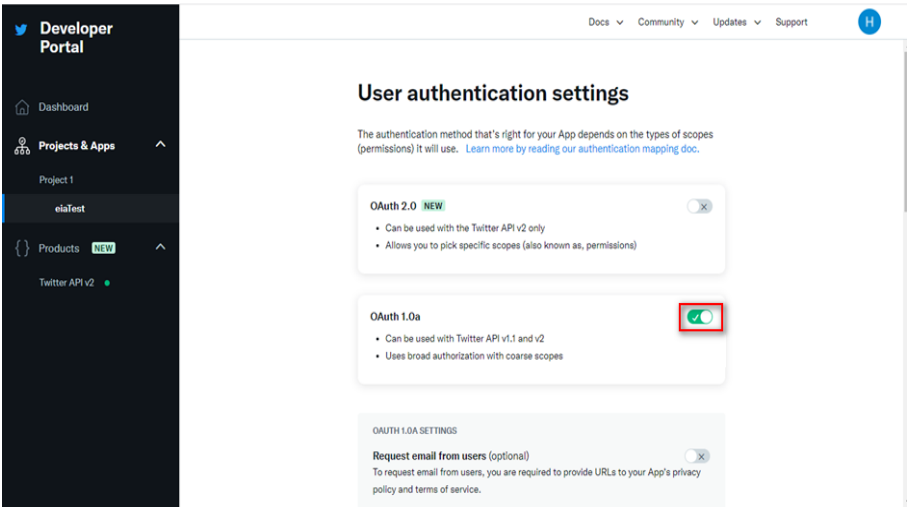


  » Click the **Set up** button in the **User authentication settings** area.



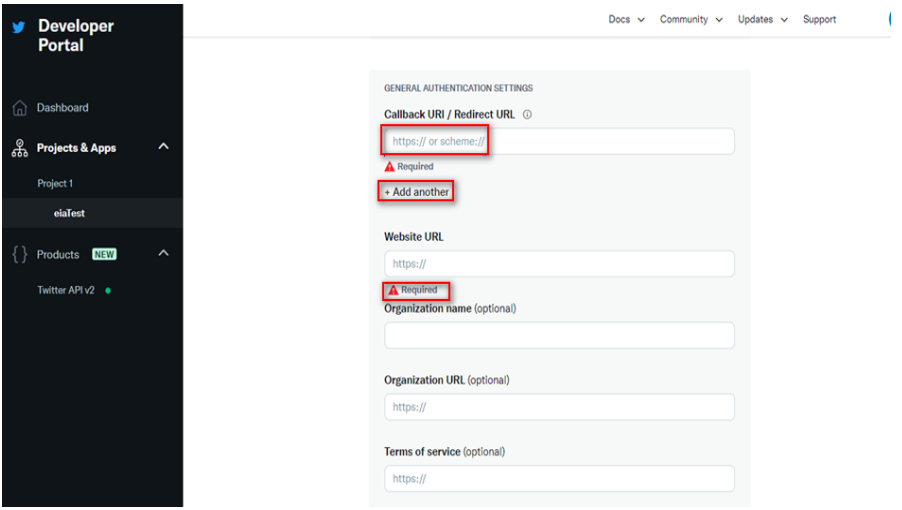
User authentication settings

» Enable Oauth 1.0a.



Enabling Oauth 1.0a.

» Specify a redirect URL and a website URL.
  » **Redirect URL**: *https://oasiscloudportal/portal/twitterCallback.html.*
  » **Website URL**: enter a URL in domain name format.



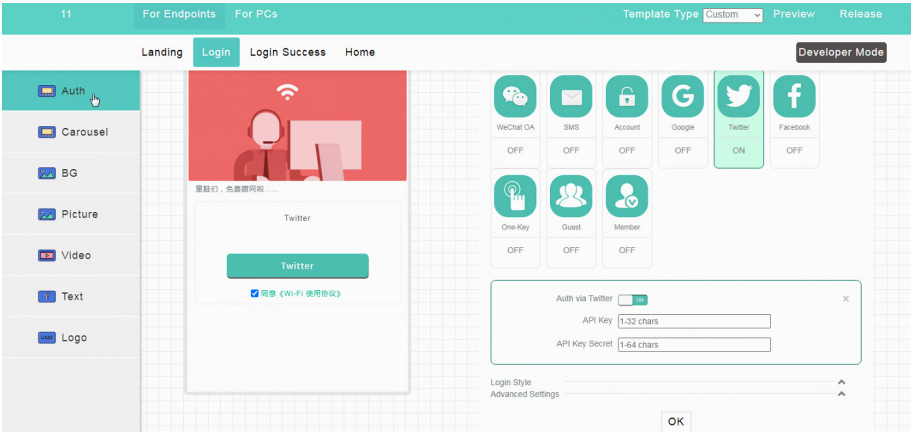
Redirect URL and website URL

Configure Twitter authentication settings on INC Cloud

The Google authentication method can be used in conjunction with:

- SMS authentication.
- Account authentication.
- Member authentication.
- Facebook authentication.
- Google authentication.

You can use up to three authentication methods simultaneously.



Twitter authentication

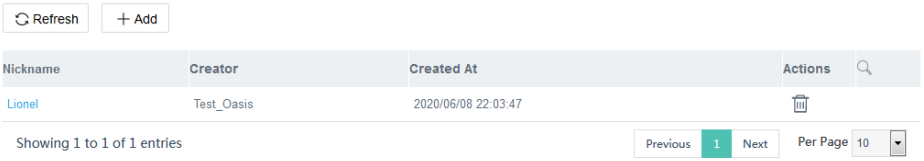
Configure guest authentication

Restrictions and guidelines

After configuration, a guest can access the network only after the approver scans the QR code on the client and authorizes the client. The QR code is valid for five minutes. When the QR code expires, the guest must refresh the QR code.

Procedure

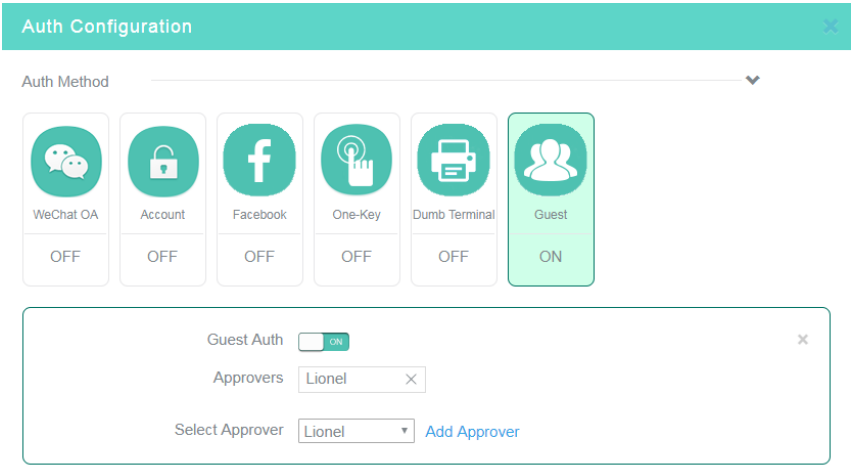
1. On the top navigation bar, click *Service*.
2. Select *Authentication* from the navigation pane, Click the *Accounts* tab.
3. Click the *Guest Accounts* tab, click *Add*.
   An approver is added after the approver scans the QR code, and then enters the verification code. If the approver is deleted, the INC Cloud automatically removes the permission from the approver.



Adding an approver

4. Select *Settings > ACs > Authentication* from the navigation pane, and then select a branch, a site, and a device from the top of the page.
5. To add an authentication template, click *Add* on the *Authentication Templates* tab. To edit an authentication template, click the *Edit* icon for that authentication template.

6. To bind an authentication template to a wireless service, click the *Edit* icon for that authentication template, select *Yes* from the *Bind to Wireless Service* field, and then click *Apply.* If the template has been bound to wireless service, skip this step.
7. Click the *Draw* icon for the target authentication template.
8. Click the *Guest* tile in the *Auth Configuration* area, and then enable guest authentication.
9. Select approvers.
   The *Approvers* field only displays the approvers authorized by this account and all its subaccounts. For tenants, the *Approvers* field displays the approvers authorized by all its subaccounts.
10. Disable other authentication methods.
11. Click *OK* or click *Release* in the upper right corner of the page.



Configuring guest authentication

Configure Facebook authentication

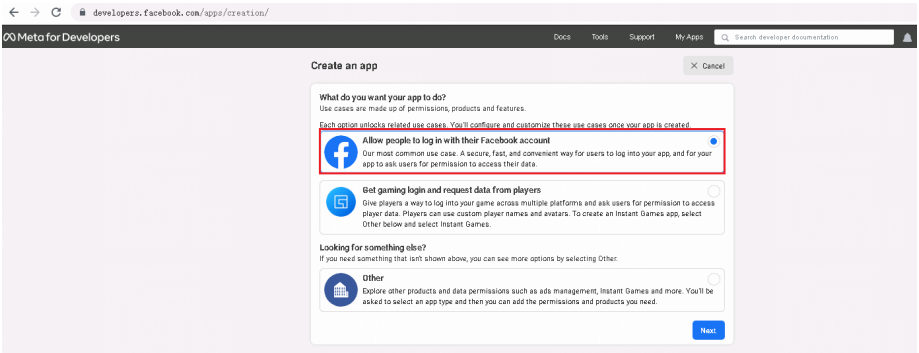
With Facebook authentication enabled, users will be redirected to the Facebook login page for authentication. They can access the network only after granting the INC Cloud to obtain his or her Facebook information (nickname, profile, and email information) from Facebook.

Creating a Facebook app

1. Log in to Meta for Developers at *https://developers.facebook.com.*
2. Click *Create App* to create a Facebook app.

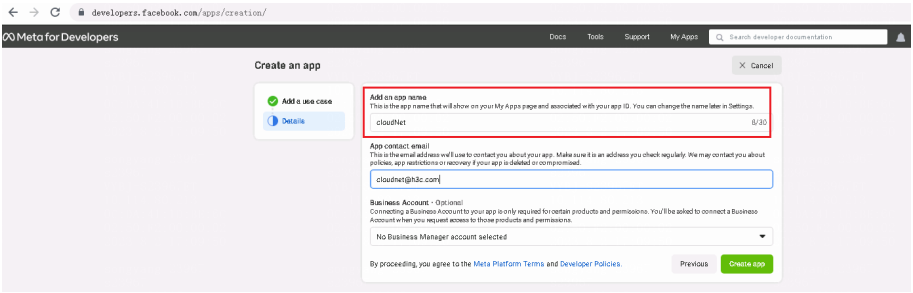
Creating an app

3. Select *Allow people to log in with their Facebook account.*



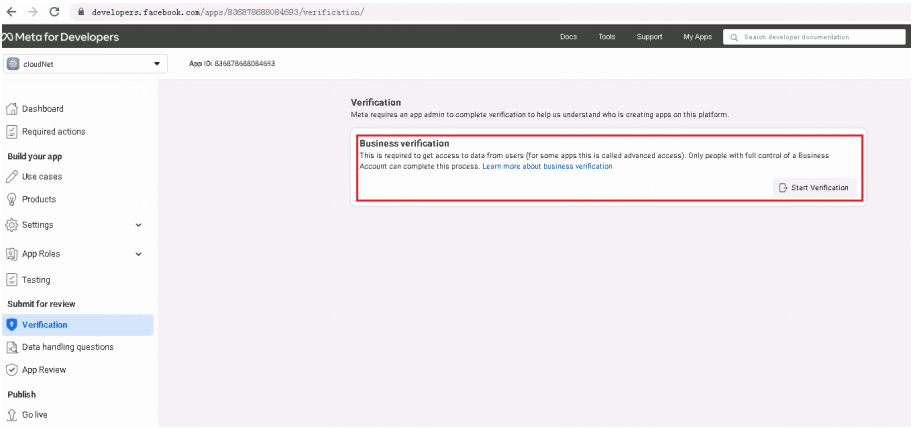
Selecting a use case

4. Specify the app name.



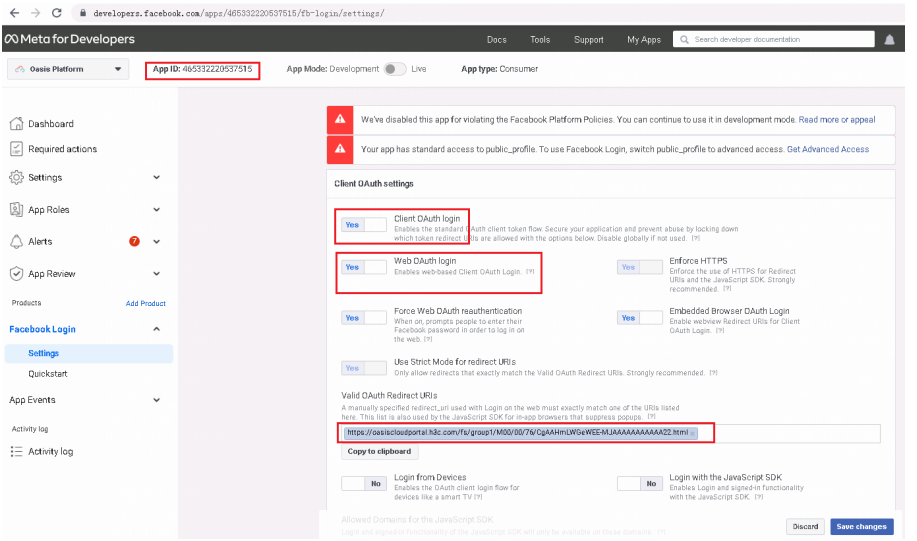
Specifying the app name

5. Start business verification.

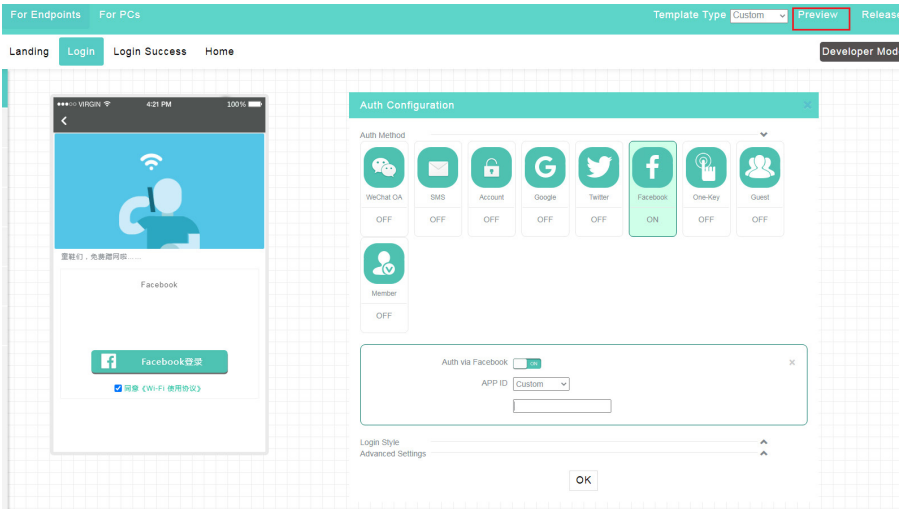


Business verification

6. On Meta for Developers, enable client OAuth login and web OAuth login, and enter the URI of the authentication login page as a valid OAuth redirect URI. To obtain the URI of the authentication login page, access the *Auth Configuration* page of INC Cloud, and click *Preview*.



OAuth settings



Auth configuration page

Authentication login page

Configuring Facebook authentication settings on INC Cloud

1. On the top navigation bar, click *Network*.
2. Select *Settings > ACs > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. To add an authentication template, click *Add* on the Authentication Templates tab.
5. To edit an authentication template, click the *Edit* icon for that authentication template.
6. To bind an authentication template to a wireless service, click the *Edit* icon for that authentication template, select *Yes* from the *Bind to Wireless Service* field, and then click *Apply.* If the template has been bound to a wireless service, skip this step.
7. Click the *Draw* icon for the target authentication template.
8. Click the *Facebook* tile in the *Auth Configuration* area, enable authentication via Facebook, enter the App ID, and disable all the other authentication methods.
9. Click *OK* or click *Release* in the upper right corner of the page.

Configuring Facebook authentication

Configure combined authentication

Restrictions and guidelines

Only the following authentication methods can be used together:

- Fixed account authentication.
- Facebook authentication.

A user can access the network as long as the user passes one authentication.

Procedure

1. Configure settings on the device as described in *Configure settings on the device* if the device software version is below 5405.
2. Configure a minimum of two authentication methods (Details not shown).

Configure dumb terminal authentication

Restrictions and guidelines

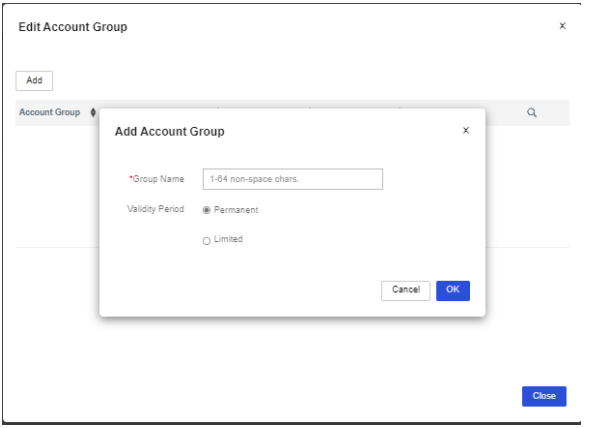
If an account group contains accounts that have been authenticated, changing the validity period of the account group will change the validity period of all the accounts in the group.

If you configure the validity period as 0, the account never expires.

You can enter the first three bytes to add MAC addresses in bulk. The validity period configuration for a complete MAC address and that for a three-byte MAC address are not mutually exclusive. Assume that you add MAC addresses that start with AA-BB-CC and specify a 5-day validity period and then add MAC address *AA-BB-CC-11-22-33* and specify a 10-day validity period. The validity periods of dumb terminals with a MAC address of *AA-BB-CC-11-22-33* and a MAC address that starts with *AA-BB-CC* are 10 and 5 days, respectively.

Procedure

1. On the top navigation bar, click *Service.*
2. Select *Authentication* from the navigation pane, Click the *Accounts* tab.
3. On the *Dumb Terminal Accounts* tab, click *Edit Account Group.*
4. Click *Add.*
5. Enter the required information and then click *OK.*

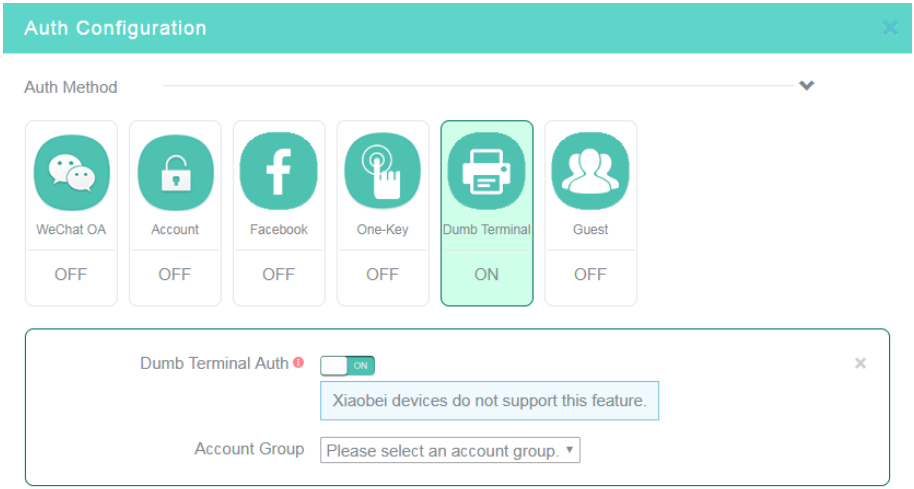


Adding an account group

6. Select an account group and then click *Add*.
7. Enter a MAC address in the required format.

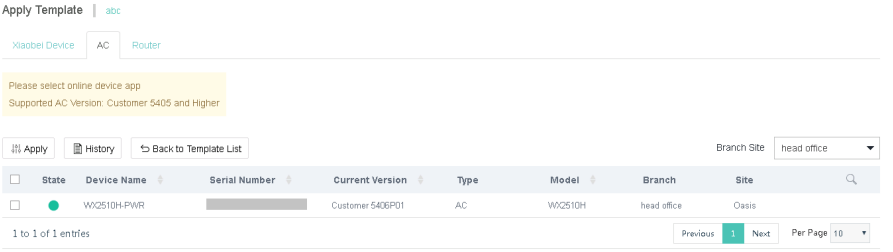
Adding a MAC address

8. Click the *Authentication Templates* tab.
9. To add an authentication template, click *Add*. To edit an authentication template, click the *Edit* icon ... for that authentication template.
10. Click the *Draw i*con for the target authentication template. You are placed on the *Login* tab.
11. Click the *Dumb Terminal* tile in the *Auth Configuration* area, and then enable dumb terminal authentication.
12. Select an account group.
13. Click *OK* or click *Release* in the upper right corner of the page.



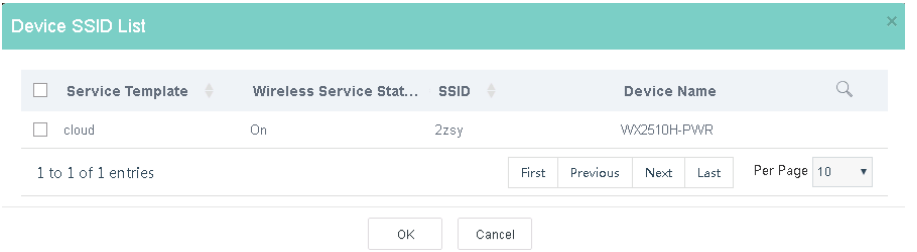
Configuring dumb terminal authentication

14. To deploy a template, perform the following steps:
    - » Click the *Deploy Template* icon for that authentication template.
    - » Click the *ACs* tab.
    - » Select a branch or site.
    - » Select an AC and then click *Apply.*
      If no devices are displayed, please check the device version.



Deploying a template

- » Select a service template or an SSID, and then click *OK.*



Selecting a service template

15. Enable MAC-triggered authentication on the device. For more information, see *Configure MAC--trigger authentication.*

Configure bulk authentication

Perform this task to deploy authentication settings in bulk.

Restrictions and guidelines

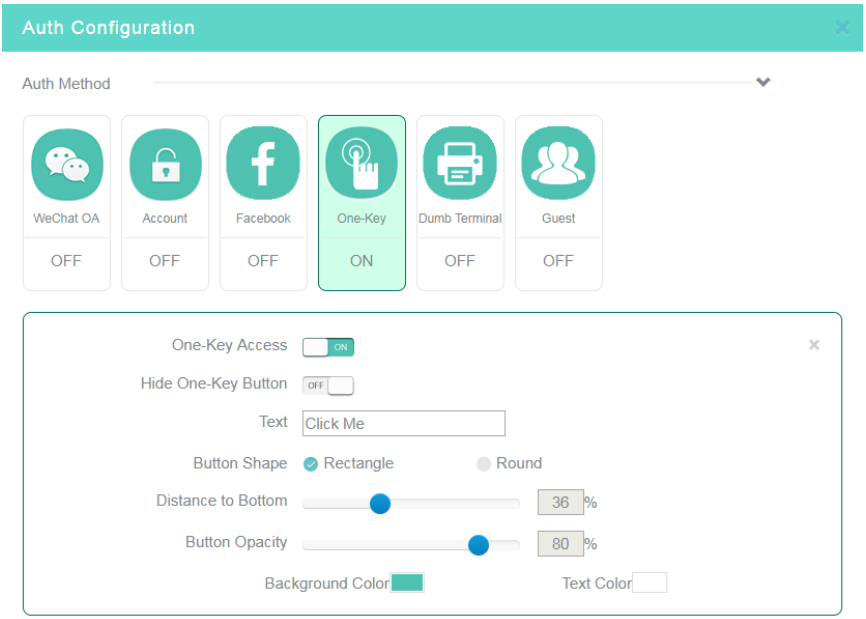
The configuration of a bulk authentication template takes precedence over that of a non-bulk authentication template. For the non-bulk authentication template to take effect, click the *Edit* icon for that authentication template, and then click *Apply.*

Before deploying the configuration in bulk, make sure the following requirements are met:

- » The devices where bulk authentication is deployed are online. If a device is offline, the deployment fails. The device will load the most recent deployed configurations at start up.
- » The software version must be 5405 or higher.
- » The wireless service name is the same as the portal Web server.

Procedure

1. On the top navigation bar, click *Service*.
2. Select *Authentication* from the navigation pane..
3. On the *Authentication Templates* tab, click *Add*.
4. Click the *Draw* icon for the target authentication template. For the detailed configuration procedures of different authentication methods, see *Configure basic settings*.

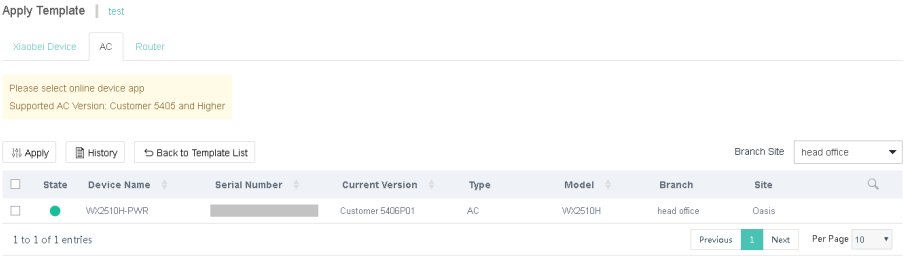


Configuring bulk authentication

5. To deploy a template, perform the following steps:

   » Click the *Deploy Template* icon for that authentication template.
   » Click the *ACs* tab.
   » Select a branch or site.
   » Select an AC and then click *Apply*.

   If no devices are displayed, please check the device version.



Deploying a template

Customize an authentication page

You can configure the landing page, login page, login success page, and home page and can push or disable the landing page or login success page as needed.

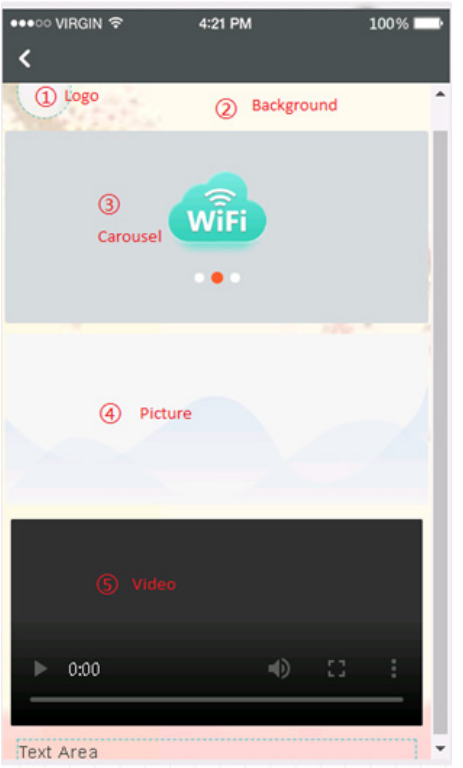
Restrictions and guidelines

The picture size cannot exceed 1 M. As a best practice, set the picture size to be in the range of 100 KB to 200 KB. Only JPG, JPEG, BMP, PNG, GIF, and SVG formats are allowed.

As a best practice to avoid affecting the loading speed of the page, do not add too many controls.

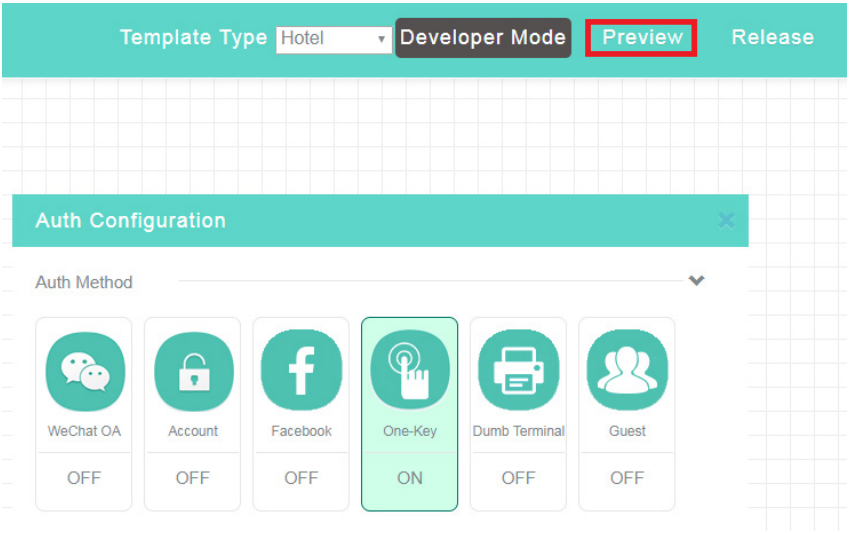
Procedure

1. On the top navigation bar, click *Service*.
2. Select *Authentication* from the navigation pane..
3. On the *Authentication Templates* tab, click the *Draw* icon for the target authentication template.
4. Configure the following settings as shown in *Figure Previewing the configuration change:*
   - » **Logo:** the aspect ratio must be 1:1. The picture will be automatically cut into a circle. You can enter a shop name with a length of less than 12 characters.
   - » **Background:** the aspect ratio must be 3:5.
   - » **Carousel:** the aspect ratio must be 11:5. Two or three pictures of the same height are required.
   - » **Picture:** the aspect ratio must be 11:5. The description for the picture cannot exceed 48 characters.
   - » **Video:** the video size cannot exceed 5 M. Only MP4, WEBM, and OGG formats are allowed.
   - » **Text:** you can edit the font, font size, bold type, and font color.



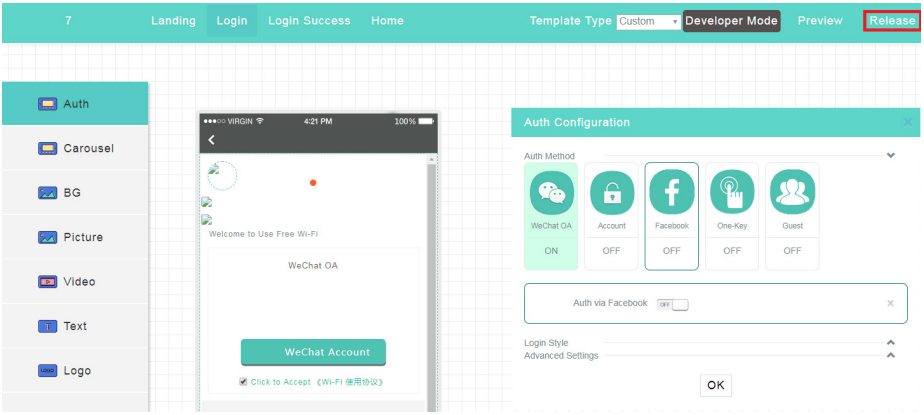
Custom template description

5. To configure the homepage, click the Home tab, and then select *Use Custom Link.*
6. Enter a custom link and then click Upload.
7. To preview the link, click *Preview* in the upper right corner of the page.



Previewing the configuration change

8. Click *Release* in the upper right corner of the page.
   The homepage pushed to users during portal authentication will be replaced by the page redirected by this custom link.



Configuring the custom template

2.2. Configure advanced settings

The INC Cloud provides advanced authentication settings to simplify authentication management, reduce cost, and optimize market promotion. *Table Advanced INC Cloud authentication features* describes available advanced features for each authentication method. You can configure these settings as needed.

Advanced INC Cloud authentication features:

Authentication method	Advanced features
One-key authentication	Captive-bypass Hiding and customizing one-key authentication button Internet access settings Authentication free Inter-site and inter-SSID re-authentication Internet access control Developer mode Domain name whitelist and blacklist Viewing and exporting history of authentication configuration deployment
Fixed-account authentication	Captive-bypass Bulk management of fixed accounts Self-service password change Collaboration with LDAP server Changing visual effects of the login page Internet access settings Authentication free Inter-site and inter-SSID re-authentication Internet access control Developer mode Domain name whitelist and blacklist Viewing and exporting history of authentication configuration deployment
Guest authentication	Captive-bypass Internet access settings Authentication free Inter-site and inter-SSID re-authentication Internet access control Developer mode Domain name whitelist and blacklist Viewing and exporting history of authentication configuration deployment
Facebook authentication	Captive-bypass Changing visual effect settings of the login page Internet access settings Inter-site and inter-SSID re-authentication Internet access control Developer mode Domain name whitelist and blacklist Viewing and exporting history of authentication configuration deployment
Dumb terminal authentication	Captive-bypass Management of dumb terminal account groups Internet access control Developer mode Domain name whitelist and blacklist Viewing and exporting history of authentication configuration deployment

Enable the captive-bypass feature

Typically, the device pushes the authentication page to a client automatically when the client attempts to access a portal authentication network. The captive-bypass feature enables the device to push the portal authentication page to the client only when the user launches a browser.

To enable the captive-bypass feature, you must perform the following steps on the device:

1. Enter system view.
   system-view
2. Enter portal Web server view of Web server **cloud**.
   Portal web-server cloud
3. Enable the captive-pass feature.
   Captive-bypass enable

Hide or customize the one-key authentication button

Perform this task to hide the one-key authentication button or change the button style. If the button is hidden, users pass the authentication automatically after the countdown timer on the login page expires.

Restrictions and guidelines

You can change the button style only when the button is not hidden.

Procedure

1. On the top navigation bar, click *Network*.
2. Select *Settings > ACs > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Draw* icon  for the target authentication template.
5. Click the *One-Key* tile in the *Auth Configuration* area, and then hide or customize the button as needed.

Manage fixed accounts

Perform this task to delete, import, or export fixed accounts in bulk.

To manage fixed accounts:

1. On the top navigation bar, click *Network*.
2. Select *Settings > ACs > Users* from the navigation pane.
3. Click the *Fixed Accounts* tab.
4. To delete fixed accounts, select the target fixed accounts and then click *Delete*.
5. To import fixed accounts, click *Import,* download the template file and fill in the file as required, and then upload the template file.
6. To export fixed accounts, click *Export*.

Enable self-service password change

This feature enables users to change passwords at login. With this feature disabled, only the administrators can change the passwords of fixed accounts.

To enable self-service password change:

1. On the top navigation bar, click *Networkt*.
2. Select *Settings > ACs > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Draw* icon  for the target authentication template.
5. Click the *Account* tile in the *Auth Configuration* area.
6. Enable *Change Password*.

Enable collaboration with an LDAP server for fixed account verification

Perform this task to enable the INC Cloud to report usernames and passwords to the LDAP server for verification when users attempt to access the WLAN by using fixed accounts. This frees network administrators from importing account information from the LDAP server to the INC Cloud.

Restrictions and guidelines

To use this feature, make sure the LDAP server has been configured.

Procedure

1. On the top navigation bar, click *Network*.
2. Select *Settings > ACs > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Draw* icon for the target authentication template.
5. Click the *Account* tile in the *Auth Configuration* area.
6. Enable *LDAP* and configure LDAP settings as needed.
7. Click *LDAP Config Verification* to verify the LDAP settings.

Change visual effect settings of the login page

Perform this task to customize the background color, background opacity, and text color on the login page.

Restrictions and guidelines

Caution:

Restoring default settings will remove all user-defined visual effect settings and the restore operation is irreversible. Please use this feature with caution.

Visual effect settings of authentication methods take effect only when multiple authentication methods are enabled.

Procedure

1. On the top navigation bar, click *Network*.
2. Select *Settings > ACs > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Draw* icon for the target authentication template.
5. Click to expand the *Login Style* menu in the *Auth Configuration* area.
6. Configure the background color, background opacity, and text color as needed.
7. The adjustment will be displayed in the preview area in real time. To restore the default visual effect settings, click *Restore Default*.

Configure Internet access settings

Procedure

1. On the top navigation bar, click *Network*.
2. Select *Settings > ACs > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Draw* icon for the target authentication template.
5. Click to expand the *Advanced Settings* menu in the *Auth Configuration* area.
6. Configure Internet access settings as needed.

Parameters

- **Session Timeout**: maximum continuous online duration of a client upon one authentication. A client will be logged off when its continuous online duration exceeds the timeout. The session timeout cannot be larger than the daily online duration.
- **Daily Online Duration**: maximum online duration of a client for a day. A client will be logged off when its online duration for a day exceeds the limit. The daily online duration cannot be smaller than the session timeout.
- **Minimum Traffic and Idle Timer**: logs off a client if its traffic within an idle timer fails to reach the minimum traffic threshold. Setting the idle timer to 0 disables the idle timer feature.

Note:

As a best practice, set the idle timer to a value no larger than half of the clients' IP address lease, enabling entries of offline clients to be deleted in time.

- **Client Rate Limit**: limited rate of uplink and downlink client traffic. This feature is supported in versions higher than 5417P01.
- **HTTPS for Landing and Login**: use HTTPS sessions for the Landing and Login page.
- **Permit PC**: Permit PCs to access the WLAN. Facebook authentication does not support this feature.

Manage dumb terminal account groups

Perform this task to create, delete, or edit dumb terminal account groups and import or export dumb terminal accounts.

If you enable dumb terminal authentication and specify an account group, only dumb terminals in the group can access the WLAN.

To manage dumb terminal account groups:

1. On the top navigation bar, click *Service.*
2. Select *Authentication* from the navigation pane Click the *Accounts* tab.
3. On the *Dumb Terminal Accounts* tab, configure dumb terminal account groups.

Configure portal automated authentication

This feature allows users that have been authenticated to access the network without re-authentication within the auth-free period. The following modes are available:

- **Portal redirection**: in this mode, users must run a browser to trigger automatic portal authentication. This mode supports pushing ads to clients.
- **MAC-trigger**: in this mode, users can access the WLAN without running a browser. This mode does not support pushing ads to clients.

Configure portal redirection authentication

1. On the top navigation bar, click *Networkt.*
2. Select *Settings > ACs > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Draw* icon for the target authentication template.
5. Click to expand the *Advanced Settings* menu in the *Auth Configuration* area.
6. Click the *Auth-Free* tab and configure the *Free Auth* feature.

Configure MAC-trigger authentication

1. Configure portal redirection authentication. For more information, see *Configure portal redirection authentication.*
2. Configure MAC-trigger authentication on the device:
   » Configure the MAC binding server.

Note:
Perform this step only in versions earlier than 5405. Version 5405 and later support automatic authentication setting deployment to devices and do not need manual configuration of commands in this step.

 # Create a MAC binding server and enter its view.

<Sysname> system-view

[Sysname] portal mac-trigger-server cloud

 # Enable cloud MAC-trigger authentication. Set the maximum number of MAC binding query attempts to 2 and the query interval to 3 seconds.

[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

» Apply MAC binding server **cloud** to service template **cloud**.
[Sysname] wlan service-template cloud

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

Configure inter-site and inter-SSID re-authentication

This feature allows clients that have been authenticated to roam between wireless services associated with different sites or different SSIDs for the same site without re-authentication. These wireless services must use the same authentication template or have the same SSID.

Restrictions and guidelines

This feature is available only for authentication templates configured in the App Center.

Procedure

1. On the top navigation bar, click *Service.*
2. Select *Authentication* from the navigation pane.
3. Click the *Draw* icon for the target authentication template.
4. Click to expand the *Advanced Settings* menu in the *Auth Configuration* area.
5. Click the *Auth-Free* tab and enable *Free Auth.*
6. Configure inter-site and inter-SSID re-authentication.

Configure Internet access control

Perform this task to specify the time ranges during which users are allowed to access the WLAN.

Restrictions and guidelines

Internet access control is on a per-hour basis. You can specify a maximum of five time ranges for a day. To specify a time range that ends at 24 o'clock, set the end time to 00. If you set a time range to 00 to 00 for a day, users can access the Internet at any time that day.

Procedure

1. On the top navigation bar, click *Network.*
2. Select *Settings > ACs > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Draw* icon for the target authentication template.
5. Click to expand the *Advanced Settings* menu in the *Auth Configuration* area.
6. Click the *Internet Access Control* tab and specify the time ranges.

Configure the developer mode

Caution:
Editing the codes of existing functions might disable INC Cloud authentication. Please use this feature with caution.

The developer mode allows users to modify the source codes of an authentication template for customization purposes.

Procedure

1. On the top navigation bar, click *Network*.
2. Select *Settings > ACs > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Draw* icon for the target authentication template.
5. Click *Developer Mode* in the upper right corner.

Configure the domain name whitelist and blacklist

Restrictions and guidelines

This feature takes effect only when wireless authentication is configured.

Procedure

1. On the top navigation bar, click *Network*.
2. Select *Settings > ACs > Authentication* from the navigation pane.
3. Click the *Domain Name Whitelist or Domain Name Blacklist* tab to configure the whitelist or blacklist.

View or export history of authentication template deployment

Perform this task to view the history of all authentication template deployment or deployment in the current day, past 7 days, or past 30 days.

To view or export history of authentication template deployment:

1. On the top navigation bar, click *Service*.
2. Select *Authentication* from the navigation pane.
3. On the *Authentication Templates* tab, click the *Apply* icon for the target authentication template.
4. Click the *ACs* tab to view the deployment history for an AC.

3. Configure INC Cloud authentication with a wireless router as the authenticator

Important:
The platform's internal captive portal does not yet support the IPv6 protocol and is only compatible with the IPv4 standard. Therefore, to ensure the proper operation of this feature, it is recommended to configure the captive authentication LAN to operate using only the IPv4 standard.

3.1. Configure basic settings

Prerequisites

Before configuring INC Cloud authentication, complete the following tasks:

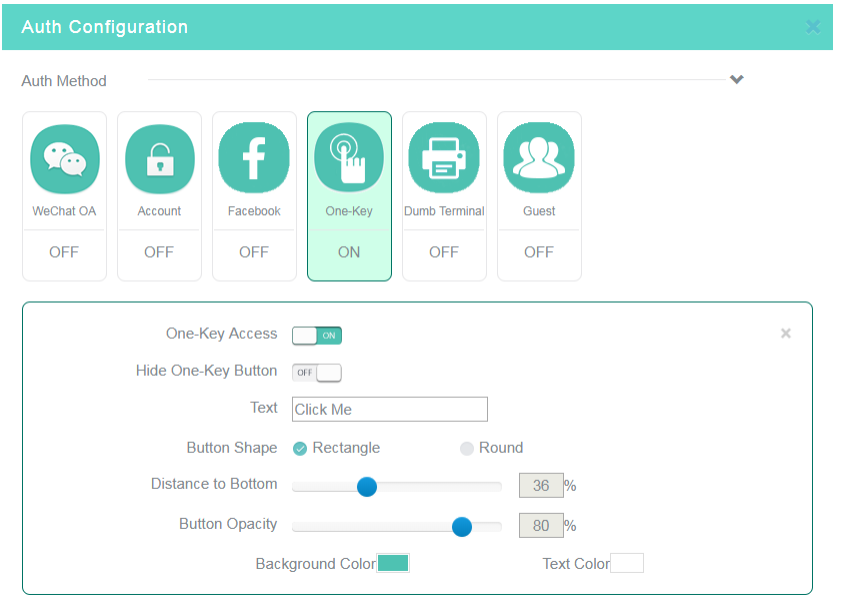
» Connect the device to the INC Cloud.
For more information, see *Intelbras INC Cloud Deployment Guide*.

» Complete the VLAN and DHCP settings.

» Configure wireless services and make sure the APs can come online.

Configure one-key authentication

1. On the top navigation bar, click *Network.*
2. Select *Settings > Routers > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. To add an authentication template, click *Add* on the *Wireless* Authentication Templates tab.
5. To edit an authentication template, click the *Edit* icon for that authentication template.
6. To bind an authentication template to a wireless service, click the *Edit* icon for that authentication template, select *Yes* from the *Bind to Wireless Service* field, and then click *Apply.* If the template has been bound to wireless service, skip this step.
7. Click the *Draw* icon for the target authentication template.
8. Click the *One-Key* tile in the *Auth Configuration* area, enable one-key authentication, and then configure other settings as needed.
9. Click *OK* or click *Release* in the upper right corner of the page.



Configuring one-key authentication

Configure fixed account authentication

Restrictions and guidelines

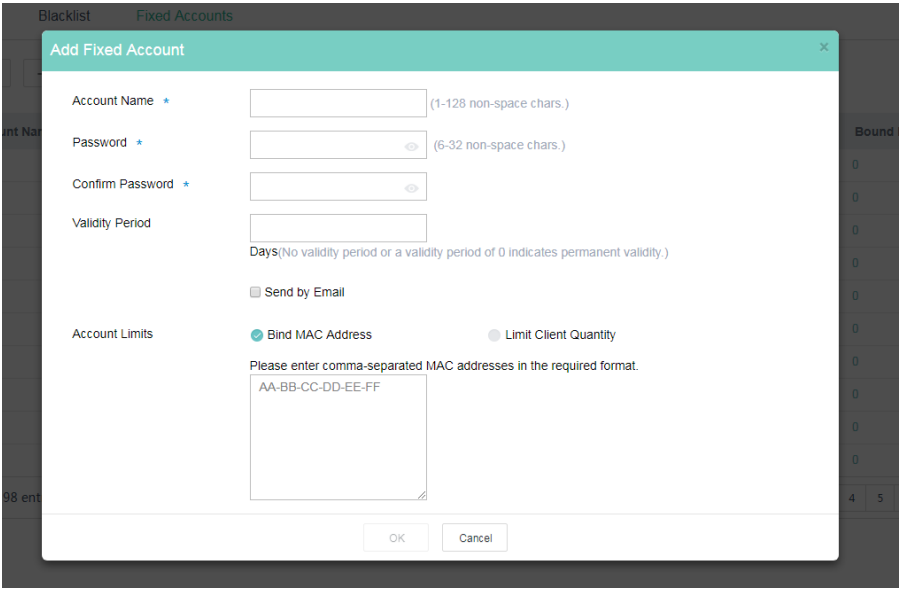
If you do not configure the validity period or configure it as 0, the account never expires.

If you select *Bind MAC Address* and do not enter any MAC addresses, clients that use the fixed account are not limited.

If you select *Sent by Email,* the system sends the account name and password to the specified email address. The number of email addresses cannot exceed 10 and must be separated by commas.

Procedure

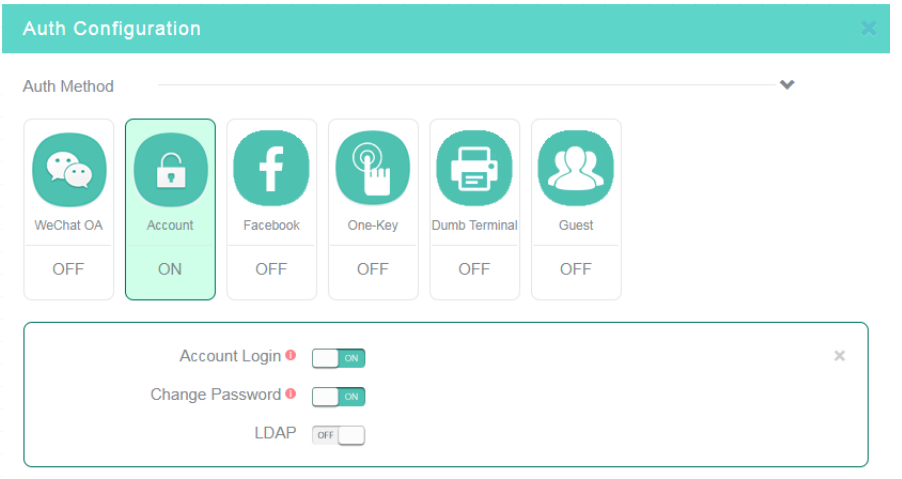
1. On the top navigation bar, click *Network*.
2. Select *Settings > Routers > Users* from the navigation pane.
3. Click the *Fixed Accounts* tab.
4. Click *Add*.
5. Configure fixed account information as required.



Adding a fixed account

6. To add or edit an authentication template, select *Settings > Routers > Authentication* from the navigation pane and then select a branch, a site, and a device from the top of the page. To add a template, click *Add* on the *Wireless Authentication Templates* tab. To edit a template, click the *Edit* icon for that authentication template.
7. To bind an authentication template to a wireless service, click the *Edit* icon for that authentication template, select *Yes* from the *Bind to Wireless Service* field, and then click *Apply*. If the template has been bound to wireless service, skip this step.
8. Click the *Draw* icon for the target authentication template.
9. Click the *Account* tile in the *Auth Configuration* area, enable fixed account authentication, and then configure other settings as needed.
10. Disable other authentication methods.

11. Click *OK* or click *Release* in the upper right corner of the page.



Configuring fixed account authentication

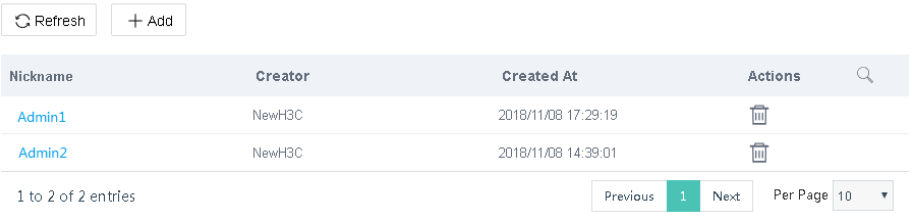
Configure guest authentication

Restrictions and guidelines

After configuration, a guest can access the network only after the approver scans the QR code on the client and authorizes the client. The QR code is valid for five minutes. When the QR code expires, the guest must refresh the QR code.

Procedure

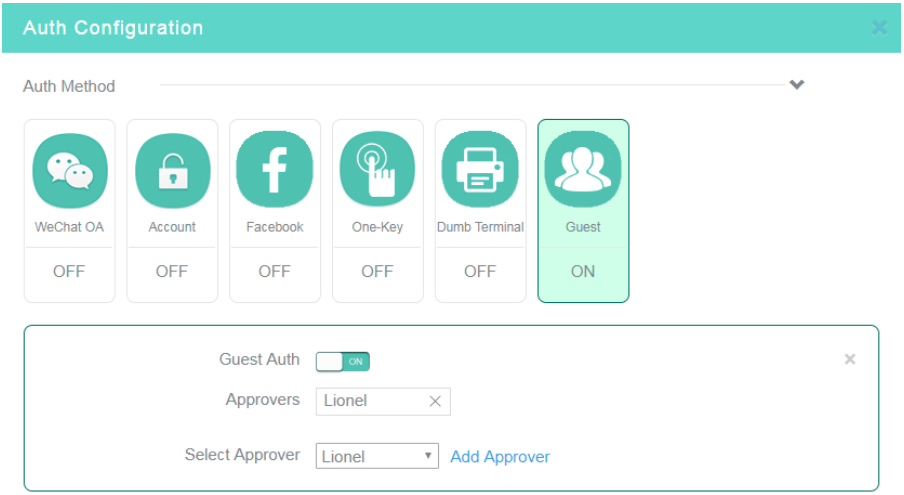
1. On the top navigation bar, click *Service*.
2. Select *Authentication* from the navigation pane Click the *Accounts* tab
3. Click the *Guest Accounts* tab, click *Add*.
   An approver is added after the approver scans the QR code, and then enters the verification code. If the approver is deleted, the INC Cloud automatically removes the permission from the approver.



Adding an approver

4. Select *Settings > Routers > Authentication* from the navigation pane, and then select a branch, a site, and a device from the top of the page.
5. To add an authentication template, click *Add* on the *Wireless Authentication Templates* tab. To edit an authentication template, click the *Edit* icon for that authentication template.
6. To bind an authentication template to a wireless service, click the *Edit* icon for that authentication template, select *Yes* from the *Bind to Wireless Service* field, and then click *Apply*. If the template has been bound to wireless service, skip this step.
7. Click the *Draw* icon for the target authentication template.

8. Click the *Guest* tile in the *Auth Configuration* area, and then enable guest authentication.
9. Select approvers.
10. The *Approvers* field only displays the approvers authorized by this account and all its subaccounts. For tenants, the *Approvers* field displays the approvers authorized by all its subaccounts.
11. Disable other authentication methods.
12. Click *OK* or click *Release* in the upper right corner of the page.



Configuring guest authentication

Configure combined authentication

Restrictions and guidelines

Only the following authentication methods can be used together:

- Fixed account authentication.
- Facebook authentication.

A user can access the network as long as the user passes one authentication.

Procedure

Configure a minimum of two authentication methods. (Details not shown.)

Configure dumb terminal authentication

Restrictions and guidelines

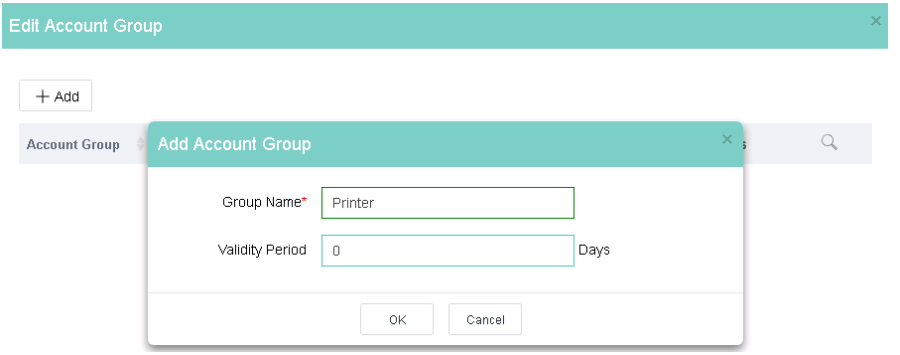
If an account group contains accounts that have been authenticated, changing the validity period of the account group will change the validity period of all the accounts in the group.

If you configure the validity period as 0, the account never expires.

You can enter the first three bytes to add MAC addresses in bulk. The validity period configuration for a complete MAC address and that for a three-byte MAC address are not mutually exclusive. Assume that you add MAC addresses that start with *AA-BB-CC* and specify a 5-day validity period and then add MAC address *AA-BB-CC-11-22-33* and specify a 10-day validity period. The validity periods of dumb terminals with a MAC address of *AA-BB-CC-11-22-33* and a MAC address that starts with *AA-BB-CC* are 10 and 5 days, respectively.

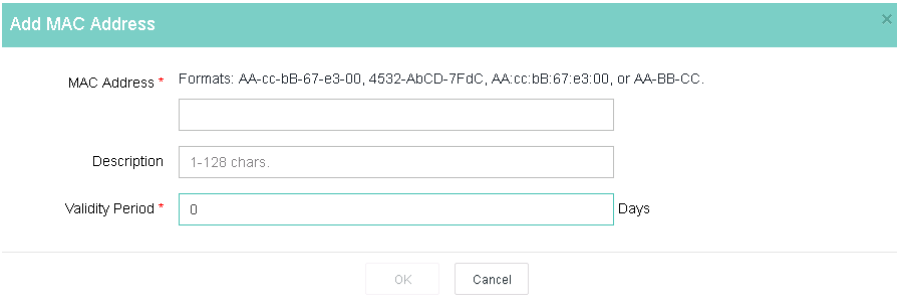
Procedure

1. On the top navigation bar, click *Service*.
2. Select *Authentication* from the navigation pane, Click the *Accounts* tab
3. On the *Dumb Terminal Accounts* tab, click *Edit Account Group*.
4. Click *Add*.
5. Enter the required information and then click *OK*.



Adding an account group

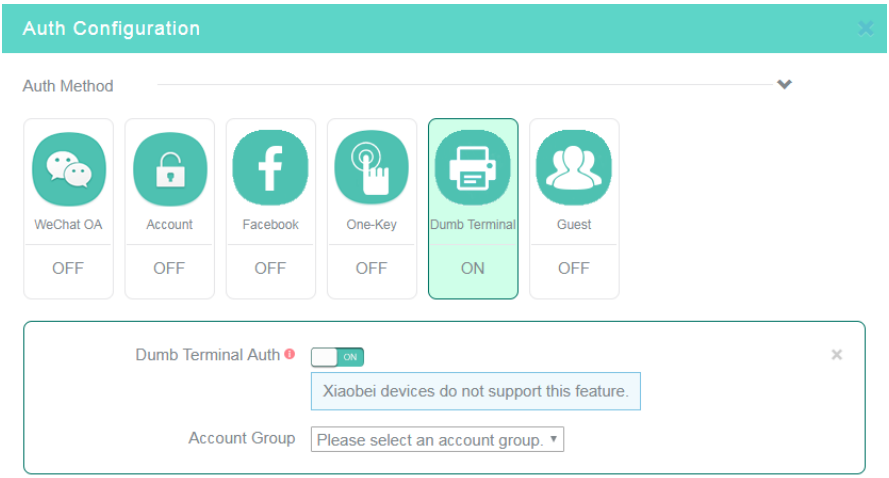
6. Select an account group and then click *Add*.
7. Enter a MAC address in the required format.



Adding a MAC address

1. Click the *Authentication Templates* tab.
2. To add an authentication template, click *Add*. To edit an authentication template, click the *Edit* icon for that authentication template.
3. Click the *Draw* icon for the target authentication template. You are placed on the **Login** tab.
4. Click the *Dumb Terminal* tile in the *Auth Configuration* area, and then enable dumb terminal authentication.
5. Select an account group.

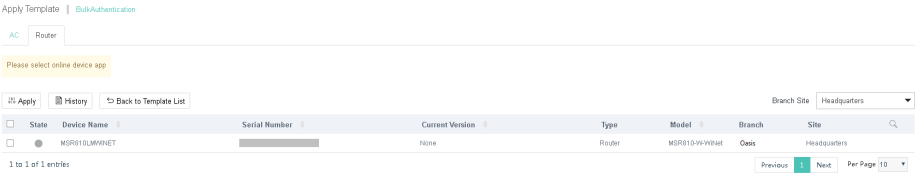
6. Click *OK* or click *Release* in the upper right corner of the page.



Configuring dumb terminal authentication

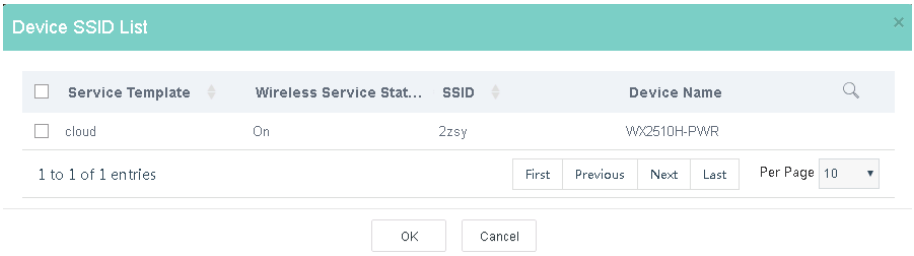
7. To deploy a template, perform the following steps:

   » Click the *Deploy Template* icon for that authentication template.
   » Click the *Router* tab.
   » Select a branch or site.
   » Select a device and then click *Apply.*
   If no devices are displayed, please check the device version.



Deploying a template

   » Select a service template or an SSID, and then click *OK.*



Selecting a service template

8. Enable MAC-triggered authentication on the device. For more information, see *Configure MAC--trigger authentication.*

Configure bulk authentication

Perform this task to deploy authentication settings in bulk.

Restrictions and guidelines

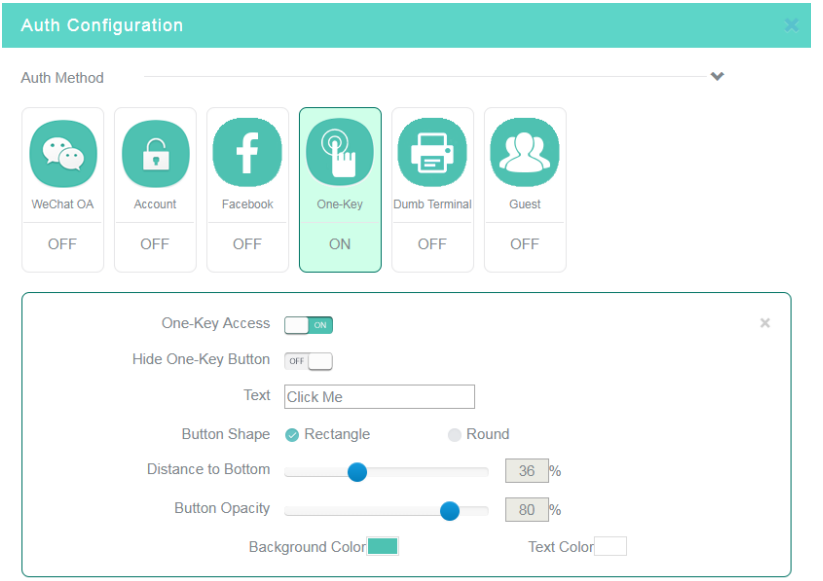
The configuration of a bulk authentication template takes precedence over that of a non-bulk authentication template. For the non-bulk authentication template to take effect, click the *Edit* icon for that authentication template, and then click *Apply.*

Before deploying the configuration in bulk, make sure the following requirements are met:

- The devices where the bulk authentication is deployed are online. If a device is offline, the deployment fails for the device. The device will load the most recent deployed configurations at start up.
- The wireless service name is the same as the portal Web server.

Procedure

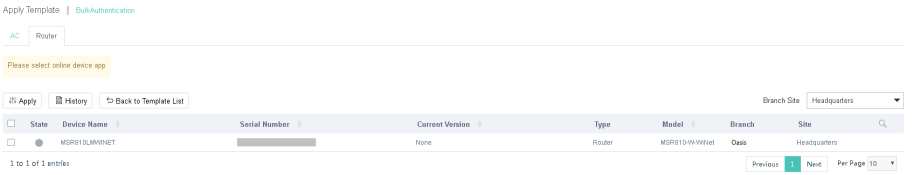
1. On the top navigation bar, click *Service.*
2. Select *Authentication* from the navigation pane,
3. Click the *Draw* icon for the target authentication template. For the detailed configuration procedures of different authentication methods, see *Configure basic settings.*



Configuring bulk authentication

4. To deploy a template, perform the following steps:
   - Click the *Deploy Template* icon for that authentication template.
   - Click the *Router* tab.
   - Select a branch or site.
   - Select a device and then click *Apply.*

   If no devices are displayed, please check the device version.



Deploying a template

Customize an authentication page

You can configure the landing page, login page, login success page, and home page and can push or disable the landing page or login success page as needed.

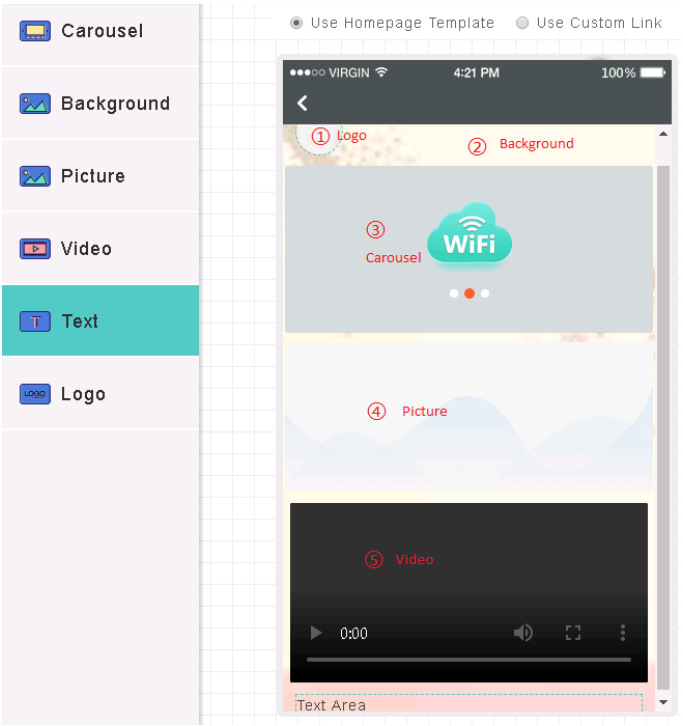
Restrictions and guidelines

The picture size cannot exceed 1 M. As a best practice, set the picture size to be in the range of 100 KB to 200 KB. Only JPG, JPEG, BMP, PNG, GIF, and SVG formats are allowed.

As a best practice to avoid affecting the loading speed of the page, do not add too many controls.

Procedure

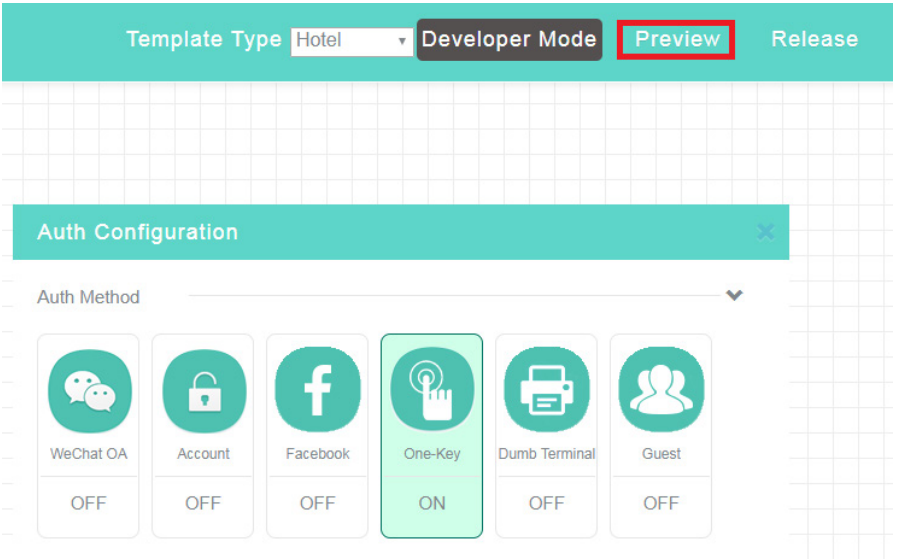
1. On the top navigation bar, click *Service*.
2. Select *Authentication* from the navigation pane.
3. On the *Authentication Templates* tab, click the *Draw* icon for the target authentication template.
4. Configure the following settings as shown in *Figure Previewing the configuration change:*
   - » **Logo:** the aspect ratio must be 1:1. The picture will be automatically cut into a circle. You can enter a shop name with a length of less than 12 characters.
   - » **Background:** the aspect ratio must be 3:5.
   - » **Carousel:** the aspect ratio must be 11:5. Two or three pictures of the same height are required.
   - » **Picture:** the aspect ratio must be 11:5. The description for the picture cannot exceed 48 characters.
   - » **Video:** the video size cannot exceed 5 M. Only MP4, WEBM, and OGG formats are allowed.
   - » **Text:** you can edit the font, font size, bold type, and font color.



Custom template description

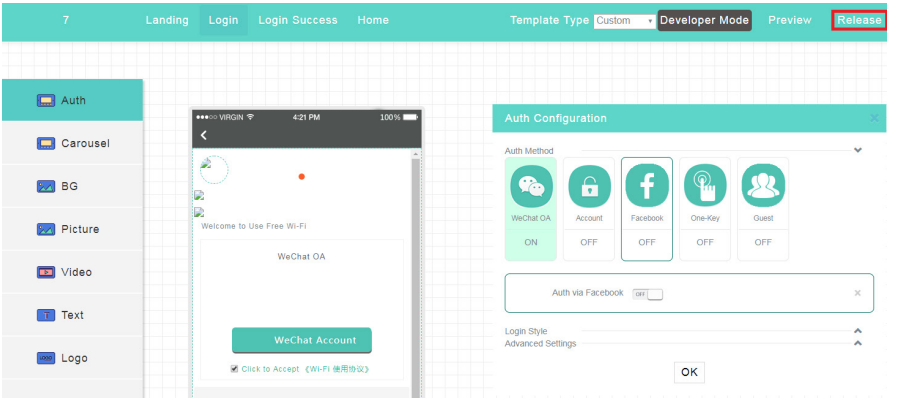
To configure the homepage, click the Home tab, and then select *Use Custom Link*.

5. Enter a custom link and then click *Upload*.
6. To preview the link, click *Preview* in the upper right corner of the page.



Previewing the configuration change

7. Click *Release* in the upper right corner of the page.
   The homepage pushed to users during portal authentication will be replaced by the page redirected by this custom link.



Configuring the custom template

3.2. Configure advanced settings

The INC Cloud provides advanced authentication settings to simplify authentication management, reduce cost, and optimize market promotion. *Table Advanced INC Cloud authentication features* describes available advanced features for each authentication method. You can configure these settings as needed.

Advanced INC Cloud authentication features:

Authentication method	Advanced features
One-key authentication	Captive-bypass Hiding and customizing one-key authentication button Internet access settings Authentication free Inter-site and inter-SSID re-authentication Internet access control Developer mode Domain name whitelist and blacklist Viewing and exporting history of authentication configuration deployment
Fixed-account authentication	Captive-bypass Bulk management of fixed accounts Self-service password change Collaboration with LDAP server Changing visual effects of the login page Internet access settings Authentication free Inter-site and inter-SSID re-authentication Internet access control Developer mode Domain name whitelist and blacklist Viewing and exporting history of authentication configuration deployment
Guest authentication	Captive-bypass Internet access settings Authentication free Inter-site and inter-SSID re-authentication Internet access control Developer mode Domain name whitelist and blacklist Viewing and exporting history of authentication configuration deployment
Dumb terminal authentication	Captive-bypass Management of dumb terminal account groups Internet access control Developer mode Domain name whitelist and blacklist Viewing and exporting history of authentication configuration deployment

Enable the captive-bypass feature

Typically, the device pushes the authentication page to a client automatically when the client attempts to access a portal authentication network. The captive-bypass feature enables the device to push the portal authentication page to the client only when the user launches a browser.

To enable the captive-bypass feature, you must perform the following steps on the device:

1. Enter system view.
   system-view
2. Enter portal Web server view of Web server **cloud**.
   Portal web-server cloud
3. Enable the captive-pass feature.
   captive-bypass enable

Hide or customize the one-key authentication button

Perform this task to hide the one-key authentication button or change the button style. If the button is hidden, users pass the authentication automatically after the countdown timer on the login page expires.

Restrictions and guidelines

You can change the button style only when the button is not hidden.

Procedure

1. On the top navigation bar, click *Network*.
2. Select *Settings > Routers > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Wireless Authentication Templates* tab.
5. Click the *Draw* icon for the target authentication template.
6. Click the *One-Key* tile in the *Auth Configuration* area, and then hide or customize the button as needed.

Manage fixed accounts

Perform this task to delete, import, or export fixed accounts in bulk.

To manage fixed accounts:

1. On the top navigation bar, click *Network*.
2. Select *Settings > Routers > Users* from the navigation pane.
3. Click the *Fixed Accounts* tab.
4. To delete fixed accounts, select the target fixed accounts and then click *Delete*.
5. To import fixed accounts, click *Import,* download the template file and fill in the file as required, and then upload the template file.
6. To export fixed accounts, click *Export*.

Enable self-service password change

This feature enables users to change passwords at login. With this feature disabled, only the administrators can change the passwords of fixed accounts.

To enable self-service password change:

1. On the top navigation bar, click *Network*.
2. Select *Settings > Routers > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Wireless Authentication Templates* tab.
5. Click the *Draw* icon for the target authentication template.
6. Click the *Account* tile in the *Auth Configuration* area.
7. Enable *Change Password*.

Enable collaboration with an LDAP server for fixed account verification

Perform this task to enable the INC Cloud to report usernames and passwords to the LDAP server for verification when users attempt to access the WLAN by using fixed accounts. This frees network administrators from importing account information from the LDAP server to the INC Cloud.

Restrictions and guidelines

To use this feature, make sure the LDAP server has been configured.

Procedure

1. On the top navigation bar, click *Network*.
2. Select *Settings > Routers > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Wireless Authentication Templates* tab.
5. Click the *Draw* icon for the target authentication template.
6. Click the *Account* tile in the *Auth Configuration* area.
7. Enable *LDAP* and configure LDAP settings as needed.
8. Click *LDAP Config Verification* to verify the LDAP settings.

Change visual effect settings of the login page

Perform this task to customize the background color, background opacity, and text color on the login page.

Restrictions and guidelines

Caution:

Restoring default settings will remove all user-defined visual effect settings and the restore operation is irreversible. Please use this feature with caution.

Visual effect settings of authentication methods take effect only when multiple authentication methods are enabled.

Procedure

1. On the top navigation bar, click *Network*.
2. Select *Settings > Routers > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Wireless Authentication Templates* tab.
5. Click the *Draw* icon for the target authentication template.
6. Click to expand the *Login Style* menu in the *Auth Configuration* area.
7. Configure the background color, background opacity, and text color as needed.
   The adjustment will be displayed in the preview area in real time. To restore the default visual effect settings, click *Restore Default*.

Configure Internet access settings

Procedure

1. On the top navigation bar, click *Network*.
2. Select *Settings > Routers > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Wireless Authentication Templates* tab.
5. Click the *Draw* icon for the target authentication template.
6. Click to expand the *Advanced Settings* menu in the *Auth Configuration* area.
7. Configure Internet access settings as needed.

Parameters

- **Session Timeout**: maximum continuous online duration of a client upon one authentication. A client will be logged off when its continuous online duration exceeds the timeout. The session timeout cannot be larger than the daily online duration.
- **Daily Online Duration**: maximum online duration of a client for a day. A client will be logged off when its online duration for a day exceeds the limit. The daily online duration cannot be smaller than the session timeout.
- **Minimum Traffic and Idle Timer**: logs off a client if its traffic within an idle timer fails to reach the minimum traffic threshold. Setting the idle timer to 0 disables the idle timer feature.

Note:

As a best practice, set the idle timer to a value no larger than half of the clients' IP address lease, enabling entries of offline clients to be deleted in time.

- **Client Rate Limit**: limited rate of uplink and downlink client traffic. This feature is supported in versions higher than 5417P01.
- **HTTPS for Landing and Login**: use HTTPS sessions for the Landing and Login page.
- **Permit PC**: Permit PCs to access the WLAN. Facebook authentication does not support this feature.

Manage dumb terminal account groups

Perform this task to create, delete, or edit dumb terminal account groups and import or export dumb terminal accounts.

If you enable dumb terminal authentication and specify an account group, only dumb terminals in the group can access the WLAN.

To manage dumb terminal account groups:

1. On the top navigation bar, click *Service*.
2. Select *Authentication* from the navigation pane.
3. Click the *Accounts* tab.
4. On the *Dumb Terminal Accounts* tab, configure dumb terminal account groups.

Configure portal automated authentication

This feature allows users that have been authenticated to access the network without re-authentication within the auth-free period. The following modes are available:

- **Portal redirection**: in this mode, users must run a browser to trigger automatic portal authentication. This mode supports pushing ads to clients.
- **MAC-trigger**: in this mode, users can access the WLAN without running a browser. This mode does not support pushing ads to clients.

Configure portal redirection authentication

1. On the top navigation bar, click *Network*.
2. Select *Settings > Routers > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Wireless Authentication Templates* tab.
5. Click the *Draw* icon for the target authentication template.
6. Click to expand the *Advanced Settings* menu in the *Auth Configuration* area.
7. Click the *Auth-Free* tab and configure the *Free Auth* feature.

Configure MAC-trigger authentication

1. Configure portal redirection authentication. For more information, see *Configure portal redirection authentication*.
2. Apply MAC binding server *cloud* to service template *cloud*.

   [Sysname] wlan service-template cloud

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

Configure inter-site and inter-SSID re-authentication

This feature allows clients that have been authenticated to roam between wireless services associated with different sites or different SSIDs for the same site without re-authentication. These wireless services must use the same authentication template or have the same SSID.

Restrictions and guidelines

This feature is available only for authentication templates configured in the App Center.

Procedure

1. On the top navigation bar, click *Service*.
2. Select *Authentication* from the navigation pane.
3. .Click the *Draw* icon for the target authentication template.
4. Click to expand the *Advanced Settings* menu in the *Auth Configuration* area.
5. Click the *Auth-Free* tab and enable *Free Auth*.
6. Configure inter-site and inter-SSID re-authentication.

Configure Internet access control

Perform this task to specify the time ranges during which users are allowed to access the WLAN.

Restrictions and guidelines

Internet access control is on a per-hour basis. You can specify a maximum of five time ranges for a day. To specify a time range that ends at 24 o'clock, set the end time to 00. If you set a time range to 00 to 00 for a day, users can access the Internet at any time that day.

Procedure

1. On the top navigation bar, click *Network*.
2. Select *Settings > Routers > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Wireless Authentication Templates* tab.
5. Click the *Draw* icon for the target authentication template.
6. Click to expand the *Advanced Settings* menu in the *Auth Configuration* area.
7. Click the *Internet Access Control* tab and specify the time ranges.

Configure the developer mode

Caution:

Editing the codes of existing functions might disable INC Cloud authentication. Please use this feature with caution.

The developer mode allows users to modify the source codes of an authentication template for customization purposes.

Procedure

1. On the top navigation bar, click *Network* .
2. Select *Settings > Routers > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Wireless Authentication Templates* tab.
5. Click the *Draw* icon for the target authentication template.
6. Click *Developer Mode* in the upper right corner.

Configure the domain name whitelist and blacklist

Restrictions and guidelines

This feature takes effect only when wireless authentication is configured.

Procedure

1. On the top navigation bar, click *Network*.
2. Select *Settings > Routers > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Domain Name Whitelist or Domain Name Blacklist* tab to configure the whitelist or blacklist.

View or export history of authentication template deployment

Perform this task to view the history of all authentication template deployment or deployment in the current day, past 7 days, or past 30 days.

To view or export history of authentication template deployment:

1. On the top navigation bar, click *Service*.
2. Select *Authentication* from the navigation pane.
3. On the *Authentication Templates* tab, click the *Apply* icon  for the target authentication template.
4. Click the ACs tab to view the deployment history for an AC.

4. Manage INC Cloud users

4.1. Configure the client blacklist

Perform this task to forbid specific clients to access the WLAN.

Restrictions and guidelines

This feature takes effect only on offline clients. If you add an online client to the blacklist, the client will be rejected at the next access attempt.

Procedure

1. On the top navigation bar, click *Network*.
2. .Select *Settings > Device Category > Users* from the navigation pane.
3. Perform either of the following tasks to add users to the blacklist:
   - On the *Guests* tab, click the *Add to Blacklist* icon  for the target user.
   - On the *Blacklist* tab, click *Add*.

4.2. Log off online users

Perform this task to log off specific online users or all online users.

Restrictions and guidelines

This feature does not take effect on auth-free users.

This feature is available only in scenarios with an AC or wired router as the authenticator.

Procedure

1. On the top navigation bar, click *Network*.
2. Select *Network > Clients > Guest Details* from the navigation pane.
3. Select a branch and a site from the top of the page.
4. On the *Online Clients* tab, click *Authenticated Clients*.
5. To log off specific clients, select the clients and then click *Log Off Selected Users*. To log off all clients, click *Log Off All Users*.

5. Configure portal fail-permit

This feature is available only in scenarios with an AC or wireless router as the authenticator.

Portal fail-permit allows users to have network access without portal authentication when the access device detects that the portal authentication server or portal Web server is unreachable.

After portal authentication resumes, unauthenticated users must pass portal authentication to access the network. Users who have passed portal authentication before the fail-permit event can continue accessing the network.

5.1. Restrictions and guidelines

For this feature to take effect, make sure you have configured basic settings on the device. For more information, see “Configure settings on the device.”

Procedure

1. Enable portal fail-permit.

   <Sysname> system-view

   [Sysname] wlan service-template cloud

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

   [Sysname-wlan-st-cloud] quit

2. Configure portal Web server detection.

Caution:
To avoid portal server flapping, follow the provided order to configure portal Web server detection.

 # Specify the URL and the type for portal Web server detection.

[Sysname] portal web-server cloud

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

 # Configure server detection:

- Set the detection interval to 600 seconds.
- Set the maximum number of consecutive detection failures to 2.
- Configure the device to send a log message and a trap massage after server reachability status changes.

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

[Sysname-portal-websvr-cloud] quit

6. Configure authentication when an AP registers to an AC over a public network

This feature is available only in scenarios with an AC or wireless router as the authenticator.

By default, the device provides HTTP port 80 for clients to exchange authentication packets. With local forwarding enabled, if APs register on the AC through the public network and port 80 is unavailable, perform this task to configure CMCC or change HTTP service port for clients to perform INC Cloud authentication.

6.1. Configure CMCC

You must configure CMCC on both the AC and the INC Cloud.

To configure CMCC:

1. Configure the CMCC protocol
   - » Configure the INC Cloud:
     - » Configure the INC Cloud in an AC+fit AP network
     - » Configure the INC Cloud in a wireless network
   - » Configure the device
2. (Optional) Configure CMCC portal redirection authentication
   - » Configure the
   - » Configure the device

6.2. Restrictions and guidelines

With CMCC configured, the session timeout, daily online duration, minimum traffic, and idle timer settings become unavailable.

Configure the CMCC protocol

Configure the INC Cloud in an *AC+fit AP network*

1. On the top navigation bar, click *Network*
2. .Select *Settings > ACs > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Draw* icon  for the target authentication template.
5. Click to expand the *Advanced Settings* menu in the *Auth Configuration* area.
6. Click the *CMCC* tab.
7. Enable *CMCC Protocol* and select a protocol as needed.

Configure the INC Cloud in a wireless network with a router as the authenticator

1. On the top navigation bar, click *Network.*
2. Select *Settings > Routers > Authentication* from the navigation pane.
3. Select a branch, a site, and a device from the top of the page.
4. Click the *Draw* icon  for the target authentication template.
5. Click to expand the *Advanced Settings* menu in the *Auth Configuration* area.
6. Click the *CMCC* tab.
7. Enable *CMCC Protocol* and select a protocol as needed.

Configure the device

 # Create the portal authentication server cloud and enter its view.

<Sysname> system-view

[Sysname] portal server cloud

 # Specify 139.217.11.74 as the IPv4 address of the portal authentication server.

[Sysname-portal-server-cloud] ip 139.217.11.74

 # Specify the type of the portal authentication server as cmcc.

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

 # Configure the device to send register packets to the portal authentication server at intervals of 60 seconds.

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

[Sysname-portal-server-cloud] quit

6.3. Configure CMCC portal redirection authentication

Configure the INC Cloud

Enable portal redirection authentication. For more information, see *Configure portal redirection authentication* for AC+fit AP networks and *Configure portal redirection authentication* for wireless networks with a wireless router as the authenticator.

Configure the device

Make sure you have configured basic settings on the device. For more information, see *Configure settings on the device.*

To configure the device:

1. Configure the MAC binding server.

Caution:

To avoid affecting wireless services, you must specify a dedicated MAC binding server for CMCC even if a MAC binding server has been created.

 # Create MAC binding server mts and enter its view.

<Sysname> system-view

[Sysname] portal mac-trigger-server mts

 # Specify the IP address of the MAC binding server as 139.217.11.74.

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

 # Specify the type of the MAC binding server as cmcc.

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

 # (Optional.) Set the free-traffic threshold for portal users, in bytes.

[Sysname-portal-mac-trigger-server-mts] free-traffic threshold 1

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

 # Bind MAC binding server mts to service template cloud.

[Sysname] wlan service-template cloud

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

2. Configure authorization attributes for users in the ISP domain.

   # Create ISP domain cloud.

   [Sysname] domain cloud

   # Set the idle timer, in minutes.

   [Sysname-isp-cloud] authorization-attribute idle-cut 30

   # Set the session timeout, in minutes.

   [Sysname-isp-cloud] authorization-attribute session-timeout 360

   [Sysname-isp-cloud] quit

6.4. Change the HTTP service port

Before performing this task, make sure you have configured basic settings on the device. For more information, see *Configure settings on the device*.

To change the HTTP service port:

1. Set the HTTP service port number. In this example, the port number is 8088.

   <Sysname> system-view

   [Sysname] ip http port 8088

2. Create an HTTP-based local portal Web service and set the listening port number to 8088.

   [Sysname] portal local-web-server http

   [Sysname-portal-local-websvr-http] tcp-port 8088

   [Sysname-portal-local-websvr-http] quit

3. Configure the portal server.

   # Configure the URL for the portal Web server. x.x.x.x represents the egress IP of the network in which the AC resides.

   [Sysname] 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 the INC Cloud server to redirect users to 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: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:8088/portal/cloudlogin.html

   [Sysname-portal-websvr-cloud] quit

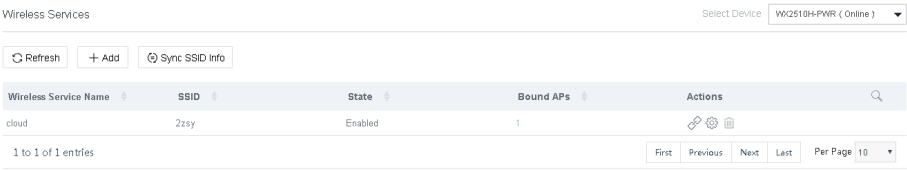
7. Configure wireless services

1. On the top navigation bar, click *Network*.
2. Select *Settings > Device Category > Wireless Services* from the navigation pane.
3. On the *Wireless Services* tab, click *Add*.
4. To configure an encryption service, select *On or Off* for the *Encryption Service* field as needed.

Configuring an encryption service

5. To synchronize SSID information, click *Sync SSID Info*.
   Make sure you have created a wireless service and configured SSID information on the device.

Note:
This feature is available only for ACs of a version earlier than 5418 and routers of a version earlier than 0809.



Synchronizing SSID information

6. To synchronize wireless service settings on devices to the INC Cloud, click *Sync to Cloud*. This operation synchronizes settings such as wireless service name, SSID, and guaranteed bandwidth ratio to the INC Cloud.

Note:
This feature is available only for ACs of version 5418 or later and routers of version 0809 or later.

8. FAQ

8.1. I modified and deployed authentication template settings successfully. Why do the previous settings take effect on clients that come online after the deployment?

Verify that the settings are modified and deployed successfully. If the issue persists, clear browser access records and caching on the client.

8.2. The Authentication Templates page in the App Center does not display devices available for template deployment. What should I do?

Verify that the device version is as required. If not, upgrade the device to the most recent version.

8.3. How can I change the SSID of a wireless service?

1. Change the Wi-Fi name from the INC Cloud. For AC+fit AP networks, you can also change the Wi-Fi name on the AC.
2. Unbind and then rebind the service template from the authentication service.

8.4. How can I update my INC Cloud to use newly released features?

Feature on the INC Cloud are automatically updated and do not require manual operations. For new authentication template features, you might need to reconfigure and then release the template for the new features to take effect.

8.5. Why can a client go offline and then come online without being authenticated even if authentication free is not configured?

The system does not remove the client entry from the authenticated client list immediately upon a client disassociation event. The entry will not be removed until the idle timer expires or the administrator logs the client off. An offline client can come online without being authenticated if its entry still exists.

You can view client entries from the INC Cloud or by executing the display portal user all command.

8.6. Why does the number of authenticated clients exceed the total number of online clients?

This symptom occurs if a client just went offline. The system does not remove the client entry from the authenticated client list immediately upon a client disassociation event. The entry will not be removed until the idle timer expires or the administrator logs the client off manually.

8.7. I have configured authentication settings on the device and the INC Cloud as required. Client access attempt can trigger portal authentication but cannot open the redirection page. What should I do?

This issue might occur if the network segment of the client's IP address is unknown to the uplink devices and packets cannot be transmitted back. To resolve this issue, configure the nat outbound command on the device's interface that connects the device to the external network, or use IGP to advertise the network segment in the network.

8.8. iOS clients cannot trigger authentication even if optimized captive-bypass is enabled. What should I do?

Execute the portal captive-bypass optimize delay *seconds* command to set the captive-bypass detection timeout. The value range is 6 to 60 seconds and the default value is 6 seconds.

To avoid affecting device performance, do not set the timeout to a large value.

9. Appendix A Authentication commands for the device

This section describes commands that need to be executed on the device for one-key, fixed-account, Facebook, dumb terminal, and guest authentication.

For app and Facebook authentications, you must configure settings in *Configure Facebook authentication and Configure Facebook authentication,* respectively, after you complete settings in this section.

To fast execute these commands on the device, edit the dimmed sections as needed and paste all the commands in user view of the device.

Note:

- Execute these commands only in versions earlier than 5405. Version 5405 and later support automatic authentication setting deployment to devices and do not need manual configuration of these commands.
- Make sure the commands do not conflict with configuration existing on the device.
- Make sure you have completed tasks in the configuration prerequisites. For more information, see *Prerequisites*.

```
system-view
domain cloud
authentication portal none
authorization portal none
accounting portal none
quit

portal web-server 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
quit

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
quit
portal local-web-server https
quit

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
portal free-rule 14 destination minorshort.weixin.qq.com
portal free-rule 15 destination extshort.weixin.qq.com
portal free-rule 16 destination szshort.weixin.qq.com
portal free-rule 17 destination szlong.weixin.qq.com
portal free-rule 18 destination szextshort.weixin.qq.com
portal free-rule 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

talk to us

Customer Support: +55 (48) 2106 0006
Forum: forum.intelbras.com.br
Support via chat: chat.apps.intelbras.com.br
Support via e-mail: suporte@intelbras.com.br
Customer Service / Where to buy? / Who installs it?: 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 | www.intelbras.com/en

01.25