H3C Cloudnet
認証ユーザーガイド

New H3C Technologies Co., Ltd.
https://www.H3C.com/

ドキュメントバージョン:6W100-20200907

環境保護

この製品は、環境保護要件に準拠するように設計されています。この製品の保管、使用、および廃棄は、適用される国内法および規制を満たしている必要があります。

序文

このガイドでは、H3C Cloudnetの導入手順について説明します。

この序文には、ドキュメントに関する次のトピックが含まれてい

ます:

- 対象読者。
- 表記法。
- ドキュメントへのフィードバック。

対象読者

このドキュメントの対象読者は次のとおりです：

- ネットワーク計画者。
- フィールドテクニカルサポートおよびサービスエンジニア。
- Cloudnetを使用するネットワーク管理者。

表記法

次の情報は、ドキュメントで使用されている表記法について説明しています。

コマンド規則

表記法	説明
太字	**太字** のテキストは、示されている文字の通りに入力するコマンドとキーワードを表します。
イタリック	*イタリック のテキストは、示されている文字の通りに入力するコマンドとキーワードを表します。*
[ ]	角括弧は、オプションの構文の選択肢（キーワードまたは引数）を囲みます。
{ x | y | ... }	中括弧は、垂直バーで区切られた必要な構文の選択肢のセットを囲み、そこから1つを選択します。
[x | y | ...]	角括弧は、縦棒で区切られたオプションの構文の選択肢のセットを囲み、そこから1つまたは何も選択しません。
{ x | y | ... }*	アスタリスクでマークされた中括弧は、垂直バーで区切られた必要な構文の選択肢のセットを囲み、そこから少なくとも1つを選択します。
[x | y | ...]*	アスタリスクでマークされた角括弧は、垂直バーで区切られたオプションの構文の選択肢を囲み、そこから1つの選択肢、複数の選択肢、または何も選択しません。
&<1-n>	アンパサンド（&）記号の前の引数またはキーワードと引数の組み合わせは、1〜n回入力できます。
#	シャープ（#）記号で始まる行はコメントです。

GUIの規則

表記法	説明
太字	ウインドウ名、ボタン名、フィールド名、およびメニュー項目は太字で表示されます。例えば、 **New User** ウインドウを開いて**OK** をクリックします。
>	マルチレベルメニューは山括弧で区切られています。例えば、 **File > Create > Folder**.

記号

表記法	説明
⚠ 警告！	理解または従わないと怪我につながる可能性のある重要な情報に注意を喚起する警告。
△ 注意：	重要な情報に注意を喚起する警告。理解または従わないと、データの損失、データの破損、またはハードウェアやソフトウェアの損傷につながる可能性があります。
ⓘ 重要：	重要な情報に注意を喚起する警告。
注意：	追加情報または補足情報を含む警告。
ヒント：	役立つ情報を提供する警告。

ネットワークトポロジーアイコン

表記法	説明
	ルーター、スイッチ、ファイアウォールなどの一般的なネットワークデバイスを表します。
	ルーターやレイヤー3スイッチなどのルーティング対応デバイスを表します。
	レイヤー2またはレイヤー3スイッチなどの汎用スイッチ、またはレイヤー2転送およびその他のレイヤー2機能をサポートするルーターを表します。
	統合有線WLANスイッチ上のアクセスコントローラ、統合有線WLANモジュール、またはアクセスコントローラエンジンを表します。
	アクセスポイントを表します。
	ワイヤレスターミネータユニットを表します。
	ワイヤレスターミネーターを表します。
	メッシュアクセスポイントを表します。
	全方向性信号を表します。
	指向性信号を表します。
	ファイアウォール、UTM、マルチサービスセキュリティゲートウェイ、負荷分散デバイスなどのセキュリティ製品を表します。
	ファイアウォール、負荷分散、NetStream、SSL VPN、IPS、ACGモジュールなどのセキュリティモジュールを表します。

このドキュメントで提供される例

このドキュメントの例では、ハードウェアモデル、構成、またはソフトウェアバージョンがデバイスとは異なるデバイスを使用している場合があります。例で示されるポート番号、サンプル出力、スクリーンショット、およびその他の情報は、デバイスにあるものとは異なる場合があります。

ドキュメントへのフィードバック

製品マニュアルに関するご意見は、info@h3c.comまで電子メールでお寄せください。 ご感想をお寄せいただければ幸いです。

内容

Cloudnet認証について

重要:
このドキュメントの一部の機能は、中国本土のみに制限されています。
- Tencentがポータル認証インターフェィスを無効にしたため、WeChat Wi-Fiとそれに依存する高度な機能は利用できません。

H3C Cloudnetは、従業員、ゲスト、IoT端末などのアクセスユーザーに対して豊富な認証方式を提供しています。クライアントがインターネットまたは特定のネットワークリソースにアクセスする場合、アクセスデバイスはクライアントをポータル認証のためにCloudnetにリダイレクトします。
H3C Cloudnetには次のようなメリットがあります。
- 認証クライアントに上限がありません。
- 豊富な認証ポリシー。
- カスタム広告プッシュサービス。

H3C Cloudnetは、表1に示す認証方式が提供されています。

表1 認証方法

認証方式	適用対象シナリオ	備考	複合認証
ワンキー	レストランや店舗など、監査および運用統計の収集要件が低い。	MACベースの認証。 ユーザーは、ポータル認証ページのボタンをクリックするだけで認証を完了できます。	サポート対象
固定アカウント	ネットワークユーザーは、キャンパスエリアやオフィスエリアなど、固定されています。	ユーザー名とパスワードに基づく認証。 次の関数がサポートされています。 •LDAP •アカウントのインポートとエクスポート •1つのアカウントを複数のMACアドレスにバインド •同時クライアント数の制限	サポート対象
WeChat公式アカウントログイン	運用統計の収集要件が高い。あらゆる種類の公共区域に適用可能。 事業者はQRコードを提供しなければなりません。	ユーザーは認証のために公式アカウントに従うだけで、電話番号やアカウントを提供する必要はありません。	サポート対象だが推奨されない
ゲスト認証	一時的なゲストアクセスが必要な企業またはショップ。	WeChat miniプログラムと併用される認証方法。ゲストは、承認者がゲストの端末上のQRコードをスキャンして端末を認証すると、ネットワークにアクセスできます。	サポート対象外
ダム端末認証	IoT機器、ワイヤレスプリンタ、POS端末	特定のワイヤレス端末での自動認証。	サポート対象外
Facebook認証	オペレーターは、Facebookを使ってネットワークユーザーに関する統計を収集します。	Cloudnetへのアクセスを許可するには、ユーザーはFacebookにログインする必要があります。 このメソッドは、https://oasiscloud.h3c.comでのみ使用できます。	サポート対象

表2 認証方法とネットワークの互換性

認証方法	異なる認証装置を持つネットワークとの互換性		
	AC	ワイヤレスルーター	有線ルーター
ワンキー認証	有	有	有
固定アカウント認証	有	有	有
ゲスト認証	有	有	有
Facebook認証	有	無し	無し
複合認証	有	有	有
ダム端末認証	有	有	無し
一括認証	有	有	無し
カスタム認証ページ	有	有	有

注意:
ワイヤレスルーターは、ACまたはファットAPとして機能し、ワイヤレス認証を提供できます。有線ルーターは、端末に直接接続するか、スイッチまたはファットAPを介して端末に接続して認証を行います。

認証装置としてACを使用するCloudnet認証の設定

基本設定の設定

前提条件

Cloudnet認証を設定する前に、次の作業を実行します。

- 装置をCloudnetに接続する。
  詳細については、『H3C Cloudnet導入ガイド』を参照してください。
- VLANとDHCPの設定を完了します。
- ワイヤレスサービスを設定し、APがオンラインになることを確認します。

デバイス設定の設定

制限事項およびガイドライン

認証設定の自動適用をサポートするのは、ソフトウェアバージョン5405以降だけです。その他のソフトウェアバージョンの場合は、デバイス上で次の設定を手動で設定します。
次の認証方式の迅速な導入については、”付録Aデバイスの認証コマンド”を参照してください。

- ワンキー認証。
- 固定アカウント認証。
- WeChat公式アカウント認証。
- Facebook認証。
- ダム端末認証。
- ゲスト認証。

一般設定の設定

1. ポータル認証ドメインを設定します。
   #cloudという名前のISPドメインを追加し、そのビューを入力します。
   <Sysname> system-view
   [Sysname] domain cloud
   #認証、認可、アカウンティングの各方式をnoneとして指定します。
   [Sysname-isp-cloud] authentication portal none
   [Sysname-isp-cloud] authorization portal none
   [Sysname-isp-cloud] accounting portal none
   [Sysname-isp-cloud] quit

2. クラウドポータル認証を設定します。
   #cloudという名前のポータルWebサーバーを追加し、そのURLとタイプを指定します。(管理者がCloudnet

でワイヤレスサービスを設定すると、設定がデバイスに自動的に適用されます)。
[Sysname] portal web-server cloud
[Sysname-portal-websvr-cloud] url http://oasisauth.h3c.com/portal/protocol
[Sysname-portal-websvr-cloud] server-type oauth
#一致規則を設定して、ユーザーエージェント文字列CaptiveNetworkSupportを伝送するHTTP要求を
URL http://oasisauth.h3c.com/generate_404にリダイレクトします。
[Sysname-portal-websvr-cloud] if-match user-agent CaptiveNetworkSupport
redirect-url http://oasisauth.h3c.com/generate_404
#一致規則を設定して、ユーザーエージェント文字列 Dalvik /2.1.0(Linux;U;Android7.0;Huawei)を伝送す
るHTTP要求をURL http://oasisauth.h3c.com/generate_404にリダイレクトします。
[Sysname-portal-websvr-cloud] if-match user-agent
Dalvik/2.1.0(Linux;U;Android7.0;HUAWEI redirect-url
http://oasisauth.h3c.com/generate_404
#一時的なパス規則を設定して、ユーザーエージェント情報にMozillaを含むユーザーパケットを通過させ、
URL http://captive.apple.com宛てのパケットをURL http://oasisauth.h3c.com/portal/protocolにリダイ
レクトできるようにします。
[Sysname-portal-websvr-cloud] if-match original-url http://captive.apple.com
user-agent Mozilla temp-pass redirect-url http://oasisauth.h3c.com/portal/protocol
#一時的なパス規則を設定して、ユーザーエージェント情報にMozillaを含むユーザーパケットを通過させ、
#URL http://www.apple.com宛てのパケットをURL http://oasisauth.h3c.com/portal/protocolにリダイレ
#クトできるようにします。
[Sysname-portal-websvr-cloud] if-match original-url http://www.apple.com user-agent
Mozilla temp-pass redirect-url http://oasisauth.h3c.com/portal/protocol
[Sysname-portal-websvr-cloud] quit
#URL http://10.168.168.168にアクセスするユーザーパケットの通過を一時的に許可する一時パス規則
#を設定します。
[Sysname] portal web-server cloud
[Sysname-portal-websvr-cloud] if-match original-url http://10.168.168.168 temp-pass
#iOSユーザーに対して最適化されたキャプティブバイパス機能をイネーブルにします。
[Sysname-portal-websvr-cloud] captive-bypass ios optimize enable
[Sysname-portal-websvr-cloud] quit
#サービステンプレートクラウドでポータルの直接認証を有効にします。
[Sysname] wlan service-template cloud
[Sysname-wlan-st-cloud] portal enable method direct
#認証ドメインをクラウドとして設定し、ポータルWebサーバークラウドをポータル認証用のクラウドポータル
Webサーバーとして指定します。
[Sysname-wlan-st-cloud] portal domain cloud
[Sysname-wlan-st-cloud] portal apply web-server cloud
[Sysname-wlan-st-cloud] quit
#ポータル一時パスを有効にし、一時パス期間を20秒に設定します。
[Sysname] wlan service-template cloud
[Sysname-wlan-st-cloud] portal temp-pass period 20 enable
[Sysname-wlan-st-cloud] quit
#HTTPベースのローカルポータルWebサービスを追加し、そのビューを入力します。
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] quit
#HTTPSベースのローカルポータルWebサービスを追加し、そのビューを入力します。
[Sysname] portal local-web-server https
[Sysname-portal-local-websvr-https] quit
#HTTPおよびHTTPSサービスを有効にします。
[Sysname] ip http enable
[Sysname] ip https enable
#ワイヤレスポータルクライアントの有効性チェックを有効にします。

[Sysname] portal host-check enable
#ポータルユーザーのログインおよびログアウトのログを有効にします。
[Sysname] portal user log enable
#ポータルユーザーが認証なしでDNSサービスにアクセスできるように、宛先ベースのポータルフリー規則#1を設定します。(この例では、114.114.114.114 255.255.255.255を使用します)。
[Sysname] portal free-rule 1 destination ip 114.114.114.114 255.255.255.255
#ポータルユーザーが認証なしでDNSサービスにアクセスできるように、宛先ベースのポータルフリー規則#2および4を設定します。
[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
#ポータルユーザーが認証なしでCloudnet認証サーバーにアクセスできるように、宛先ベースのポータル#フリー規則5を設定します。
[Sysname] portal free-rule 5 destination oasisauth.h3c.com
#ポータルユーザーが認証なしでCloudnet認証サーバーにアクセスできるように、宛先ベースのポータル#フリー規則10～22を設定します。
[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-rule19destination 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
#ポータルのセーフリダイレクトを有効にします。
[Sysname] portal safe-redirect enable
#ポータルのセーフリダイレクトで許可されるHTTP要求メソッドを指定します。
[Sysname] portal safe-redirect method get post
#ポータルのセーフリダイレクトで許可されるブラウザタイプを指定します。
[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 WeChat
[Sysname] portal safe-redirect user-agent iPhone
[Sysname] portal safe-redirect user-agent micromessenger

Facebook認証の設定

重要:

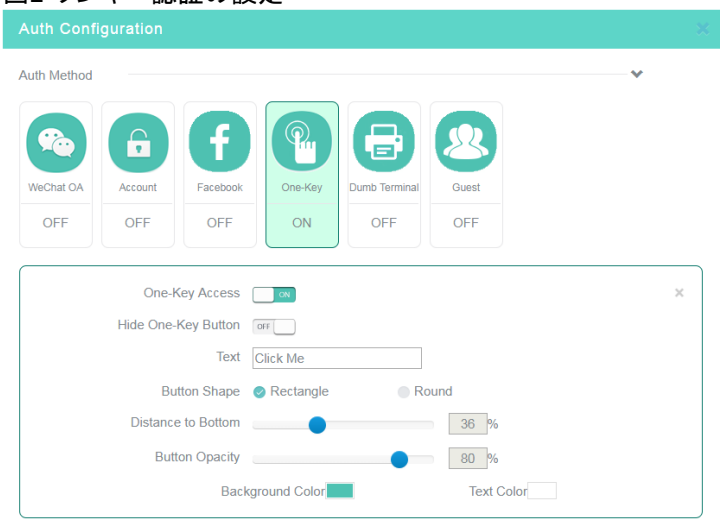
- このセクションのコマンドは、”一般設定の設定”または”付録Aデバイスの認証コマンド”の設定セクションのコマンドを実行します。
- Free-rule 38はアプリが画像を表示できないようにするかもしれません。必要に応じてこのルールを設定するか、テクニカルサポートに連絡してください。

#Facebook関連のホスト名を持つHTTP/HTTPS要求を送信するポータルユーザーが認証なしでネット
#ワークリソースにアクセスできるように、宛先ベースのポータルフリー規則を設定します。
<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

ワンキー認証の設定

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠で**Settings** > **ACs** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. 認証テンプレートを追加するには、**Authentication Templates**タブの**Add**をクリックします。
5. 認証テンプレートを編集するには、その認証テンプレートの**Edit** アイコンをクリックします。
6. 認証テンプレートをワイヤレスサービスにバインドするには、その認証テンプレートの**Edit**アイコン をクリックし、**Bind to Wireless Service**フィールドから**Yes**を選択して、**Apply**をクリックします。テンプレートがワイヤレスサービスにバインドされている場合は、この手順を省略します。
7. 対象の認証テンプレートの**Draw**アイコン をクリックします。
8. **Auth Configuration**領域の**One-Key**タイルをクリックし、ワンキー認証を有効にして、必要に応じて他の設定を行います。
9. **OK**をクリックするか、ページの右上隅にある**Release**をクリックします。

図1 ワンキー認証の設定



固定アカウント認証の設定

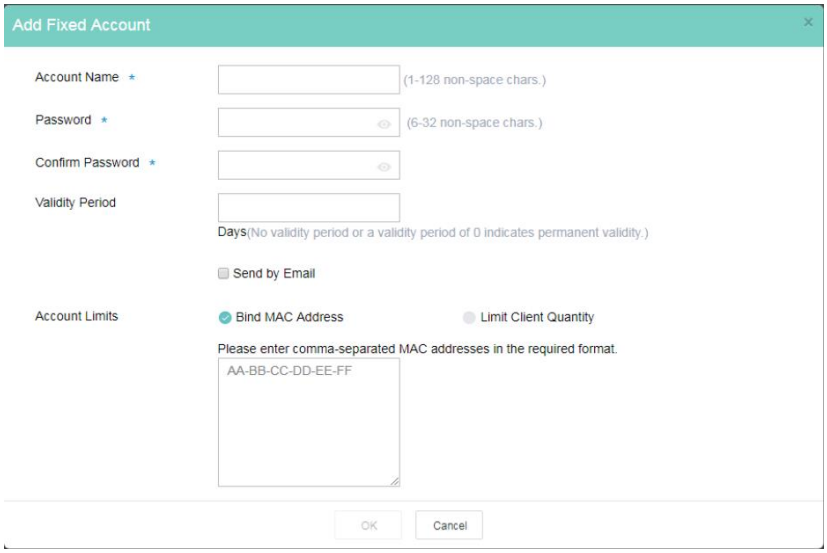
制限事項およびガイドライン

有効期間を設定しない場合、または有効期間を0に設定しない場合、アカウントは期限切れになりません。
Bind MAC Addressを選択し、MACアドレスを入力しない場合、固定アカウントを使用するクライアントは制限されません。
Sent by Emailを選択すると、指定した電子メールアドレスにアカウント名とパスワードが送信されます。電子メールアドレスの数は10を超えることはできず、コンマで区切る必要があります。

手順

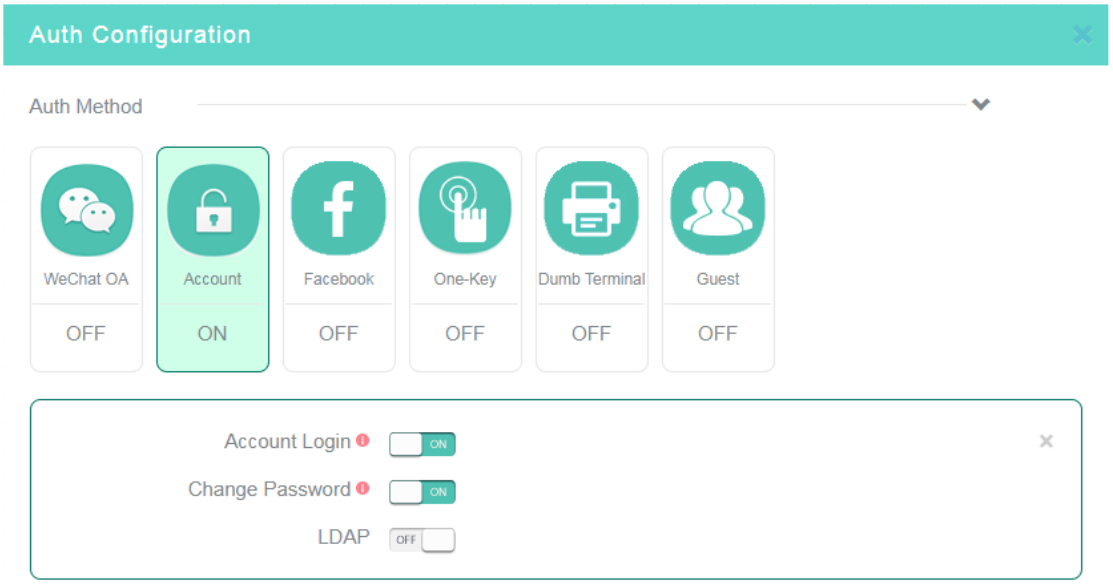
1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **ACs** > **Users**を選択します。
3. **Fixed Accounts**タブをクリックします。
4. **Add**をクリックします。
5. 必要に応じて固定アカウント情報を設定します。

図2 固定アカウントの追加



6. 認証テンプレートを追加または編集するには、ナビゲーション枠で**Settings** > **AC** > **Authentication**を選択し、ページ上部からブランチ、サイト、およびデバイスを選択します。テンプレートを追加するには、**Authentication Template**タブの**Add**をクリックします。テンプレートを編集するには、その認証テンプレートの**Edit**アイコン をクリックします。
7. 認証テンプレートをワイヤレスサービスにバインドするには、その認証テンプレートの**Edit**アイコン をクリックし、**Bind to Wireless Service**フィールドから**Yes**を選択して、**Apply**をクリックします。テンプレートがワイヤレスサービスにバインドされている場合は、この手順を省略します。
8. 対象の認証テンプレートの**Draw**アイコン をクリックします。
9. **Auth Configuration**領域の**Account**タイルをクリックし、固定アカウント認証を有効にして、必要に応じて他の設定を行います。
10. 他の認証方式を無効にします。
11. **OK**をクリックするか、ページの右上隅にある**Release**をクリックします。

図3 固定アカウント認証の設定



WeChat公式アカウント認証の設定

制限事項およびガイドライン

テナントは、Tencentによって認証されたWeChatサービスアカウントを持っていなければなりません。

WeChat公式アカウントプラットフォームを設定する

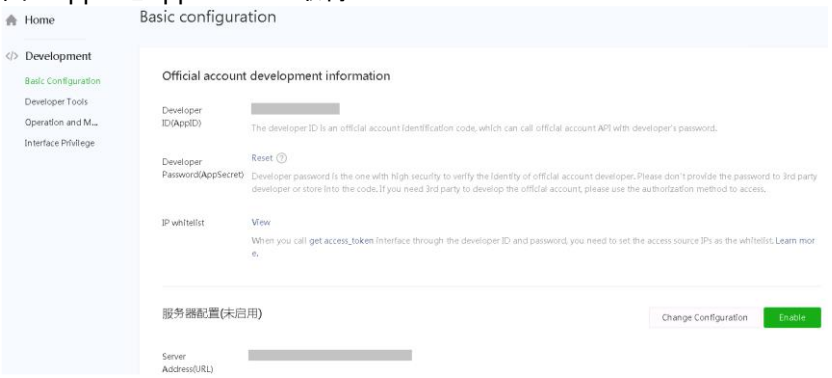
1. 適用されたWeChatサービスアカウントを使用して、https://mp.weixin.qq.com/のWeChat公式アカウントプラットフォームにアクセスします。

図4 サービスアカウントへのログイン

2. ナビゲーション枠で**Development** > **Basic Configuration**を選択します。
   a. 開いたページで、**AppID**と**AppSecret**を取得します。

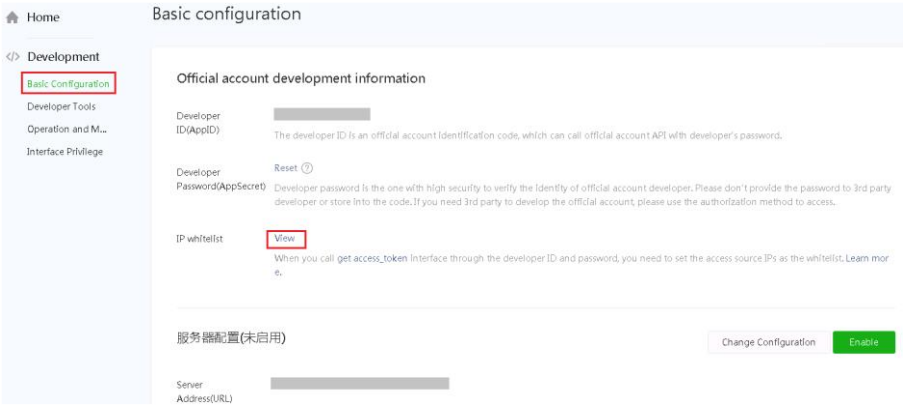
AppSecretを有効にして生成した後、WeChat公式アカウントプラットフォームは**AppSecret**を保存したり表示したりしないで正しく保存してください

図5 AppIDとAppSecretの取得



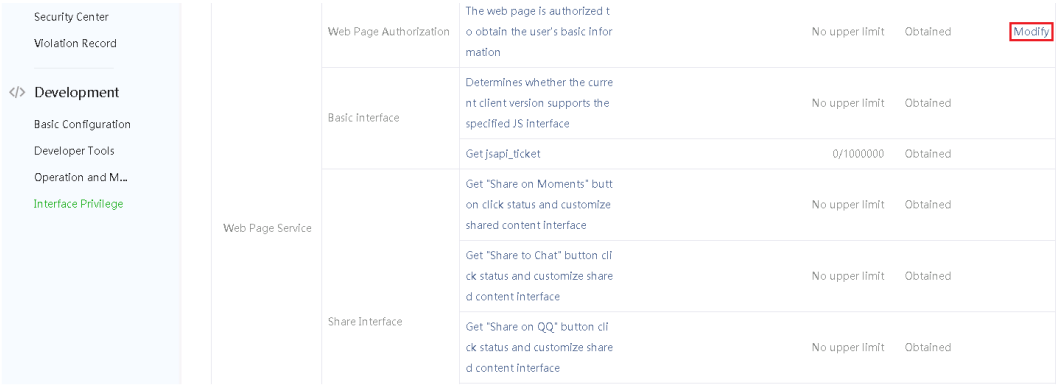
IPアドレス139.217.7.53、139.217.17.204、および139.219.0.33をIPホワイトリストに追加します。

図6 ホワイトリストへのIPアドレスの追加



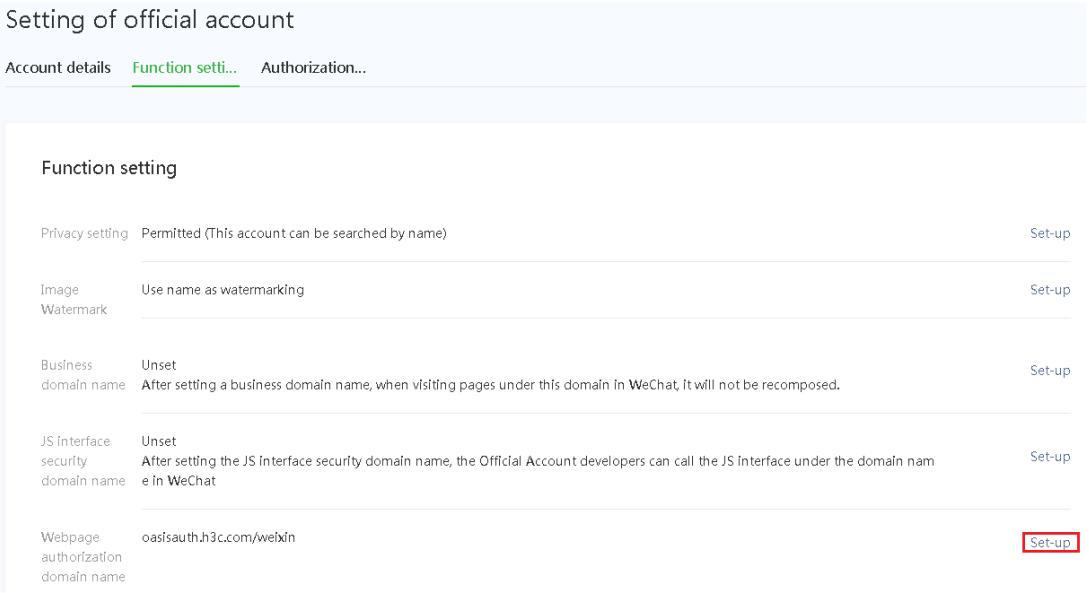
3. ナビゲーション枠で**Development** > **Interface Privilege**を選択し、**Web Page Authentication**フィールドで**Modify**をクリックします。

図7 Webページ認証の変更



4. **Function Setting**タブで、**Webpage authentication domain name**フィールドの**Set-up**をクリックします。

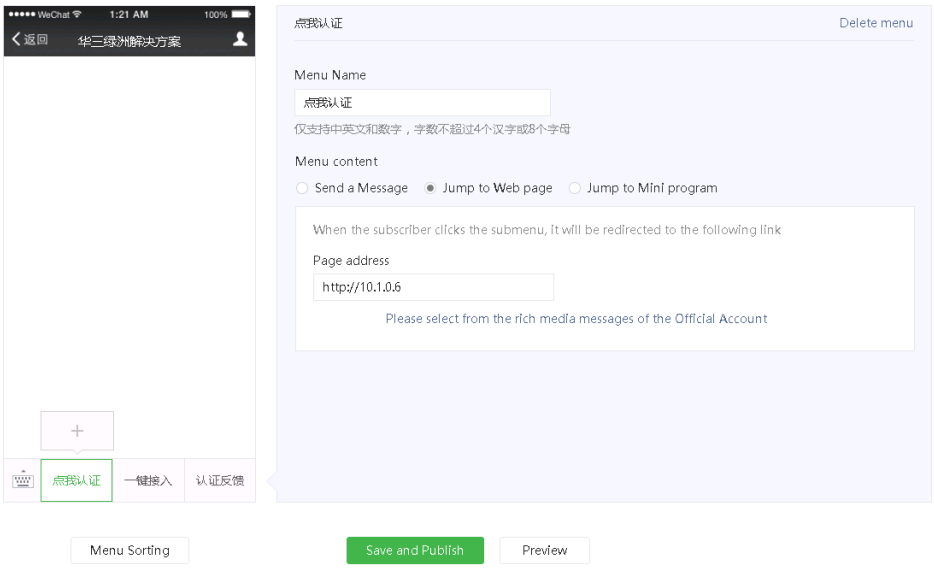
図8 Webページの認証ドメイン名の編集



5. ナビゲーション枠から**Function** > **Custom Menu**を選択し、追加アイコン+をクリックして、必要に応じて他の設定を設定します。

ベストプラクティスとして、**Page address**フィールドにhttp://10.168.168.1inと入力します。

図9 メニューの指定

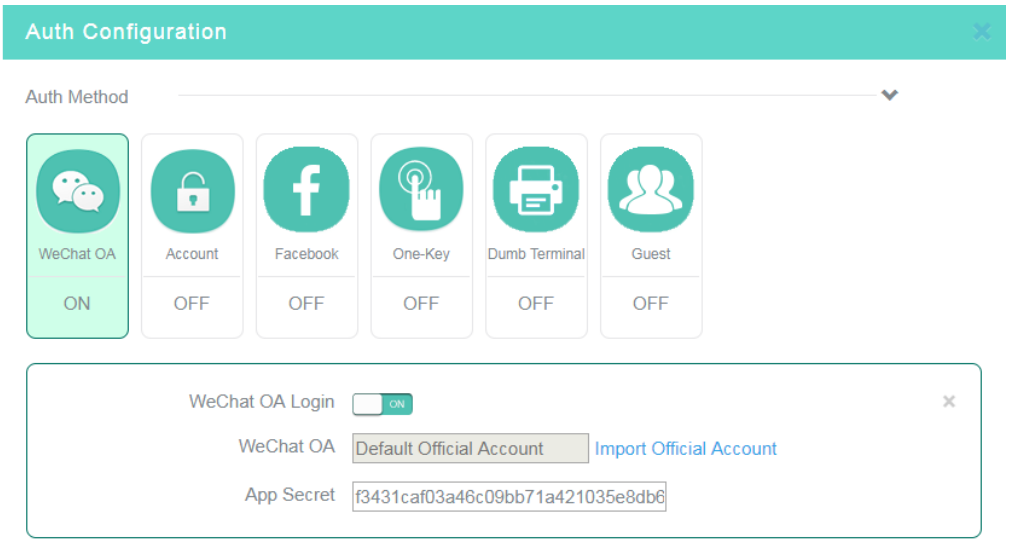


WeChat公式アカウント認証の設定

1. ナビゲーション枠で**Settings** > **ACs** > **Authentication**を選択します。
2. ページ上部からブランチ、サイトおよびデバイスを選択します。
3. 認証テンプレートを追加するには、**Authentication Template**タブで**Add**をクリックします。認証テンプレートを編集するには、その認証テンプレートの**Edit**アイコン をクリックします。
4. 認証テンプレートをワイヤレスサービスにバインドするには、その認証テンプレートの**Edit**アイコン をクリックし、**Bind to Wireless Service**フィールドから**Yes**を選択して、**Apply**をクリックします。テンプレートがワイヤレスサービスにバインドされている場合は、この手順を省略します。
5. 対象の認証テンプレートの**Draw**アイコン をクリックします。

6. **Auth Configuration**エリアのWeChat OAタイルをクリックし、WeChat公式アカウント認証を有効にします。
7. **Import Official Account**をクリックして、QRコードをスキャンします。
8. **AppSecret**を入力します。
9. 他の認証方式を無効にします。
10. **OK**をクリックするか、ページの右上隅にある**Release**をクリックします。

図10 WeChat公式アカウント認証の設定



ゲスト認証の設定

制限事項およびガイドライン

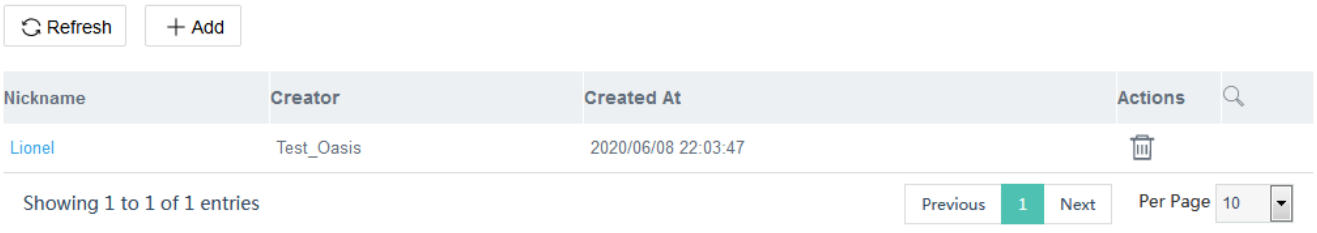
設定後、ゲストがネットワークにアクセスできるのは、承認者がクライアント上のQRコードをスキャンしてクライアントを認証した後だけです。QRコードは5分間有効です。QRコードが期限切れになると、ゲストはQRコードを更新する必要があります。

手順

1. トップナビゲーションバーの**Service**をクリックします。
2. ナビゲーション枠で**Authentication**を選択し、**Accounts**タブをクリックします。
3. **Guest Accounts**タブをクリックし、**Add**をクリックします。

承認者は、承認者がQRコードをスキャンしコードを入力した後に追加されます。承認者が削除されると、Cloudnetは自動的に承認者から権限を削除します。

図11 承認者の追加

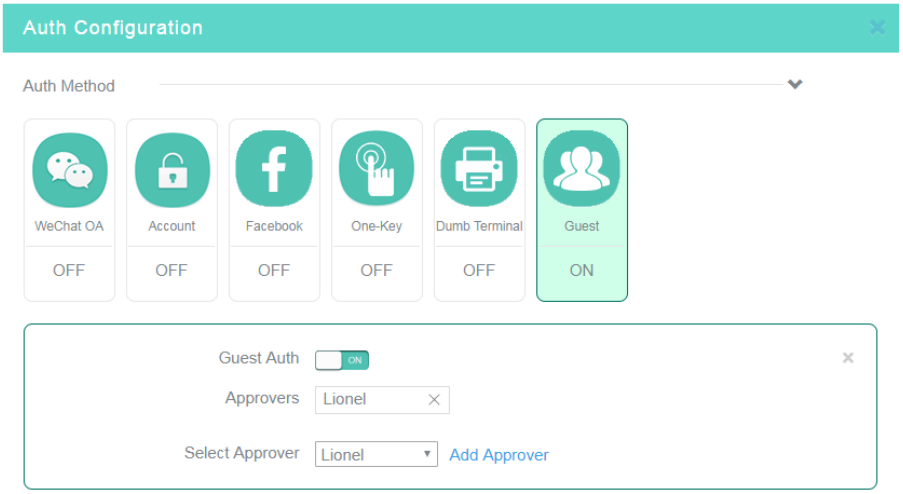


4. ナビゲーション枠で**Settings** > **ACs** > **Authentication**を選択し、ページ上部からブランチ、サイト、およびデバイスを選択します。
5. 認証テンプレートを追加するには、**Authentication Template**タブの**Add**をクリックします。認証テンプレート

を編集するには、その認証テンプレートの**Edit**アイコン をクリックします。

6. 認証テンプレートをワイヤレスサービスにバインドするには、その認証テンプレートの**Edit**アイコン をクリックし、**Bind to Wireless Service**フィールドから**Yes**を選択して、**Apply**をクリックします。テンプレートがワイヤレスサービスにバインドされている場合は、この手順を省略します。
7. 対象の認証テンプレートの**Draw**アイコン をクリックします。
8. **Auth Configuration**領域の**Guest**タイルをクリックし、ゲスト認証を有効にします。
9. 承認者を選択します。
    1. **Approvers**フィールドには、このアカウントおよびそのすべてのサブアカウントによって承認された承認者のみが表示されます。テナントの場合、**Approvers**フィールドには、そのすべてのサブアカウントによって承認された承認者が表示されます。
10. 他の認証方式を無効にします。
11. **OK**をクリックするか、ページの右上隅にある**Release**をクリックします。

図12 ゲスト認証の設定



Facebook認証の設定

Facebook認証を有効にすると、ユーザーは認証のためにFacebookログインページにリダイレクトされます。CloudnetがFacebookから自分のFacebook情報(ニックネーム、プロフィール、メール情報)を取得することを許可した場合にのみ、ネットワークにアクセスできます。

前提条件

Facebook認証を設定する前に、Facebookで次のタスクを完了する必要があります。

1. Facebookアプリケーションを作成し、アプリケーションIDを取得します。
2. クライアント**OAuth**ログインと**Web OAuth**ログインを有効にし、**OAuth**リダイレクトURIとして https://oasiscloudportal.h3c.comと入力します。

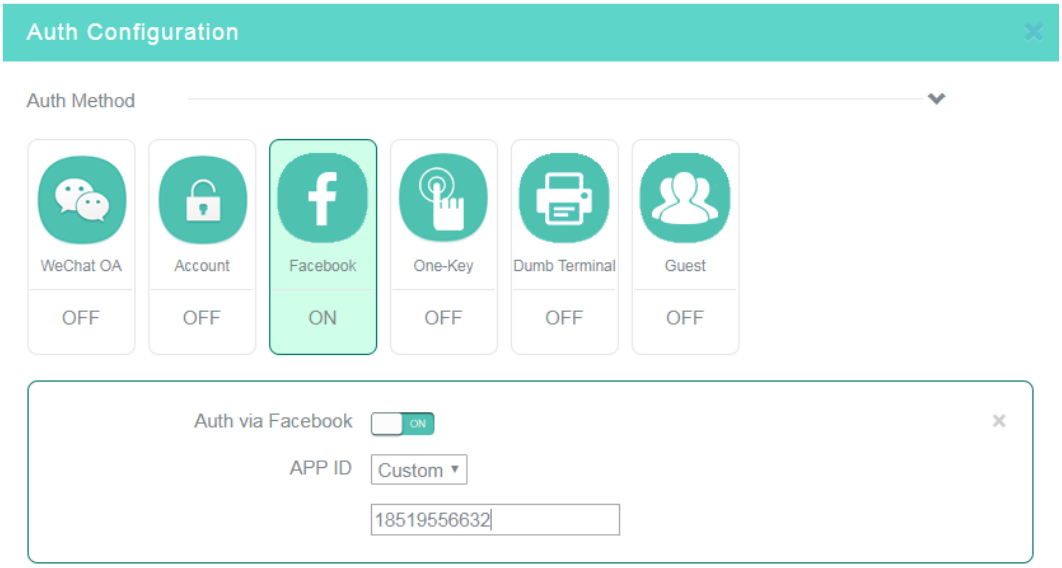
手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠で**Settings** > **ACs** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. 認証テンプレートを追加するには、**Authentication Template**タブの**Add**をクリックします。
5. 認証テンプレートを編集するには、その認証テンプレートの**Edit**アイコン をクリックします。
6. 認証テンプレートをワイヤレスサービスにバインドするには、その**Edit**アイコン をクリックします。

認証テンプレートの場合は、**Bind to Wireless Service**フィールドで**Yes**を選択し、**Apply**をクリックします。テンプレートがワイヤレスサービスにバインドされている場合は、この手順を省略します。

7. 対象の認証テンプレートの**Draw**アイコン をクリックします。
8. **Auth Configuration**領域の**Facebook**タイルをクリックし、Facebook経由の認証を有効にし、App IDを入力して、他のすべての認証方法を無効にします。
9. **OK**をクリックするか、ページの右上隅にある**Release**をクリックします。

図13 Facebook認証の設定



複合認証の設定

制限事項およびガイドライン

次の認証方式だけを併用できます。

- 固定アカウント認証。
- WeChat公式アカウント認証。
- Facebook認証。

ベストプラクティスとして、WeChat公式アカウント認証を他の認証方法と併用しないでください。
ユーザーは、1つの認証を通過する限り、ネットワークにアクセスできます。

手順

1. デバイスのソフトウェアバージョンが5405未満の場合は、”デバイスの設定を設定する”の説明に従ってデバイスの設定を設定します。
2. “WeChat公式アカウントの設定”の説明に従って、WeChat公式アカウントプラットフォームを設定します。

“アカウント認証”とは、WeChat公式アカウント認証が使用される場合を指します。

3. 少なくとも2つの認証方式を設定します(詳細は表示されません)。

ダム端末認証の設定

制限事項およびガイドライン

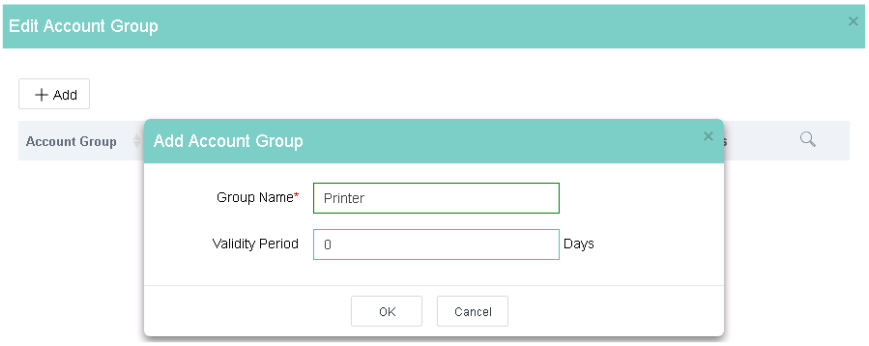
アカウントグループに認証済みアカウントが含まれている場合、アカウントグループの有効期間を変更すると、グ

ループ内のすべてのアカウントの有効期間が変更されます。
有効期間を0に設定すると、アカウントは期限切れになりません。
最初の3バイトを入力すると、MACアドレスを一括で追加できます。完全なMACアドレスの有効期間設定と3バイトMACアドレスの有効期間設定は、相互に排他的ではありません。**AA-BB-CC**で始まるMACアドレスを追加し、5日間の有効期間を指定した後、MACアドレス**AA-BB-CC-11-22-33**を追加し、10日間の有効期間を指定したとします。MACアドレスが**AA-BB-CC-11-22-33**のダム端末macアドレスが**AA-BB-CC**で始まるダム端末の有効期間は、それぞれ10日と5日です。

手順

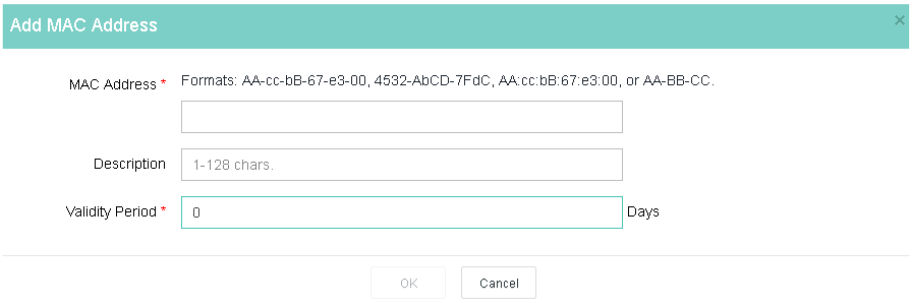
1. トップナビゲーションバーの**Service**をクリックします。
2. ナビゲーション枠で**Authentication**を選択し、**Account**タブをクリックします。
3. **Dumb Terminal Accounts**タブで、**Edit Account Group**をクリックします。
4. **Add**をクリックします。
5. 必要な情報を入力し、**OK**をクリックします。

図14 アカウントグループの追加



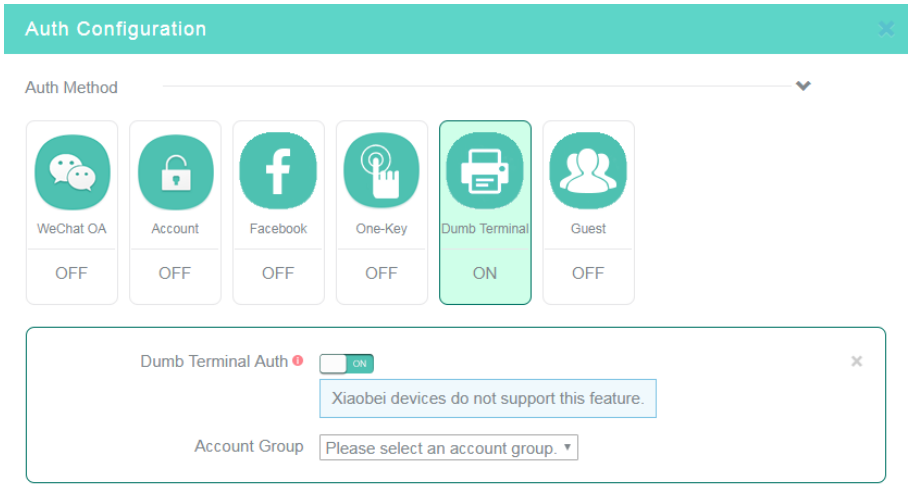
6. アカウントグループを選択し、**Add**をクリックします。
7. 必要な形式でMACアドレスを入力します。

図15 MACアドレスの追加



8. **Authentication Template**タブをクリックします。
9. 認証テンプレートを追加するには、**Add**をクリックします。認証テンプレートを編集するには、その認証テンプレートの**Edit**アイコン をクリックします。
10. 対象の認証テンプレートの**Draw** アイコンをクリックします。**Login**タブが表示されます。
11. **Auth Configuration**の**Dumb Terminal**タイルをクリックし、ダム端末認証を有効にします。
12. アカウントグループを選択します。
13. **OK**をクリックするか、ページの右上隅にある**Release**リリースをクリックします。

図16 ダム端末認証の設定



14. テンプレートを適用するには、次の手順を実行します。

a. その認証テンプレートの**Deploy Template**アイコンをクリックします。

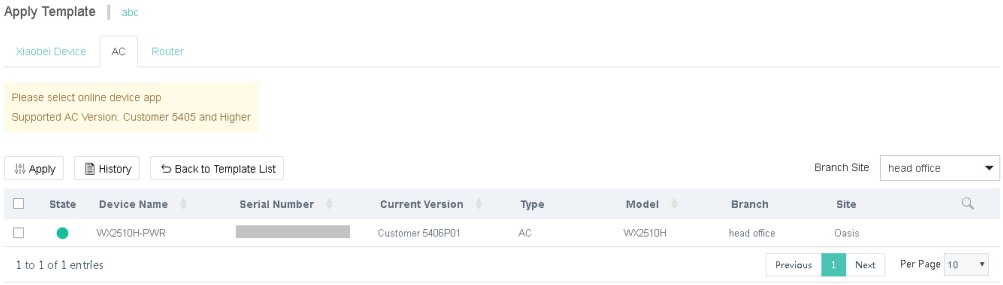
b. **ACs**タブをクリックします。

c. ブランチまたはサイトを選択します。

d. **AC**を選択し、**Apply**をクリックします。

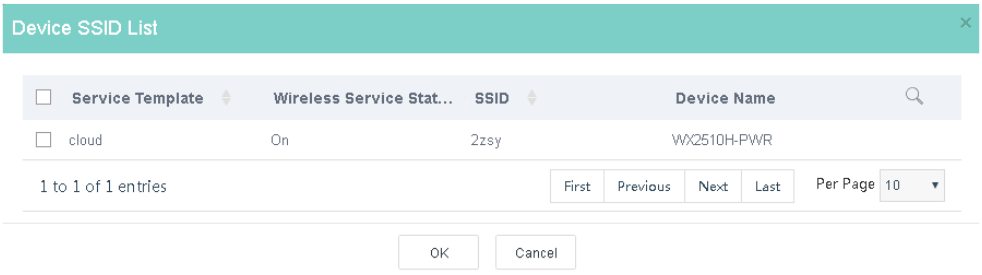
デバイスが表示されない場合は、デバイスのバージョンを確認してください。

図17 テンプレートの適用



e. サービステンプレートまたは**SSID**を選択し、**OK**をクリックします。

図18 サービステンプレートの選択



15. デバイスでMACトリガー認証をイネーブルにします。詳細については、”MACトリガー認証を設定する”を参照してください。

一括認証の設定

認証設定を一括して適用するには、次の作業を実行します。

制限事項およびガイドライン

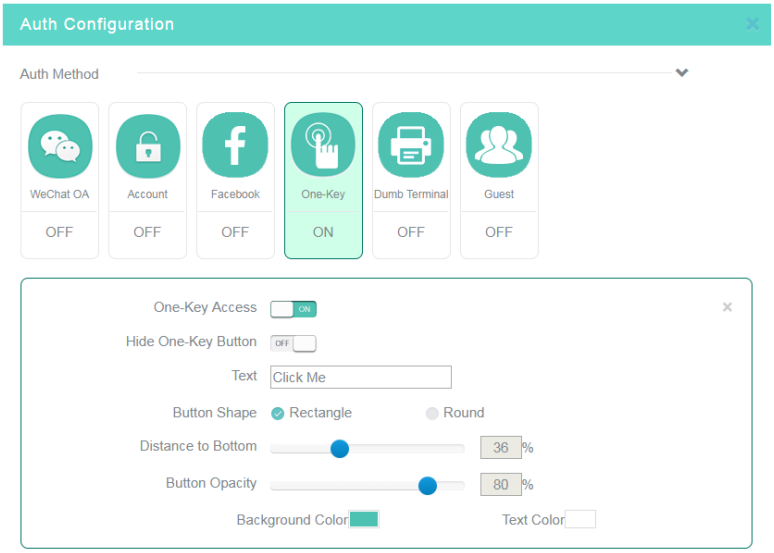
一括認証テンプレートの設定は、非一括認証テンプレートの設定よりも優先されます。非一括認証テンプレートを有効にするには、その認証テンプレートの**Edit**アイコン をクリックし、**Apply**をクリックします。
設定を一括して適用する前に、次の要件が満たされていることを確認してください。

- 一括認証が導入されているデバイスはオンラインです。デバイスがオフラインの場合、適用は失敗します。デバイスは、起動時に最新の適用済みコンフィギュレーションをロードします。
- ソフトウェアバージョンは5405以上である必要があります。
- ワイヤレスサービス名はポータルWebサーバーと同じです。

手順

1. トップナビゲーションバーの**Service**をクリックします。
2. ナビゲーション枠から**Authentication**を選択します。
3. **Authentication Template**タブで**Add**をクリックします。
4. 対象の認証テンプレートの**Draw**アイコン をクリックします。様々な認証方法の設定手順の詳細は、”基本設定の設定”を参照してください。

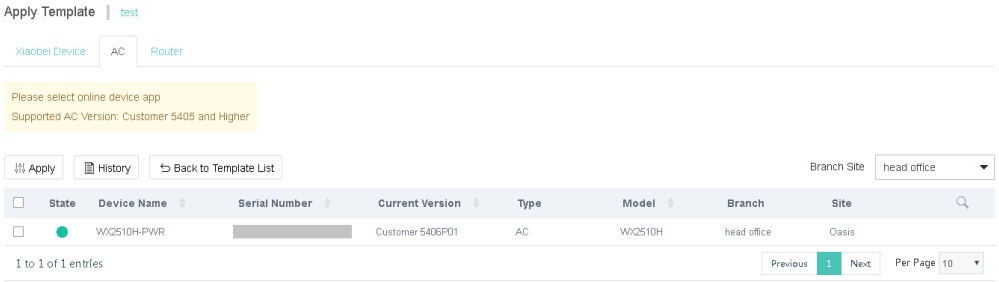
図19 一括認証の設定



5. テンプレートを適用するには、次の手順に従います。

   a. 認証テンプレートの**Deploy Template**アイコン をクリックします。
   b. **ACs**タブをクリックします。
   c. ブランチまたはサイトを選択します。
   d. **AC**を選択し、**Apply**をクリックします。
   デバイスが表示されない場合は、デバイスのバージョンを確認してください。

図20 テンプレートの適用



認証ページのカスタマイズ

ランディングページ、ログインページ、ログイン成功ページ、およびホームページを設定し、必要に応じてランディングページまたはログイン成功ページをプッシュまたはディセーブルにできます。

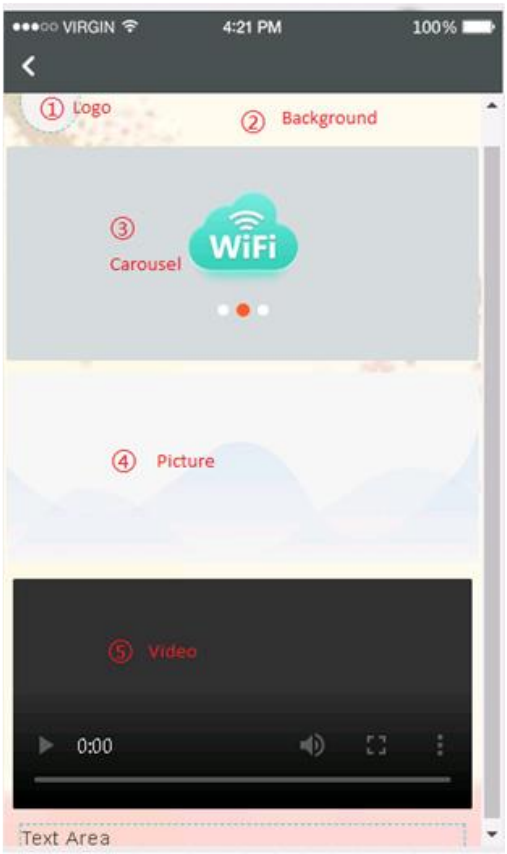
制限事項およびガイドライン

画像サイズは1Mを超えることはできません。画像サイズは100～200KBの範囲で設定することをお勧めします。
JPG、JPEG、BMP、PNG、GIF、およびSVG形式のみが許可されます。
ページの読み込み速度に影響を与えないようにするためのベストプラクティスとして、コントロールを追加しすぎないようにしてください。

手順

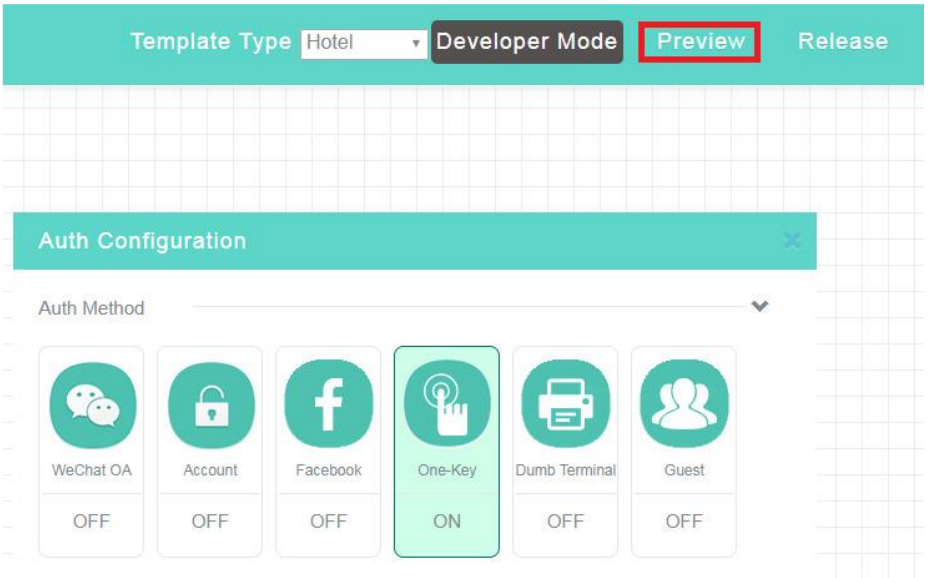
1. トップナビゲーションバーの**Service**をクリックします。
2. ナビゲーション枠から**Authentication**を選択します。
3. **Authentication Template**タブで、対象の認証テンプレートの**Draw**アイコン をクリックします。
4. 図21に示すように、次の設定を設定します。
   - **Logo**-アスペクト比は1:1でなければなりません。画像は自動的に円形に切り取られます。12文字未満のショップ名を入力できます。
   - **Background**-アスペクト比は3:5でなければなりません。
   - **Carousel**-アスペクト比は11:5でなければなりません。同じ高さの写真が2、3枚必要です。
   - **Picture**-アスペクト比は11:5である必要があります。ピクチャの説明は48文字を超えることはできません。
   - **Video**-ビデオサイズは5Mを超えることはできません。MP4、WEBM、およびOGGフォーマットのみが許可されます。
   - **Text**-フォント、フォントサイズ、太字、フォント色を編集できます。

図21 カスタムテンプレートの説明



5. ホームページを構成するには、**Home**タブをクリックし、**Use Custom Link**を選択します。
6. カスタムリンクを入力し、**Upload**をクリックします。
7. リンクをプレビューするには、ページの右上隅にある**Preview**をクリックします。

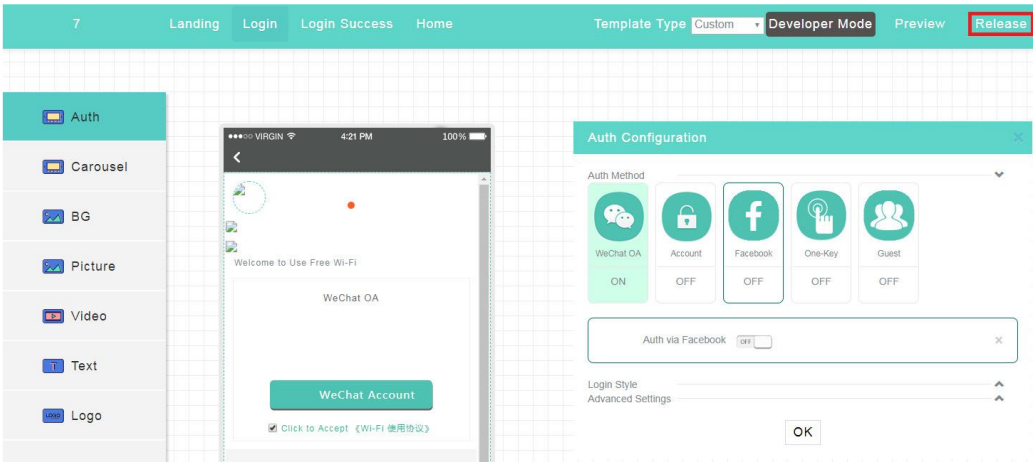
図22 設定変更のプレビュー



8. ページの右上隅にある**Release**をクリックします。

ポータル認証中にユーザーにプッシュされたホームページは、このカスタムリンクによってリダイレクトされたページに置き換えられます。

図23 カスタムテンプレートの設定



詳細設定の設定

Cloudnetは、認証管理を簡素化し、コストを削減し、マーケットプロモーションを最適化するための高度な認証設定を提供します。表3に、各認証方式で使用可能な高度な機能を示します。これらの設定は必要に応じて設定できます。

表3 高度なCloudnet認証機能

認証方式	高度な機能
ワンキー認証	キャプティブバイパス ワンキー認証ボタンの非表示とカスタマイズ インターネットアクセス設定 認証が不要 サイト間およびSSID間の再認証 インターネットアクセス制御 開発者モード ドメイン名ホワイトリストとブラックリスト 認証設定の履歴の表示とエクスポート 適用
固定アカウント認証	キャプティブバイパス 固定アカウントの一括管理 セルフサービスパスワードの変更 LDAPサーバーとの連携 ログインページの視覚効果の変更 インターネットアクセス設定 認証が不要 サイト間およびSSID間の再認証 インターネットアクセス制御 開発者モード ドメイン名ホワイトリストとブラックリスト 認証設定の履歴の表示とエクスポート 適用
WeChat公式アカウント認証	キャプティブバイパス ログインページの視覚効果設定の変更 インターネットアクセス設定

	認証が不要 サイト間およびSSID間の再認証 インターネットアクセス制御 開発者モード ドメイン名ホワイトリストとブラックリスト 認証設定の履歴の表示とエクスポート 適用
ゲスト認証	キャプティブバイパス インターネットアクセス設定 認証が不要 サイト間およびSSID間の再認証 インターネットアクセス制御 開発者モード ドメイン名ホワイトリストとブラックリスト 認証設定の履歴の表示とエクスポート 適用
Facebook認証	キャプティブバイパス ログインページの視覚効果設定の変更 インターネットアクセス設定 サイト間およびSSID間の再認証 インターネットアクセス制御 開発者モード ドメイン名ホワイトリストとブラックリスト 認証設定の履歴の表示とエクスポート 適用
ダム端末認証	キャプティブバイパス ダム端末アカウントグループの管理 インターネットアクセス制御 開発者モード ドメイン名ホワイトリストとブラックリスト 認証設定の履歴の表示とエクスポート 適用

キャプティブバイパス機能をイネーブルにする

通常、クライアントがポータル認証ネットワークにアクセスしようとすると、デバイスは自動的に認証ページをクライアントにプッシュします。キャプティブバイパス機能を使用すると、ユーザーがブラウザを起動したときにだけ、デバイスがポータル認証ページをクライアントにプッシュできます。

キャプティブバイパス機能をイネーブルにするには、デバイスで次の手順を実行する必要があります。

1. System viewを入力します。

system-view

2. WebサーバーであるcloudのポータルWebサーバービューを入力します。

portal web-server cloud

3. キャプティブパス機能をイネーブルにします。

captive-bypass enable

ワンキー認証ボタンを非表示またはカスタマイズ

ワンキー認証ボタンを非表示にするか、ボタンスタイルを変更するには、次の作業を実行します。ボタンが非表示の場合、ユーザーはログインページのカウントダウンタイマーが期限切れになると、自動的に認証を受けます。

制限事項およびガイドライン

ボタンスタイルを変更できるのは、ボタンが非表示になっていない場合だけです。

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠で**Settings** > **ACs** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. 対象の認証テンプレートの**Draw**アイコン をクリックします。
5. **Auth Configuration**領域の**One-Key**タイルをクリックし、ボタンを非表示にするかカスタマイズします。

固定アカウントの管理

固定アカウントを一括して削除、インポートまたはエクスポートするには、次のタスクを実行します。
固定アカウントを管理する手順は、次のとおりです。

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **ACs** > **Users**を選択します。
3. **Fixed Accounts**タブをクリックします。
4. **Fixed Accounts**を削除するには、ターゲット**Fixed Accounts**を選択して**Delete**をクリックします。
5. **Fixed Accounts**をインポートするには、**Import**をクリックし、テンプレートファイルをダウンロードして必要に応じてファイルに入力し、テンプレートファイルをアップロードします。
6. **Fixed Accounts**をエクスポートするには、**Export**をクリックします。

セルフサービスパスワード変更を有効にする

この機能により、ユーザーはログイン時にパスワードを変更できます。この機能を無効にすると、管理者だけが固定アカウントのパスワードを変更できます。
セルフサービスパスワード変更を有効にする手順は、次のとおりです。

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠で**Settings** > **ACs** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. 対象の認証テンプレートの**Draw**アイコン をクリックします。
5. **Auth Configuration**領域の**Account**タイルをクリックします。
6. **Change Password**を有効にします。

固定アカウント検証のためのLDAPサーバーとの連携を有効にする

ユーザーが固定アカウントを使用してWLANにアクセスしようとしたときに検証するために、Cloudnetがユーザー名とパスワードをLDAPサーバーに報告できるようにするには、次の作業を実行します。これにより、ネットワーク管理者はLDAPサーバーからCloudnetにアカウント情報をインポートする必要がなくなります。

制限事項およびガイドライン

この機能を使用するには、LDAPサーバーが設定されていることを確認します。

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠で**Setting**s > **ACs** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. 対象の認証テンプレートの**Draw**アイコン をクリックします。
5. **Auth Configuration**領域の**Account**タイルをクリックします。
6. LDAPを有効にし、必要に応じてLDAP設定を設定します。
7. **LDAP Config Verification**をクリックして、LDAP設定を検証します。

ログインページの視覚効果の設定を変更

ログインページの背景色、背景の不透明度、およびテキストの色をカスタマイズするには、次の作業を実行します。

制限事項およびガイドライン

注意:
既定の設定を復元すると、ユーザー定義の視覚効果の設定がすべて削除され、復元操作は元に戻せなくなります。この機能は注意して使用してください。

認証方式の視覚効果設定は、複数の認証方式が有効になっている場合にのみ有効になります。

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠で**Settings** > **ACs** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. 対象の認証テンプレートの**Draw**アイコン をクリックします。
5. **Auth Configuration**領域の**Login Style**メニューをクリックして適用します。
6. 必要に応じて、背景色、背景の不透明度、テキストの色を設定します。

調整はリアルタイムでプレビュー領域に表示されます。既定の視覚効果設定に戻すには、**Restore Default**をクリックします。

インターネットアクセス設定の設定

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠で**Settings** > **ACs** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. 対象の認証テンプレートの**Draw**アイコン をクリックします。

5. **Auth Configuration**領域の**Advanced Settings**メニューをクリックして適用します。
6. 必要に応じてインターネットアクセス設定を設定します。

パラメータ

- **Session Timeout:**1回の認証でのクライアントの最大連続オンライン時間。クライアントは、継続的なオンライン時間がタイムアウトを超えるとログオフされます。セッションタイムアウトは、毎日のオンライン時間より長くすることはできません。
- **Daily Online Duration:**クライアントの1日の最大オンライン時間。クライアントは、1日のオンライン時間が制限を超えるとログオフされます。毎日のオンライン時間をセッションタイムアウトより短くすることはできません。
- **Minimum Traffic and Idle Timer:**アイドルタイマー内のトラフィックが最小トラフィックしきい値に到達できなかった場合に、クライアントからログオフします。アイドルタイマーを0に設定すると、アイドルタイマー機能がディセーブルになります。

注意:
ベストプラクティスとして、アイドルタイマーをクライアントのIPアドレスリースの半分以下の値に設定し、オフラインクライアントのエントリを時間内に削除できるようにします。

- **Client Rate Limit**:アップリンクおよびダウンリンククライアントトラフィックの制限レート。この機能は、5417P01以降のバージョンでサポートされています。

- **HTTPS for Landing and Login: Landing and Login**ページにHTTPSセッションを使用します。
- **Permit PC**:PCがWLANにアクセスできるようにします。Facebook認証はこの機能をサポートしていません。

ダム端末アカウントグループの管理

ダム端末アカウントグループを作成、削除、または編集し、ダム端末アカウントをインポートまたはエクスポートするには、次の作業を実行します。
ダム端末認証をイネーブルにしてアカウントグループを指定すると、グループ内のダム端末だけがWLANにアクセスできます。
ダム端末アカウントグループを管理するには:
1. トップナビゲーションバーの**Service**をクリックします。
2. ナビゲーション枠で**Authentication**を選択します。**Accounts**タブをクリックします。
3. **Dumb Terminal Accounts**タブでダムターミナルアカウントグループを設定します。

ポータル自動認証の設定

この機能を使用すると、認証済みのユーザーは、無認証期間内に再認証を行わずにネットワークにアクセスできます。次のモードを使用できます。

- **Portal redirection -** このモードでは、ユーザーはブラウザを実行して自動ポータル認証をトリガーする必要があります。このモードでは、クライアントに広告をプッシュすることができます。
- **MAC-trigger** - このモードでは、ユーザーはブラウザを実行せずにWLANにアクセスできます。このモードでは、クライアントに広告をプッシュすることはできません。

ポータルリダイレクト認証の設定

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠で**Settings** > **ACs** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。

4. 対象の認証テンプレートの**Draw**アイコン をクリックします。
5. Auth Configuration領域の**Advanced Settings**メニューをクリックして適用します。
6. **Auth-Free**タブをクリックし、**Free Auth**機能を設定します。

MACトリガー認証の設定

1. ポータルリダイレクション認証を設定します。詳細については、”ポータルリダイレクト認証を設定する”を参照してください。
2. デバイスでMACトリガー認証を設定します。
a. MACバインディングサーバーを設定します。

注意:
この手順は、5405より前のバージョンでのみ実行してください。バージョン5405以降では、デバイスへの自動認証設定適用がサポートされているため、この手順でコマンドを手動で設定する必要はありません。

#MACバインディングサーバーを作成し、そのビューを入力します。
<Sysname> system-view
[Sysname] portal mac-trigger-server cloud
#クラウドMACトリガー認証を有効にします。MACバインディングクエリーの最大試行回数を2に設定し、クエ
#リー間隔を3秒に設定します。
[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

b.MACバインディングサーバークラウドをサービステンプレートクラウドに適用します。
[Sysname] wlan service-template cloud
[Sysname-wlan-st-cloud] portal apply mac-trigger-server cloud

サイト間およびSSID間の再認証の設定

この機能を使用すると、認証されたクライアントは、再認証を行わずに、異なるサイトに関連付けられたワイヤレスサービス間、または同じサイトの異なるSS ID間でローミングできます。これらのワイヤレスサービスでは、同じ認証テンプレートを使用するか、同じSSIDを使用する必要があります。

制限事項およびガイドライン

この機能は、App Centerで設定された認証テンプレートでのみ使用できます。

手順

1. トップナビゲーションバーの**Service**をクリックします。
2. ナビゲーション枠で**Authentication**を選択します。
3. 対象の認証テンプレートの**Draw**アイコン をクリックします。
4. **Auth Configuration**領域の**Advanced Settings**メニューをクリックして適用します。
5. **Auth-free**タブをクリックし、**Free Auth**を有効にします。
6. サイト間およびSSID間の再認証を設定します。

インターネットアクセス制御の設定

ユーザーがWLANにアクセスできる時間範囲を指定するには、次の作業を実行します。

制限事項およびガイドライン

インターネットアクセス制御は時間単位で行われます。1日に最大5つの時間範囲を指定できます。24時に終了する時間範囲を指定するには、終了時間を00に設定します。1日の時間範囲を00～00に設定すると、ユーザーはその日いつでもインターネットにアクセスできます。

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠で**Settings** > **ACs** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. 対象の認証テンプレートの**Draw**アイコン をクリックします。
5. **Auth Configuration**領域の**Advanced Settings**メニューをクリックして適用します。
6. **Internet Access Control**タブをクリックし、時間範囲を指定します。

開発者モードの設定

注意:
既存の機能のコードを編集すると、Cloudnet認証が無効になる場合があります。この機能は注意して使用してください。

開発者モードでは、カスタマイズの目的で認証テンプレートのソースコードを変更できます。

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠で**Settings** > **ACs** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. 対象の認証テンプレートの**Draw**アイコン をクリックします。
5. 右上隅にある**Developer Mode**をクリックします。

ドメイン名のホワイトリストとブラックリストの設定

制限事項およびガイドライン

この機能は、ワイヤレス認証が設定されている場合にだけ有効です。

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠で**Settings** > **ACs** > **Authentication**を選択します。
3. **Domain Name Whitelist**または**Domain Name Blacklist**タブをクリックして、ホワイトリストまたはブラックリストを設定します。

認証テンプレートデプロイメントの履歴の表示またはエクスポート

現在、過去7日間、または過去30日間におけるすべての認証テンプレートの適用または適用の履歴を表示するには、次の作業を実行します。
認証テンプレートデプロイメントの履歴を表示またはエクスポートする手順は、次のとおりです:

1. トップナビゲーションバーの**Service**をクリックします。
2. ナビゲーション枠で**Authentication**を選択します。
3. **Authentication Template**タブで、対象の認証テンプレートの**Apply**アイコン  をクリックします。
4. **ACs**タブをクリックして、ACの適用履歴を表示します。

無線ルーターを認証装置として使用したCloudnet認証の設定

基本設定の設定

前提条件

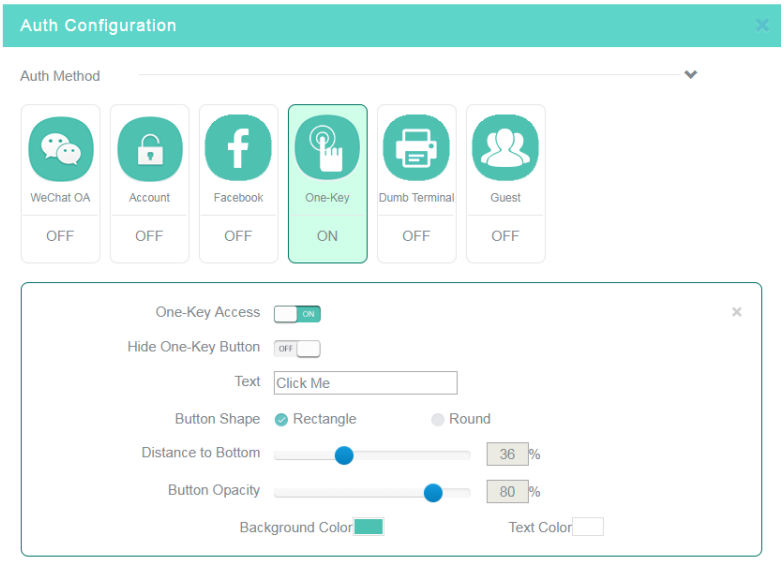
Cloudnet認証を設定する前に、次の作業を実行します。

- 装置をCloudnetに接続する。
  詳細については、”H3C Cloudnet導入ガイド”を参照してください。
- VLANとDHCPの設定を完了します。
- ワイヤレスサービスを設定し、APがオンラインになることを確認します。

ワンキー認証の設定

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Routers** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. 認証テンプレートを追加するには、Wireless Authentication Templatesタブの**Add**をクリックします。
5. 認証テンプレートを編集するには、その認証テンプレートの**Edit**アイコン をクリックします。
6. 認証テンプレートをワイヤレスサービスにバインドするには、その認証テンプレートのEditアイコン をクリックし、**Bind to Wireless Service**フィールドにバインド**Bind to Wireless Service**フィールドから**Yes**を選択して、**Apply**をクリックします。テンプレートがワイヤレスサービスにバインドされている場合は、この手順を省略します。
7. 対象の認証テンプレートの**Draw**アイコン をクリックします。
8. **Auth Configuration**領域の**One-Key**タイルをクリックし、ワンキー認証をイネーブルにして、必要に応じてその他の設定を行います。
9. **OK**をクリックするか、ページの右上隅にある**Release**をクリックします。

図24 ワンキー認証の設定



固定アカウント認証の設定

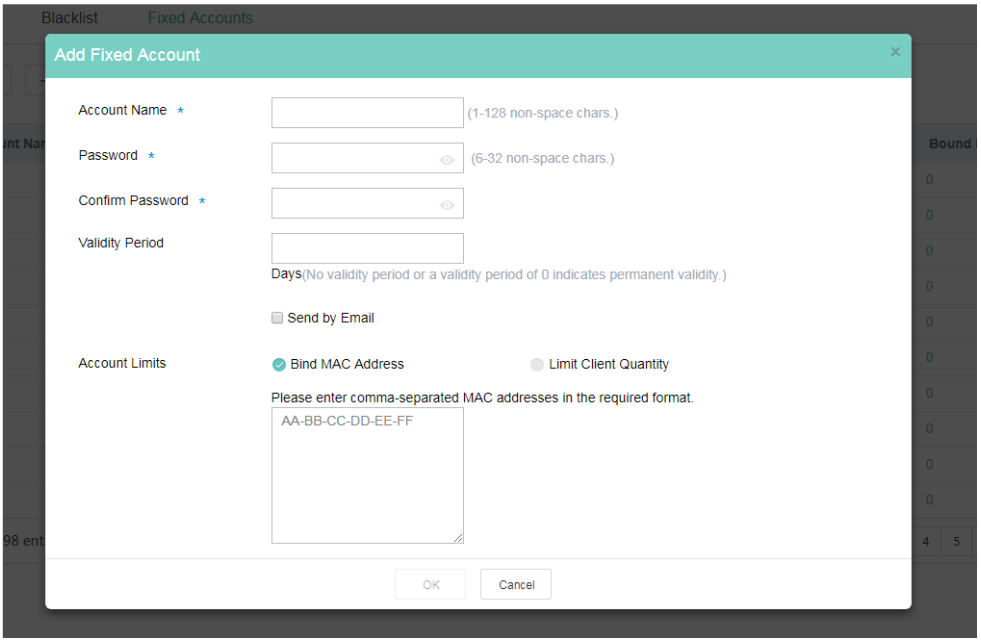
制限事項およびガイドライン

有効期間を設定しない場合、または有効期間を0に設定しない場合、アカウントは期限切れになりません。
Bind MAC Addressを選択し、MACアドレスを入力しない場合、固定アカウントを使用するクライアントは制限されません。
Send by Emailを選択すると、指定した電子メールアドレスにアカウント名とパスワードが送信されます。電子メールアドレスの数は10を超えることはできず、コンマで区切る必要があります。

手順

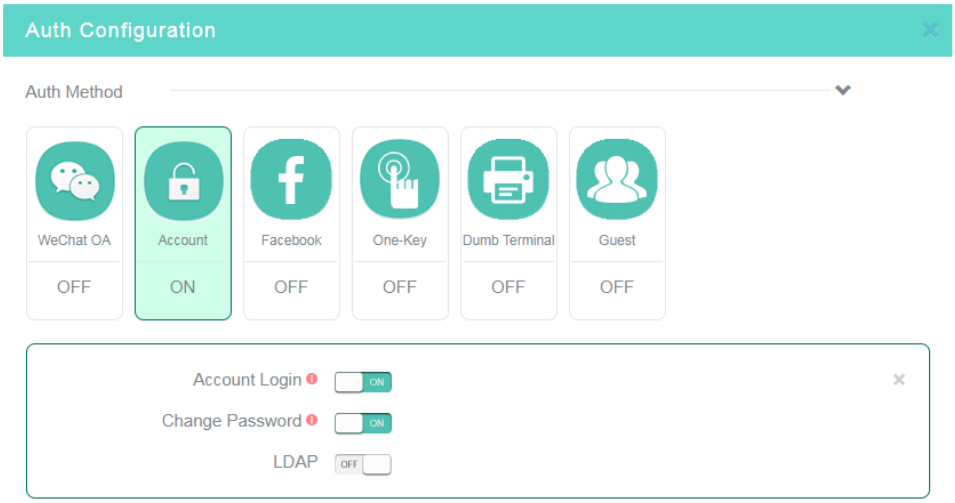
1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Routers** > **Users**を選択します。
3. **Fixed Accounts**タブをクリックします。
4. **Add**をクリックします。
5. 必要に応じて固定アカウント情報を設定します。

図25 固定アカウントの追加



6. 認証テンプレートを追加または編集するには、ナビゲーション枠で**Settings** > **Routers** > **Authentication**を選択し、ページの上部からブランチ、サイト、およびデバイスを選択します。テンプレートを追加するには、**Wireless Authentication Templates**タブの**Add**をクリックします。テンプレートを編集するには、その認証テンプレートの**Edit**アイコン をクリックします。
7. 認証テンプレートをワイヤレスサービスにバインドするには、その認証テンプレートの**Edit**アイコン をクリックし、**Bind to Wireless Service**フィールドから**Yes**を選択して、**Apply**をクリックします。テンプレートがワイヤレスサービスにバインドされている場合は、この手順を省略します。
8. 対象の認証テンプレートの**Draw**アイコン をクリックします。
9. **Auth Configuration**領域の**Account**タイルをクリックし、固定アカウント認証を有効にして、必要に応じて他の設定を行います。
10. 他の認証方式を無効にします。
11. **OK**をクリックするか、ページの右上隅にある**Release**をクリックします。

図26 固定アカウント認証の設定



WeChat公式アカウント認証の設定

制限事項およびガイドライン

テナントは、Tencentによって認証されたWeChatサービスアカウントを持っていなければならない。WeChat公式アカウントプラットフォームを設定します。

1. 適用されたWeChatサービスアカウントを使用して、https://mp.weixin.qq.com/のWeChat公式アカウントプラットフォームにアクセスします。

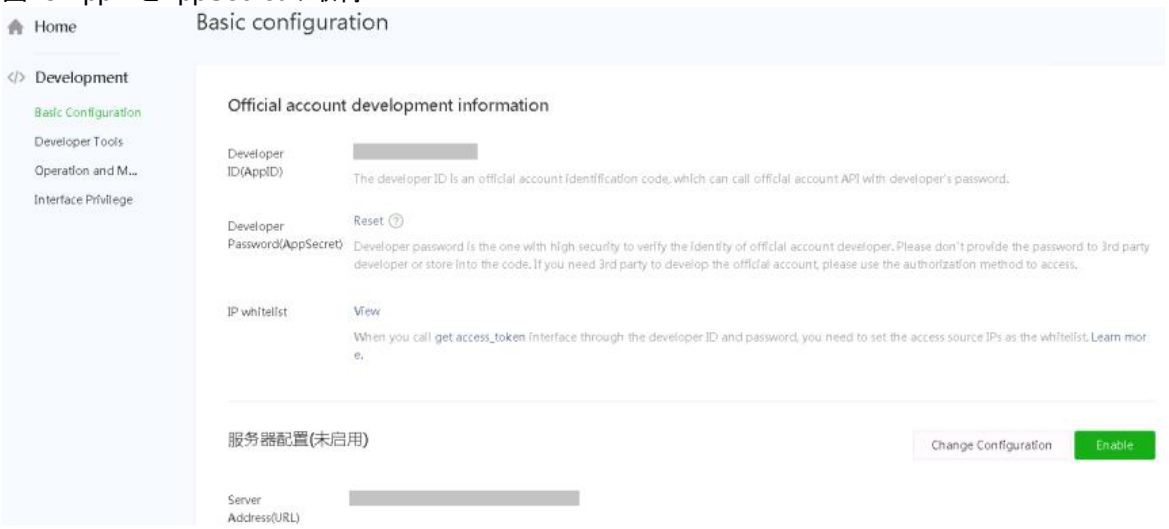
図27 サービスアカウントへのログイン

2. ナビゲーション枠で**Development** > **Basic Configuration**を選択します。

a. 開いたページで、AppIDとAppSecretを取得します。

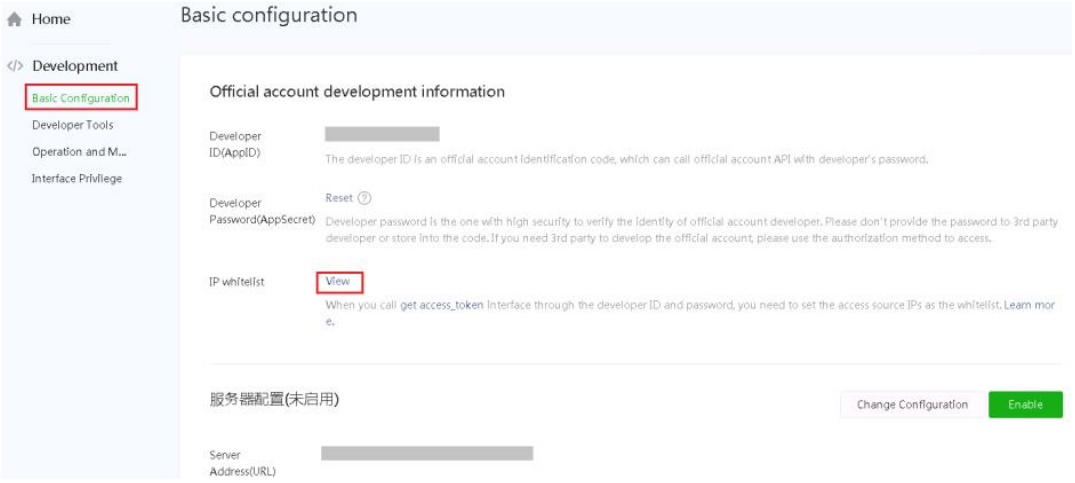
AppSecretを有効にして生成した後、WeChat公式アカウントプラットフォームは**AppSecret**を保存したり表示したりはしませんので、必ず保存してください。

図28 AppIDとAppSecretの取得



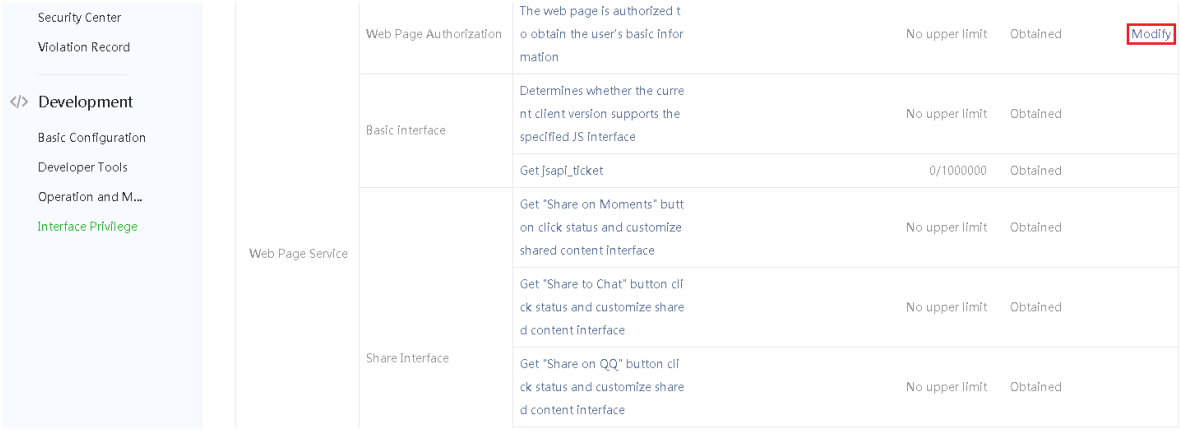
a. IPアドレス139.217.7.53、139.217.17.204、および139.219.0.33をIPホワイトリストに追加します。

図29 ホワイトリストへのIPアドレスの追加



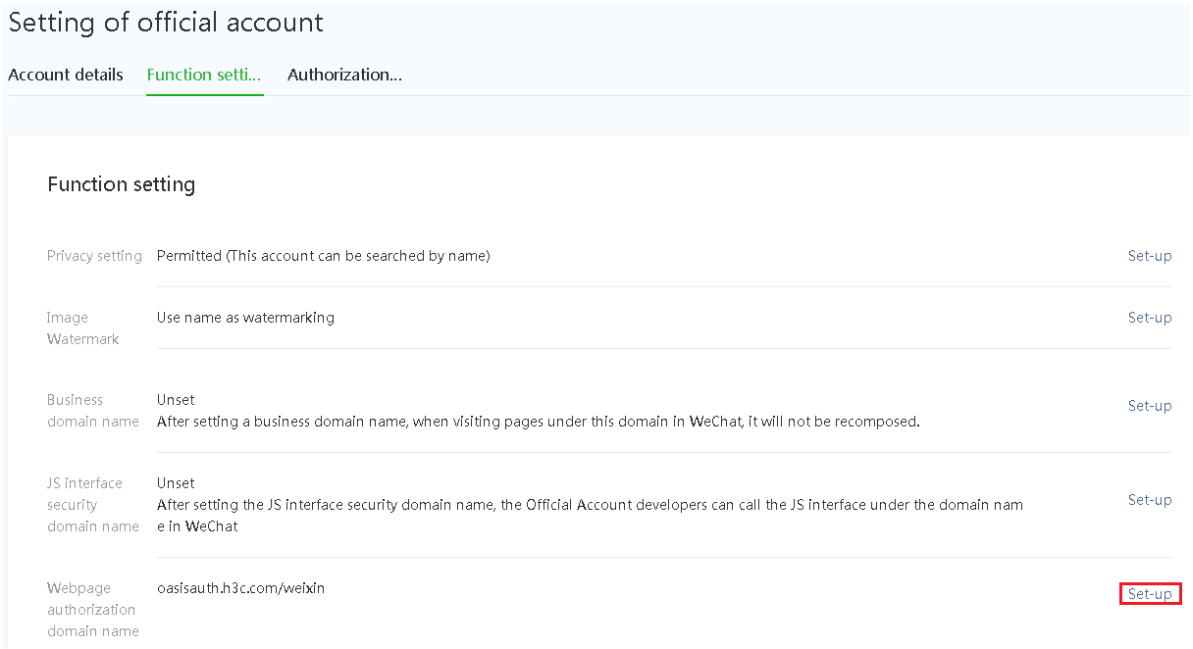
3. ナビゲーション枠で**Development** > **Interface Privilege**を選択し、**Web Page Authentication**フィールドで**Modify**をクリックします。

図30 Webページ認証の変更



4. **Function Setting**タブで、**webpage authentication domain name**フィールドの**Set-up**をクリックします。

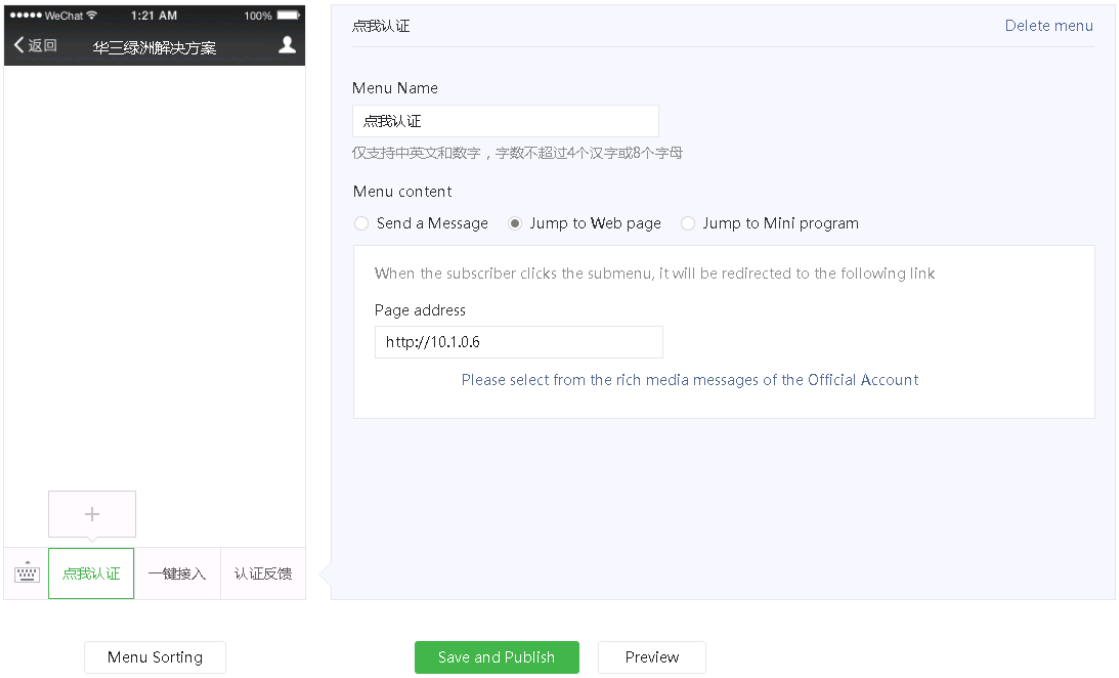
図31 Webページの編集ドメイン名の認証



5. ナビゲーション枠から**Function** > **Custom Menu**を選択し、追加アイコン+をクリックして、必要に応じて他の設定を設定します。

ベストプラクティスとして、**Page address**フィールドにhttp://10.168.168.1inと入力します。

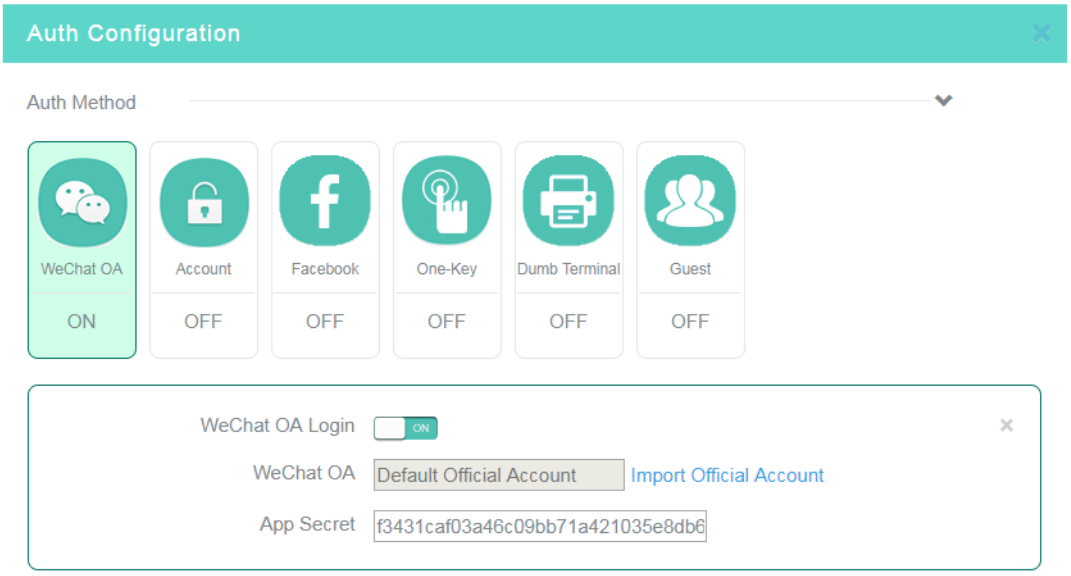
図32 メニューの指定



WeChat公式アカウント認証の設定

1. ナビゲーション枠から**Settings** > **Routers** > **Authentication**を選択します。
2. ページ上部からブランチ、サイトおよびデバイスを選択します。
3. 認証テンプレートを追加するには、**Wireless Authentication Templates**タブの**Add**をクリックします。
6. 認証テンプレートを編集するには、その認証テンプレートの**Edit**アイコン をクリックします。
4. 認証テンプレートをワイヤレスサービスにバインドするには、その認証テンプレートの**Edit**アイコン をクリックし、**Bind to Wireless Service**フィールドから**Yes**を選択して、**Apply**をクリックします。テンプレートがワイヤレスサービスにバインドされている場合は、この手順を省略します。
5. 対象の認証テンプレートの**Draw**アイコン をクリックします。
6. **Auth Configuration**エリアのWeChat OAタイルをクリックし、WeChat公式アカウント認証を有効にします。
7. **Import Official Account**をクリックして、QRコードをスキャンします。
8. AppSecretを入力します。
9. 他の認証方式を無効にします。
10. **OK**をクリックするか、ページの右上隅にある**Release**をクリックします。

図33 WeChat公式アカウント認証の設定



ゲスト認証の設定

制限事項およびガイドライン

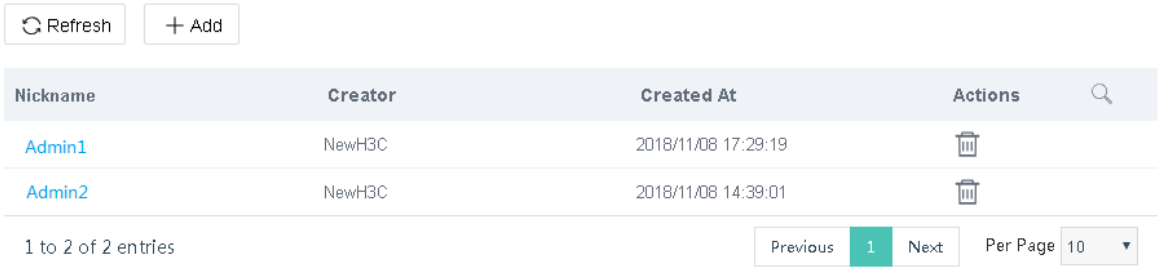
設定後、ゲストがネットワークにアクセスできるのは、承認者がクライアント上のQRコードをスキャンしてクライアントを認証した後だけです。QRコードは5分間有効です。QRコードが期限切れになると、ゲストはQRコードを更新する必要があります。

手順

1. トップナビゲーションバーの**Service**をクリックします。
2. ナビゲーション枠から**Authentication**を選択します。**Accounts**タブをクリックします。
3. **Guest Account**tタブをクリックし、**Add**をクリックします。

承認者は、承認者がQRコードをスキャンしコードを入力した後に追加されます。承認者が削除されると、Cloudnetは自動的に承認者から権限を削除します。

図34 承認者の追加



4. ナビゲーション枠で**Settings** > **Routers** > **Authentication**を選択し、ページの上部からブランチ、サイト、およびデバイスを選択します。
5. 認証テンプレートを追加するには、**Wireless Authentication Templates**タブの**Add**をクリックします。

認証テンプレートを編集するには、その認証テンプレートの**Edit**アイコン をクリックします。

6. 認証テンプレートをワイヤレスサービスにバインドするには、その認証テンプレートの**Edit**アイコン をクリッ

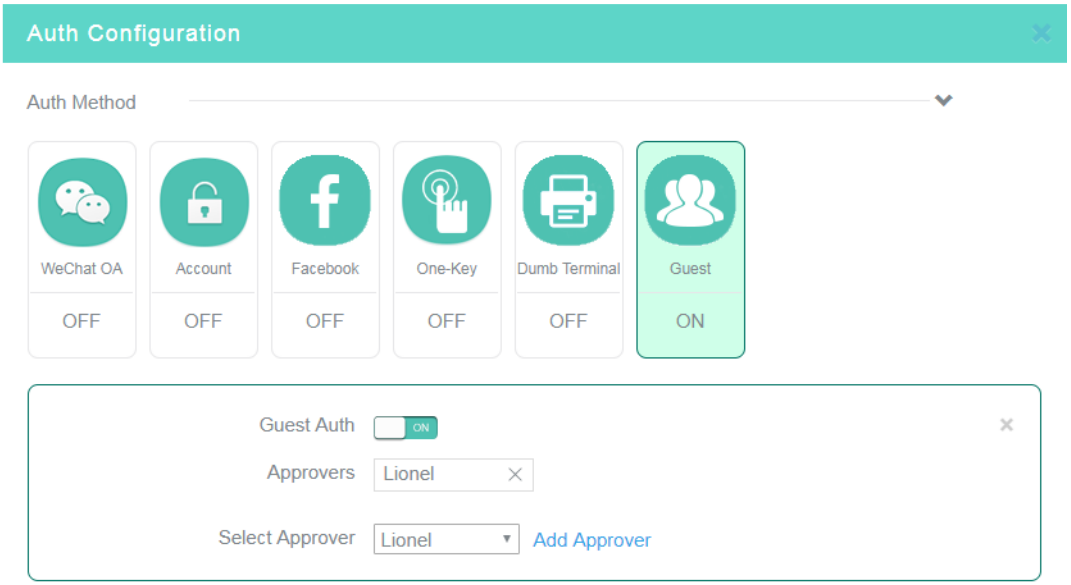
クし、**Bind to Wireless Service**フィールドから**Yes**を選択して、**Apply**をクリックします。テンプレートがワイヤレスサービスにバインドされている場合は、この手順を省略します。

7. 対象の認証テンプレートの**Draw**アイコン をクリックします。
8. **Auth Configuration**領域の**Guest**タイルをクリックし、ゲスト認証を有効にします。
9. 承認者を選択します。

Approverフィールドには、このアカウントおよびそのすべてのサブアカウントによって承認された承認者のみが表示されます。テナントの場合、**Approvers**フィールドには、そのすべてのサブアカウントによって承認された承認者が表示されます。

10. 他の認証方式を無効にします。
11. **OK**をクリックするか、ページの右上隅にある**Release**をクリックします。

図35 ゲスト認証の設定



複合認証の設定

制限事項およびガイドライン

次の認証方式だけを併用できます。

- 固定アカウント認証。
- WeChat公式アカウント認証。
- Facebook認証。

ベストプラクティスとして、WeChat公式アカウント認証を他の認証方法と併用しないこと。
ユーザーは、1つの認証を通過する限り、ネットワークにアクセスできます。

手順

少なくとも2つの認証方式を設定します。(詳細は表示されません)。

ダム端末認証の設定

制限事項およびガイドライン

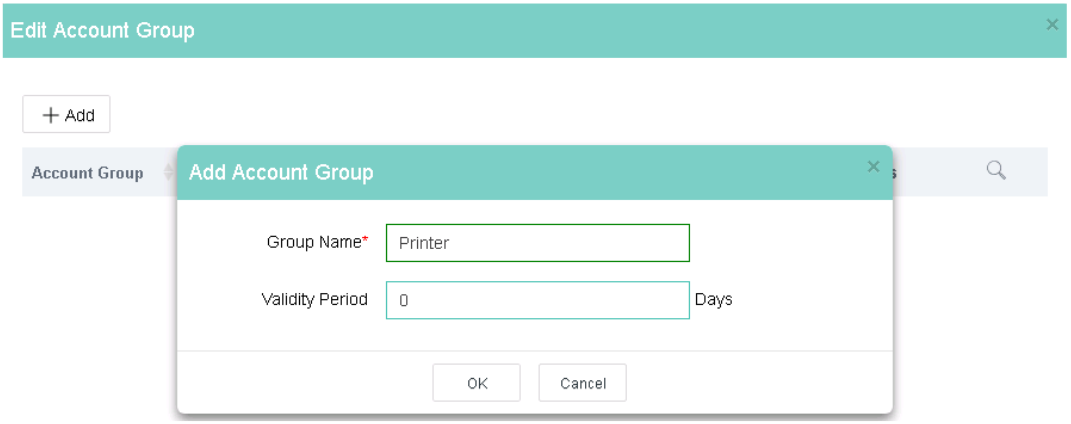
アカウントグループに認証済みアカウントが含まれている場合、アカウントグループの有効期間を変更すると、グ

ループ内のすべてのアカウントの有効期間が変更されます。
有効期間を0に設定すると、アカウントは期限切れになりません。
最初の3バイトを入力すると、MACアドレスを一括で追加できます。完全なMACアドレスの有効期間設定と3バイトMACアドレスの有効期間設定は、相互に排他的ではありません。**AA-BB-CC**で始まるMACアドレスを追加し、5日間の有効期間を指定した後、MACアドレス**AA-BB-CC-11-22-33**を追加し、10日間の有効期間を指定したとします。MACアドレスが**AA-BB-CC-11-22-33**のダム端末macアドレスが**AA-BB-CC**で始まるダム端末の有効期間は、それぞれ10日と5日です。

手順

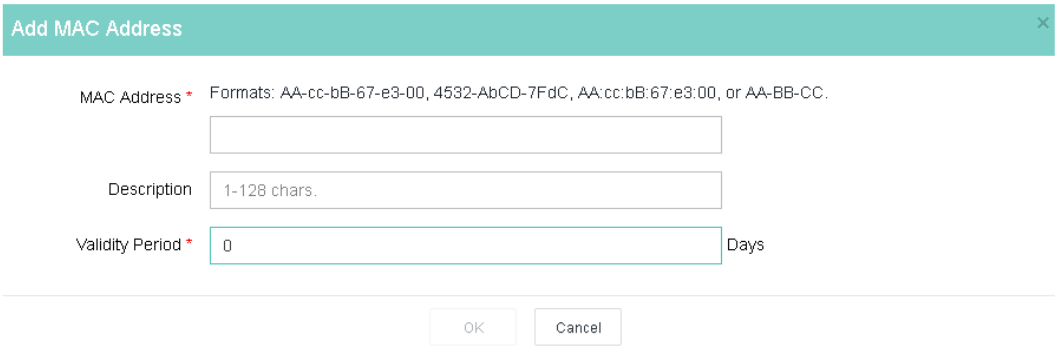
1. トップナビゲーションバーの**Service**をクリックします。
2. ナビゲーション枠で**Authentication**を選択し、**Accounts**タブをクリックします。
3. **Dumb Terminal Accounts**タブで、**Edit Account Group**をクリックします。
4. **Add**をクリックします。
5. 必要な情報を入力し、**OK**をクリックします。

図36 アカウントグループの追加



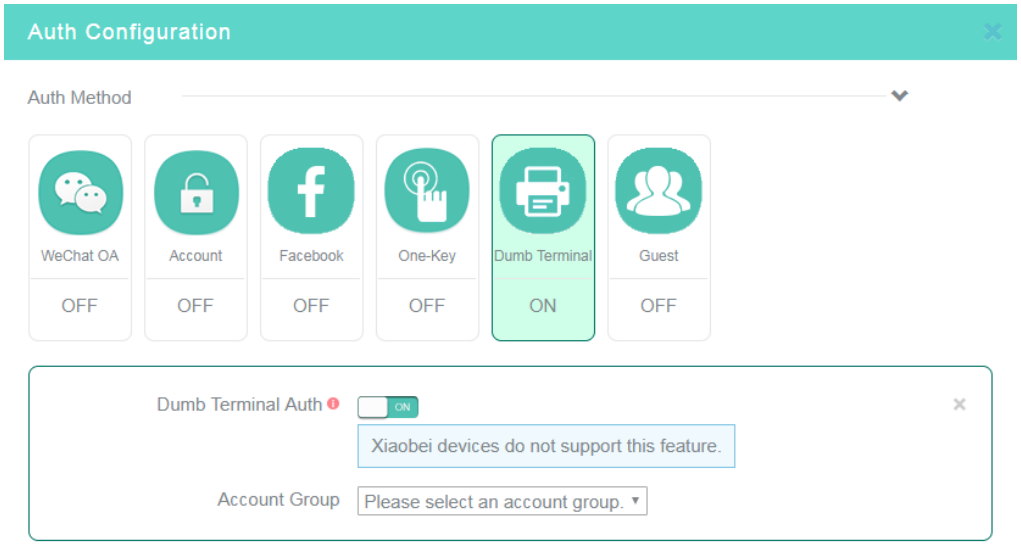
6. アカウントグループを選択し、**Add**をクリックします。
7. 必要な形式でMACアドレスを入力します。

図37 MACアドレスの追加



8. **Authentication Templates**タブをクリックします。
9. 認証テンプレートを追加するには、**Add**をクリックします。認証テンプレートを編集するには、その認証テンプレートの**Edit**アイコン をクリックします。
10. 対象の認証テンプレートの**Draw**アイコン をクリックします。**Login**タブが表示されます。
11. **Auth Configuration**の**Dumb Terminal**タイルをクリックし、ダム端末認証を有効にします。
12. 勘定科目グループを選択します。
13. **OK**をクリックするか、ページの右上隅にある**Release**をクリックします。

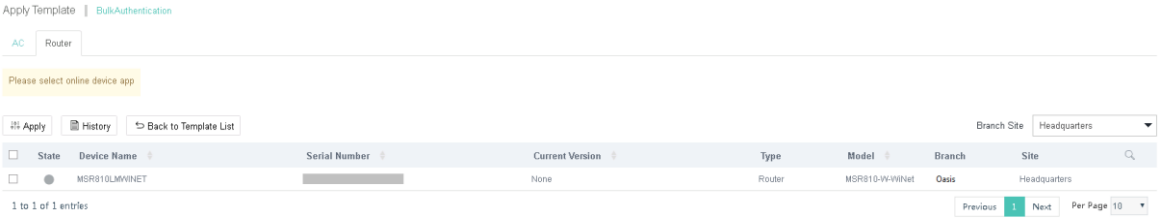
図38 ダム端末認証の設定



14. テンプレートを適用するには、次の手順を実行します。

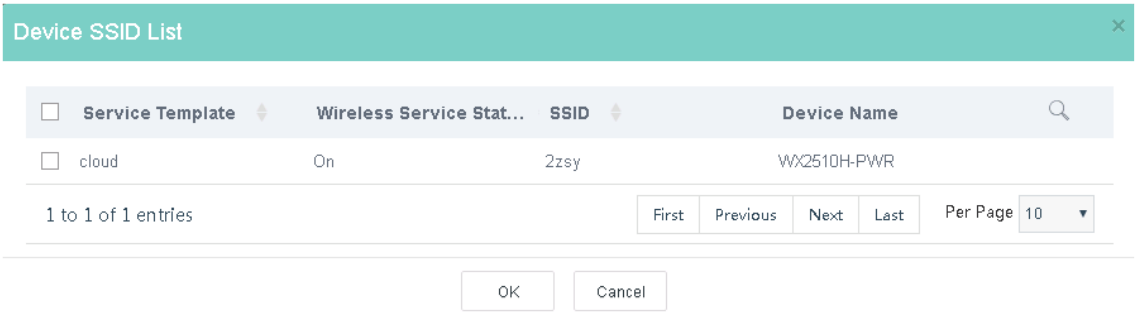
a. その認証テンプレートの**Deploy Template**アイコン をクリックします。
b. **Router**タブをクリックします。
c. ブランチまたはサイトを選択します。
d. デバイスを選択し、**Apply**をクリックします。
デバイスが表示されない場合は、デバイスのバージョンを確認してください。

図39 テンプレートの適用



a. サービステンプレートまたは**SSID**を選択し、**OK**をクリックします。

図40 サービステンプレートの選択



15. デバイスでMACトリガー認証をイネーブルにします。詳細については、”MACトリガー認証の設定” を参照してください。

一括認証の設定

認証設定を一括して適用するには、次の作業を実行します。

制限事項およびガイドライン

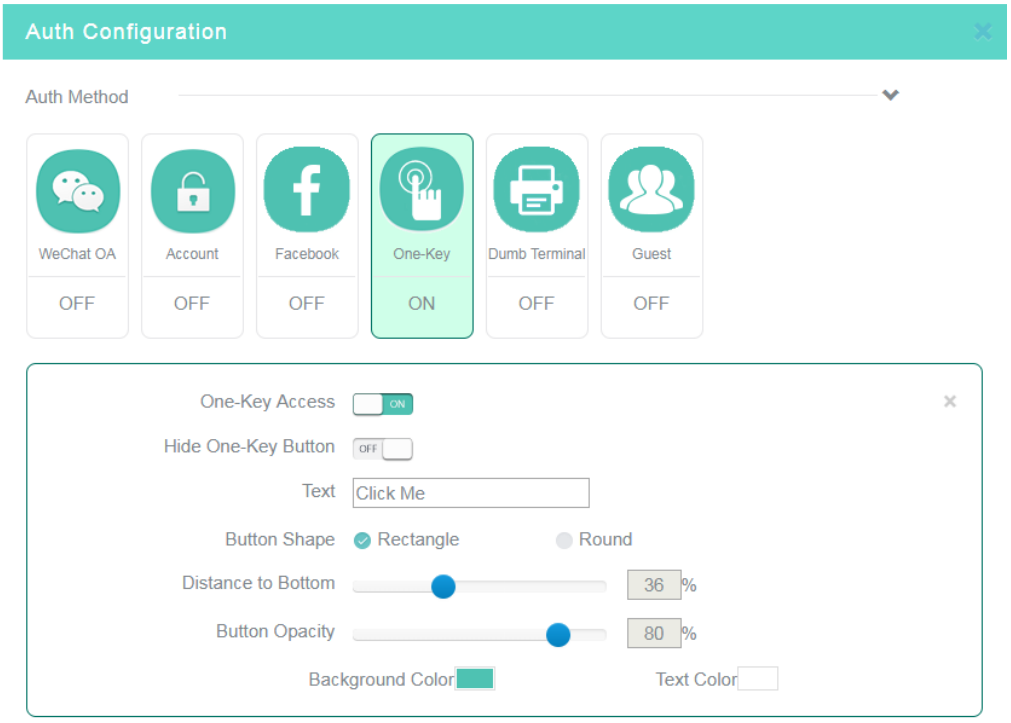
一括認証テンプレートの設定は、非一括認証テンプレートの設定よりも優先されます。非一括認証テンプレートを有効にするには、その認証テンプレートの**Edit**アイコンをクリックし、**Apply**をクリックします。
設定を一括して適用する前に、次の要件が満たされていることを確認してください。

- 一括認証が導入されるデバイスはオンラインです。デバイスがオフラインの場合、そのデバイスの適用は失敗します。デバイスは、起動時に最新の適用済みコンフィギュレーションをロードします。
- ワイヤレスサービス名はポータルWebサーバーと同じです。

手順

1. トップナビゲーションバーの**service**をクリックします。
2. ナビゲーション枠で**Authentication**を選択します。
3. 対象の認証テンプレートの**Draw**アイコン をクリックします。様々な認証方式の設定手順の詳細は、”基本設定の設定”を参照してください。

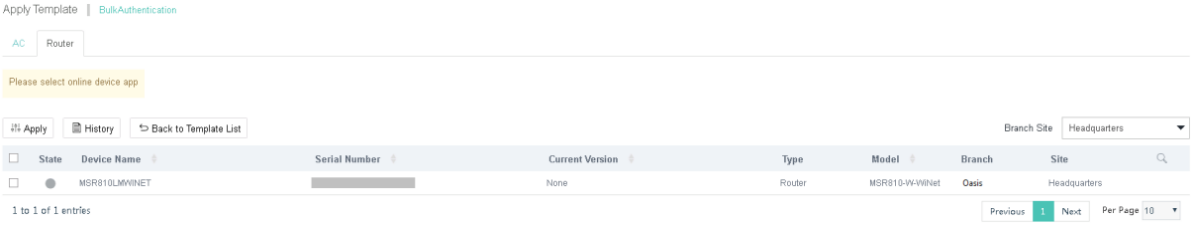
図41 一括認証の設定



4. テンプレートを適用するには、次の手順を実行します。

a. 認証テンプレートの**Deploy Template**アイコン をクリックします。
b. **Router**タブをクリックします。
c. ブランチまたはサイトを選択します。
d. デバイスを選択し、**Apply**をクリックします。
デバイスが表示されない場合は、デバイスのバージョンを確認してください。

図42 テンプレートの適用



認証ページのカスタマイズ

ランディングページ、ログインページ、ログイン成功ページ、およびホームページを設定し、必要に応じてランディングページまたはログイン成功ページをプッシュまたはディセーブルにできます。

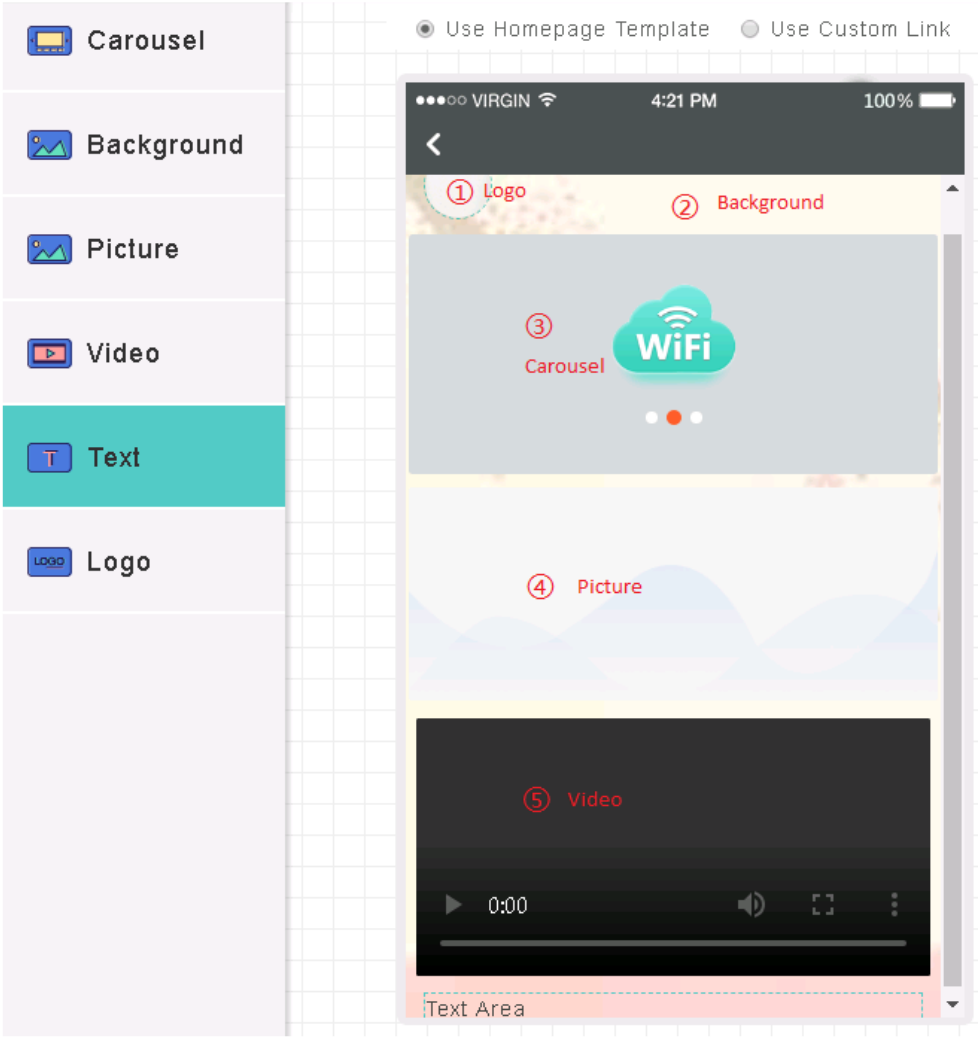
制限事項およびガイドライン

画像サイズは1Mを超えることはできません。画像サイズは100～200KBの範囲で設定することをお勧めします。JPG、JPEG、BMP、PNG、GIF、およびSVG形式のみが許可されます。
ページの読み込み速度に影響を与えないようにするためのベストプラクティスとして、コントロールを追加しすぎないようにしてください。

手順

1. トップナビゲーションバーの**Service**をクリックします。
2. ナビゲーション枠で**Authentication**を選択します。
3. **Authentication Templates**タブで、対象の認証テンプレートの**Draw**アイコン をクリックします。
4. 図43に示すように、次の設定を設定します。
   - **Logo** – アスペクト比は1:1でなければなりません。画像は自動的に円形に切り取られます。12文字未満のショップ名を入力できます。
   - **Background** – アスペクト比は3:5でなければなりません。
   - **Carousel** – アスペクト比は11:5でなければなりません。同じ高さの写真が2、3枚必要です。
   - **Picture** – アスペクト比は11:5である必要があります。ピクチャの説明は48文字を超えることはできません。
   - **Video** – ビデオサイズは5Mを超えることはできません。MP4、WEBM、およびOGGフォーマットのみが許可されます。
   - **Text** – フォント、フォントサイズ、太字、フォント色を編集できます。

図43 カスタムテンプレートの説明

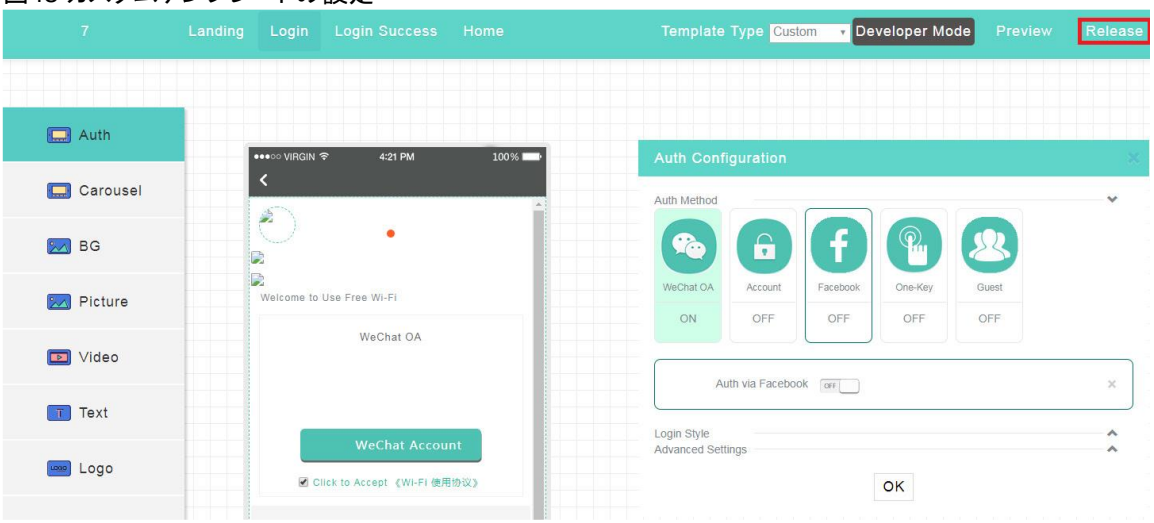


5. ホームページを設定するには、**Home**タブをクリックし、**Use Custom Link**を選択します。
6. カスタムリンクを入力し、**Upload**をクリックします。
7. リンクをプレビューするには、ページの右上隅にある**Preview**をクリックします。

図44 設定変更のプレビュー

8. ページの右上隅にある**Release**をクリックします。
ポータル認証中にユーザーにプッシュされたホームページは、このカスタムリンクによってリダイレクトされたページに置き換えられます。

図45 カスタムテンプレートの設定



詳細設定の設定

Cloudnetは、認証管理を簡素化し、コストを削減し、マーケットプロモーションを最適化するための高度な認証設定を提供します。表5に、各認証方式で使用可能な高度な機能を示します。これらの設定は必要に応じて設定できます。

表4 高度なCloudnet認証機能

認証方式	高度な機能
ワンキー認証	キャプティブバイパス ワンキー認証ボタンの非表示とカスタマイズ インターネットアクセス設定 認証が不要 サイト間およびSS ID間の再認証 インターネットアクセス制御 開発者モード ドメイン名ホワイトリストとブラックリスト 認証設定の履歴の表示とエクスポート 適用
固定アカウント認証	キャプティブバイパス 固定アカウントの一括管理 セルフサービスパスワードの変更 LDAPサーバーとの連携 ログインページの視覚効果の変更 インターネットアクセス設定 認証が不要 サイト間およびSS ID間の再認証 インターネットアクセス制御 開発者モード ドメイン名ホワイトリストとブラックリスト 認証設定の履歴の表示とエクスポート 適用
WeChat公式アカウント認証	キャプティブバイパス ログインページの視覚効果設定の変更 インターネットアクセス設定 認証が不要 サイト間およびSS ID間の再認証 インターネットアクセス制御 開発者モード ドメイン名ホワイトリストとブラックリスト 認証設定の履歴の表示とエクスポート 適用
ゲスト認証	キャプティブバイパス インターネットアクセス設定 認証が不要 サイト間およびSS ID間の再認証 インターネットアクセス制御 開発者モード ドメイン名ホワイトリストとブラックリスト 認証設定の履歴の表示とエクスポート 適用
ダム端末認証	キャプティブバイパス ダム端末アカウントグループの管理 インターネットアクセス制御 開発者モード ドメイン名ホワイトリストとブラックリスト 認証設定の履歴の表示とエクスポート 適用

キャプティブバイパス機能をイネーブルにする

通常、クライアントがポータル認証ネットワークにアクセスしようとすると、デバイスは自動的に認証ページをクライアントにプッシュします。キャプティブバイパス機能を使用すると、ユーザーがブラウザを起動したときにだけ、デバイスがポータル認証ページをクライアントにプッシュできます。
キャプティブバイパス機能をイネーブルにするには、デバイスで次の手順を実行する必要があります。

1. **System view**を入力します。

```
system-view
```

2. Webサーバー名がCloudのポータルWebサーバービューを入力します。

```
portal web-server cloud
```

3. キャプティブパス機能をイネーブルにします。

```
captive-bypass enable
```

ワンキー認証ボタンを非表示またはカスタマイズ

ワンキー認証ボタンを非表示にするか、ボタンスタイルを変更するには、次の作業を実行します。ボタンが非表示の場合、ユーザーはログインページのカウントダウンタイマーが期限切れになると、自動的に認証を受けます。

制限事項およびガイドライン

ボタンスタイルを変更できるのは、ボタンが非表示になっていない場合だけです。

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Routers** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. **Wireless Authentication Templates**タブをクリックします。
5. 対象の認証テンプレートの**Draw**アイコン をクリックします。
6. **Auth Configuration**領域の**One-Key**タイルをクリックし、必要に応じてボタンを非表示にするかカスタマイズします。

固定アカウントの管理

固定アカウントを一括して削除、インポートまたはエクスポートするには、次のタスクを実行します。
固定アカウントを管理する手順は、次のとおりです。

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Routers** > **Users**選択します。
3. **Fixed Accounts**タブをクリックします。
4. **Fixed Accounts**を削除するには、ターゲット**Fixed Accounts**を選択して**Delete**をクリックします。
5. **Fixed Accounts**をインポートするには、**Import**をクリックし、テンプレートファイルをダウンロードして必要に応じてファイルに入力し、テンプレートファイルをアップロードします。
6. **Fixed Accounts**をエクスポートするには、**Export**をクリックします。

セルフサービスパスワード変更を有効にする

この機能により、ユーザーはログイン時にパスワードを変更できます。この機能を無効にすると、管理者だけが固定アカウントのパスワードを変更できます。

セルフサービスパスワード変更を有効にする手順は、次のとおりです。

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Routers** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. **Wireless Authentication Templates**タブをクリックします。
5. 対象の認証テンプレートの**Draw**アイコン をクリックします。
6. **Auth Configuration**領域の**Account**タイルをクリックします。
7. **Change Password**を有効にします。

固定アカウント検証のためのLDAPサーバーとの連携を有効にする

ユーザーが固定アカウントを使用してWLANにアクセスしようとしたときに検証するために、Cloudnetがユーザー名とパスワードをLDAPサーバーに報告できるようにするには、次の作業を実行します。これにより、ネットワーク管理者はLDAPサーバーからCloudnetにアカウント情報をインポートする必要がなくなります。

制限事項およびガイドライン

この機能を使用するには、LDAPサーバーが設定されていることを確認します。

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Routers** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. **Wireless Authentication Templates**タブをクリックします。
5. 対象の認証テンプレートの**Draw**アイコン をクリックします。
6. **Auth Configuration**領域の**Account**タイルをクリックします。
7. LDAPを有効にし、必要に応じてLDAP設定を設定します。
8. **LDAP Config Verification**をクリックして、LDAP設定を確認します。

ログインページの視覚効果の設定を変更

ログインページの背景色、背景の不透明度、およびテキストの色をカスタマイズするには、次の作業を実行します。

制限事項およびガイドライン

注意:
既定の設定を復元すると、ユーザー定義の視覚効果の設定がすべて削除され、復元操作は元に戻せなくなります。この機能は注意して使用してください。

認証方式の視覚効果設定は、複数の認証方式が有効になっている場合にのみ有効になります。

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Routers** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. **Wireless Authentication Templates**タブをクリックします。
5. 対象の認証テンプレートの**Draw**アイコン をクリックします。
6. **Auth Configuration**領域の**Login Style**メニューをクリックして適用します。
7. 必要に応じて、背景色、背景の不透明度、テキストの色を設定します。

調整はリアルタイムでプレビュー領域に表示されます。既定の視覚効果設定に戻すには、**Restore Default**をクリックします。

インターネットアクセス設定の設定

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Routers** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. **Wireless Authentication Templates**タブをクリックします。
5. 対象の認証テンプレートの**Draw**アイコン をクリックします。
6. **Auth Configuration**領域の**Advanced Settings**メニューをクリックして適用します。
7. 必要に応じてインターネットアクセス設定を設定します。

パラメータ

- **Session Timeout**:1回の認証でのクライアントの最大連続オンライン時間。クライアントは、継続的なオンライン時間がタイムアウトを超えるとログオフされます。セッションタイムアウトは、毎日のオンライン時間より長くすることはできません。
- **Daily Online Duration**:クライアントの1日の最大オンライン時間。クライアントは、1日のオンライン時間が制限を超えるとログオフされます。毎日のオンライン時間をセッションタイムアウトより短くすることはできません。
- **Minimum Traffic and Idle Timer**:アイドルタイマー内のトラフィックが最小トラフィックしきい値に到達できない場合に、クライアントからログオフします。アイドルタイマーを0に設定すると、アイドルタイマー機能がディセーブルになります。

注意:
ベストプラクティスとして、アイドルタイマーをクライアントのIPアドレスリースの半分以下の値に設定し、オフラインクライアントのエントリを時間内に削除できるようにします。

- **Client Rate Limit**:アップリンクおよびダウンリンククライアントトラフィックの制限レート。この機能は、5417P01以降のバージョンでサポートされています。
- **HTTPS for Landing and Login**:Landing and LoginページにHTTPSセッションを使用します。
- **Permit PC**:PCがWLANにアクセスできるようにします。Facebook認証はこの機能をサポートしていません。

ダム端末アカウントグループの管理

ダム端末アカウントグループを作成、削除、または編集し、ダム端末アカウントをインポートまたはエクスポートするには、次の作業を実行します。

ダム端末認証をイネーブルにしてアカウントグループを指定すると、グループ内のダム端末だけがWLANにアクセスできます。
ダム端末アカウントグループを管理するには:

1. トップナビゲーションバーの**Service**をクリックします。
2. ナビゲーション枠で**Authentication**を選択します。
3. Accountsタブをクリックします。
4. **Dumb Terminal Accounts**タブでダムターミナルアカウントグループを設定します。

ポータル自動認証の設定

この機能を使用すると、認証済みのユーザーは、無認証期間内に再認証を行わずにネットワークにアクセスできます。次のモードを使用できます。

- **Portal redirection -** このモードでは、ユーザーはブラウザを実行して自動ポータル認証をトリガーする必要があります。このモードでは、クライアントに広告をプッシュすることができます。
- **MAC-trigger -** このモードでは、ユーザーはブラウザを実行せずにWLANにアクセスできます。このモードでは、クライアントに広告をプッシュすることはできません。

ポータルリダイレクト認証の設定

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Routers** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. **Wireless Authentication Templates**タブをクリックします。
5. 対象の認証テンプレートの**Draw**アイコン をクリックします。
6. **Auth Configuration**領域の**Advanced Settings**メニューをクリックして適用します。
7. **Auth-Free**タブをクリックし、**Free Auth**機能を設定します。

MACトリガー認証の設定

1. ポータルリダイレクション認証を設定します。詳細については、”ポータルリダイレクト認証を設定する”を参照してください。
2. MACバインディングサーバークラウドをサービステンプレートクラウドに適用する。

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

サイト間およびSSID間の再認証の設定

この機能を使用すると、認証されたクライアントは、再認証を行わずに、異なるサイトに関連付けられたワイヤレスサービス間、または同じサイト異なるSSID間でローミングできます。これらのワイヤレスサービスでは、同じ認証テンプレートを使用するか、同じSSIDを使用する必要があります。

制限事項およびガイドライン

この機能は、App Centerで設定された認証テンプレートでのみ使用できます。

手順

1. トップナビゲーションバーの**Service**をクリックします。
2. ナビゲーション枠で**Authentication**を選択します。
3. 対象の認証テンプレートの**Draw**アイコン をクリックします。
4. **Auth Configuration**領域の**Advanced Settings**メニューをクリックして適用します。
5. **Auth-free**タブをクリックし、**Free Auth**を有効にします。

6. **サイト間およびSSID間の再認証を設定します。**

インターネットアクセス制御の設定

ユーザーがWLANにアクセスできる時間範囲を指定するには、次の作業を実行します。

制限事項およびガイドライン

インターネットアクセス制御は時間単位で行われます。1日に最大5つの時間範囲を指定できます。24時に終了する時間範囲を指定するには、終了時間を00に設定します。1日の時間範囲を00～00に設定すると、ユーザーはその日いつでもインターネットにアクセスできます。

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Routers** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. **Wireless Authentication Templates**タブをクリックします。
5. 対象の認証テンプレートの**Draw**アイコン をクリックします。
6. **Auth Configuration**領域の**Advanced Settings**メニューをクリックして適用します。
7. **Internet Access Control**タブをクリックし、時間範囲を指定します。

開発者モードの設定

注意:
既存の機能のコードを編集すると、Cloudnet認証が無効になる場合があります。この機能は注意して使用してください。

開発者モードでは、カスタマイズの目的で認証テンプレートのソースコードを変更できます。

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Routers** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. **Wireless Authentication Templates**タブをクリックします。
5. 対象の認証テンプレートの**Draw**アイコン をクリックします。
6. 右上隅にある**Developer Mode**をクリックします。

ドメイン名のホワイトリストとブラックリストの設定

制限事項およびガイドライン

この機能は、ワイヤレス認証が設定されている場合にだけ有効です。

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Routers** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. **Domain Name Whitelist**または**Domain Name Blacklist**タブをクリックして、ホワイトリストまたはブラックリストを設定します。

認証テンプレートデプロイメントの履歴の表示またはエクスポート

現在、過去7日間、または過去30日間におけるすべての認証テンプレートの適用または適用の履歴を表示するには、次の作業を実行します。
認証テンプレートデプロイメントの履歴を表示またはエクスポートする手順は、次のとおりです:

1. トップナビゲーションバーの**Service**をクリックします。
2. ナビゲーション枠で**Authentication**を選択します。
3. **Authentication Templates**タブで、対象の認証テンプレートの**Apply**アイコン をクリックします。
4. **ACs**タブをクリックして、ACの適用履歴を表示します。

Cloudnetユーザーの管理

クライアントブラックリストの設定

特定のクライアントのWLANへのアクセスを禁止するには、次の作業を実行します。

制限事項およびガイドライン

この機能は、オフラインクライアントでのみ有効です。ブラックリストにオンラインクライアントを追加すると、次回のアクセス試行時にクライアントが拒否されます。

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Device Category** > **Users**を選択します。
3. ブラックリストにユーザーを追加するには、次のいずれかのタスクを実行します。

- **Guest**タブで、ターゲットユーザーの**Add to Blacklist**アイコン  をクリックします。
- **Blacklist**タブで、**Add**をクリックします。

オンラインユーザーからログオフする

特定のオンラインユーザーまたはすべてのオンラインユーザーをログオフするには、次の作業を実行します。

制限事項およびガイドライン

この機能は、auth-freeユーザーには有効になりません。
この機能は、認証装置としてACまたは有線ルーターを使用するシナリオでだけ使用できます。

手順

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Network** > **Client** > **Guest Details**を選択します。
3. ページ上部からブランチとサイトを選択します。
4. **Online Clients**タブで、**Authenticated Clients**をクリックします。
5. 特定のクライアントをログオフするには、クライアントを選択し、**Log Off Selected Users**をクリックします。すべてのクライアントからログオフするには、**Log Off All Users**をクリックします。

ポータルのfail-permitの設定

この機能は、認証装置としてACまたはワイヤレスルーターを使用するシナリオでのみ使用できます。
ポータルのfail-permitを使用すると、アクセスデバイスがポータル認証サーバーまたはポータルWebサーバーが到達不能であることを検出したときに、ユーザーはポータル認証なしでネットワークアクセスできます。
ポータル認証が再開された後、認証されていないユーザーは、ネットワークにアクセスするためにポータル認証に合格する必要があります。fail-permitイベントの前にポータル認証に合格したユーザーは、引き続きネットワークにアクセスできます。

制限事項およびガイドライン

この機能を有効にするには、デバイスの基本設定が完了していることを確認してください。詳細については、”デバイスの設定を設定する”を参照してください。

手順

1. ポータルの**fail-Permit**を有効にします。

<Sysname> system-view
[Sysname] wlan service-template cloud
[Sysname-wlan-st-cloud] portal fail-permit web-server
[Sysname-wlan-st-cloud] quit

2. ポータルWebサーバーの検出を設定します。

注意:
ポータルサーバーのフラッピングを回避するには、所定の順序に従ってポータルWebサーバー検出を設定します。

#ポータルWebサーバー検出用のURLとタイプを指定します。
[Sysname] portal web-server cloud
[Sysname-portal-websvr-cloud] server-detect url http://oasisauth.h3c.com/portal/ping detect-type http
#サーバー検出の設定:

- 検出間隔を600秒に設定してください。
- 連続検出失敗の最大数を2に設定する。
- サーバーの到達可能性ステータスが変更された後に、ログメッセージとトラップメッセージを送信するようにデバイスを設定します。

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

APが公共ネットワーク経由でACに登録する

この機能は、認証装置としてACまたはワイヤレスルーターを使用するシナリオでのみ使用できます。
デフォルトでは、デバイスはクライアントが認証パケットを交換するためのHTTPポート80を提供します。ローカル転送がイネーブルの場合、公共ネットワークを介してACにAPが登録され、ポート80が使用できない場合は、次の作業を実行してCMCCを設定するか、クライアントがCloudnet認証を実行するためのHTTPサービスポートを変更します。

CMCCの設定

ACとCloudnetの両方でCMCCを設定する必要があります。
CMCCを設定するには、次の手順を実行します。

1. CMCCプロトコルの設定
   - Cloudnetの設定:
     - AC+fit APネットワークでCloudnetを設定します。
     - ワイヤレスネットワークでのCloudnetの設定
   - デバイスの設定
2. 2.(オプション)CMCCポータルリダイレクション認証の設定
   - Cloudnetの設定
   - デバイスの設定

制限事項およびガイドライン

CMCCが設定されている場合、セッションタイムアウト、毎日のオンライン時間、最小トラフィック、およびアイドルタイマーの設定が使用できなくなります。

CMCCプロトコルの設定

AC+fit APネットワークでCloudnetの設定

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠で**Settings** > **ACs** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。
4. 対象の認証テンプレートの**Draw**アイコン をクリックします。
5. **Auth Configuration**領域の**Advanced Settings**メニューをクリックして適用します。
6. **CMCC**タブをクリックします。
7. **CMCC**プロトコルを有効にし、必要に応じてプロトコルを選択します。

ルーターを認証装置として使用するワイヤレスネットワークのCloudnetの設定

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Routers** > **Authentication**を選択します。
3. ページ上部からブランチ、サイトおよびデバイスを選択します。

4. 対象の認証テンプレートの**Draw**アイコン をクリックします。
5. **Auth Configuration**領域の**Advanced Settings**メニューをクリックして適用します。
6. **CMCC**タブをクリックします。
7. **CMCC**プロトコルを有効にし、必要に応じてプロトコルを選択します。

デバイスの設定

#ポータル認証サーバークラウドを作成し、そのビューを表示します。
<Sysname> system-view
[Sysname] portal server cloud
#ポータル認証サーバーのIPv4アドレスとして139.217.11.74を指定します。
[Sysname-portal-server-cloud] ip 139.217.11.74
#ポータル認証サーバーのタイプをcmccとして指定します。
[Sysname-portal-server-cloud] server-type cmcc
#登録パケットを60秒間隔でポータル認証サーバーに送信するようにデバイスを設定します。
[Sysname-portal-server-cloud] server-register interval 60
[Sysname-portal-server-cloud] quit

CMCCポータルリダイレクション認証の設定

Cloudnetの設定

ポータルリダイレクト認証を有効にします。詳細については、AC+fit APネットワークの場合は”ポータルリダイレクト認証を設定する”を、ワイヤレスルーターを認証装置として使用するワイヤレスネットワークの場合は”ポータルリダイレクト認証を設定する”を参照してください。

デバイスの設定

デバイスの基本設定が完了していることを確認します。詳細については、”デバイスの設定を設定する”を参照してください。

デバイスを設定するには、次の手順を実行します

1. MACバインディングサーバーを設定します。

注意:
無線サービスへの影響を回避するには、MACバインディングサーバーが作成されている場合でも、CMCC専用のMACバインディングサーバーを指定する必要があります。

#MACバインディングサーバーmtsを作成し、そのビューを表示します。
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
#MACバインディングサーバーのIPアドレスを139.217.11.74に指定します。
[Sysname-portal-mac-trigger-server-mts] ip 139.217.11.74
#MACバインディングサーバーのタイプをcmccとして指定します。
[Sysname-portal-mac-trigger-server-mts] server-type cmcc
#(オプション)ポータルユーザーの空きトラフィックしきい値をバイト単位で設定します。
[Sysname-portal-mac-trigger-server-mts] free-traffic threshold 1
[Sysname-portal-mac-trigger-server-mts] quit
#MACバインディングサーバーmtsをサービステンプレートクラウドにバインドします。
[Sysname] wlan service-template cloud
[Sysname-wlan-st-cloud] portal apply mac-trigger-server mts

2. ISPドメイン内のユーザーの認証属性を設定します。
#ISPドメインクラウドを作成します。

[Sysname] domain cloud
#アイドルタイマーを分単位で設定します。
[Sysname-isp-cloud] authorization-attribute idle-cut 30
#セッションタイムアウトを分単位で設定します。
[Sysname-isp-cloud] authorization-attribute session-timeout 360
[Sysname-isp-cloud] quit

HTTPサービスポートの変更

この作業を実行する前に、デバイスの基本設定が完了していることを確認してください。詳細については、”デバイスの設定を設定する”を参照してください。

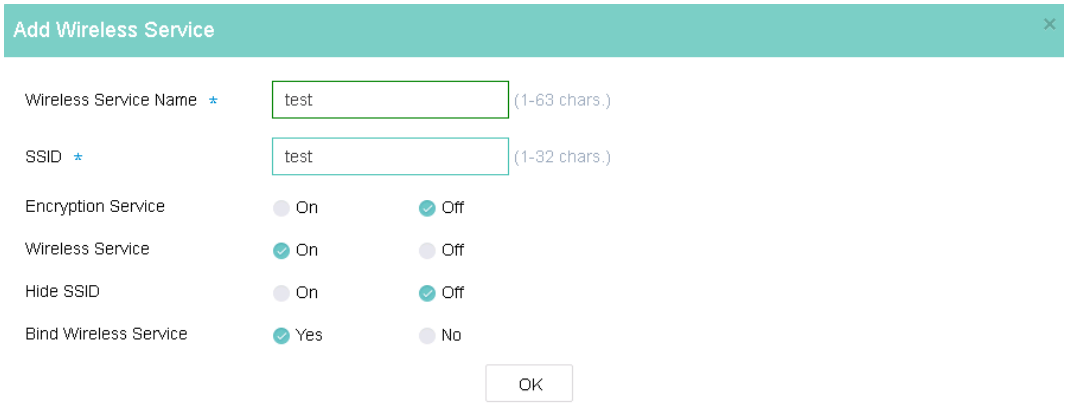
HTTPサービスポートを変更するには、次の手順に従います。

1. HTTPサービスポート番号を設定します。この例では、ポート番号は8088です。
<Sysname> system-view
[Sysname] ip http port 8088
2. HTTPベースのローカルポータルWebサービスを作成し、リスニンポート番号を8088に設定します。
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] tcp-port 8088
[Sysname-portal-local-websvr-http] quit
3. ポータルサーバーを設定します。
#ポータルWebサーバーのURLを設定します。x.x.x.xは、ACが存在するネットワークの出力IPを表します。
[Sysname] portal web-server cloud
[Sysname-portal-websvr-cloud] url
http://oasisauth.h3c.com/portal/protocol?redirect_uri=http://x.x.x.x:8088/portal/cloudlogin.html
#ユーザーをx.x.x.x:8088にリダイレクトするようにCloudnetサーバーを設定します。
[Sysname-portal-websvr-cloud] if-match original-url http://captive.apple.com
user-agent Mozilla temp-pass redirect-url
http://oasisauth.h3c.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.h3c.com/portal/protocol?redirect_uri=http://x.x.x.x:8088/portal/cloudlogin.html
[Sysname-portal-websvr-cloud] quit

ワイヤレスサービスの設定

1. 上部のナビゲーションバーで、**Network**をクリックします。
2. ナビゲーション枠から**Settings** > **Device Category** > **Wireless Services**を選択します。
3. **Wireless Services**タブで、**Add**をクリックします。
4. 暗号化サービスを設定するには、必要に応じて**Encryption Service**フィールドで**On**または**Off**を選択します。

図 46 暗号化サービスの設定



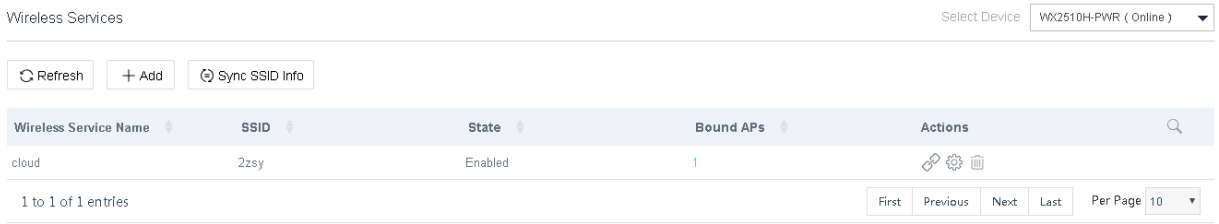
5. SSID情報を同期するには、**Sync SSID Info**をクリックします。

ワイヤレスサービスが作成され、デバイスにSSID情報が設定されていることを確認します。

注意:

この機能は、5418より前のバージョンのACおよび0809より前のバージョンのルーターだけで使用できます。

図47 SSID情報の同期



6. デバイスのワイヤレスサービス設定をCloudnetに同期させるには、**Sync to Cloud**をクリックします。この操作により、ワイヤレスサービス名、SSID、保証帯域幅比などの設定がCloudnetと同期されます。

注意:

この機能は、バージョン5418以降のACおよびバージョン0809以降のルーターでだけ使用できます。

よくある質問

認証テンプレート設定の変更と適用に成功しました。適用後にオンラインになるクライアントに対して、以前の設定が有効になるのはなぜですか。

設定が変更され、正常に適用されていることを確認します。問題が解決しない場合は、クライアント上のブラウザアクセスレコードとキャッシュをクリアします。

App CenterのAuthentication Templatesページには、テンプレートできるデバイスは表示されません。どうすればいいですか?

デバイスのバージョンが要求どおりであることを確認します。そうでない場合は、デバイスを最新バージョンにアップグレードします。

ワイヤレスサービスのSSIDを変更するにはどうしたらいいですか?

1. Wi-Fi名をCloudnetから変更します。AC+fit APネットワークの場合は、ACのWi-Fi名を変更することもできます。
2. WeChat公式アカウントプラットフォームからSSIDを変更します。https://mp.weixin.qq.com/でプラットフォームにアクセスします。ナビゲーション枠でFunction > Wi-Fiを選択し、Device Manageタブをクリックして、SSIDを変更します。
3. 認証サービスからサービステンプレートをアンバインドし、再バインドします。

新しく公開された機能を使用するためにCloudnetを更新する方法

Cloudnetのフィーチャーは自動的に更新され、手動操作は必要ありません。新しい認証テンプレート機能を有効にするには、テンプレートを再設定してから公開する必要があります。

authentication freeが設定されていない場合でも、クライアントがオフラインになり、認証されずにオンラインになるのはなぜですか。

クライアントのアソシエーション解除イベントが発生しても、、認証済みクライアントリストからクライアントエントリが削除されることはありません。アイドルタイマーが期限切れになるか、管理者がクライアントをログオフするまで、エントリは削除されません。オフラインクライアントは、そのエントリがまだ存在する場合、認証されずにオンラインになることができます。
Cloudnetから、またはdisplay portal user allコマンドを実行して、クライアントエントリを表示できます。

認証済みクライアントの数がオンラインクライアントの合計数を超えるのはなぜですか。

この症状は、クライアントがオフラインになった直後に発生します。クライアントのアソシエーション解除イベントが発生しても、、認証済みクライアントリストからクライアントエントリが削除されることはありません。アイドルタイマーが期限切れになるか、管理者がクライアントを手動でログオフするまで、エントリは削除されません。

必要に応じて、デバイスとCloudnetの認証設定を行いました。クライアントアクセス試行はポータル認証をトリガーできますが、リダイレクションページを開くことはできません。どうすればいいですか?

この問題は、クライアントのIPアドレスのネットワークセグメントがアップリンクデバイスに認識されず、パケットを返送できない場合に発生する可能性があります。この問題を解決するには、デバイスを外部ネットワークに接続するデバイスのインターフェィス上でnat outboundコマンドを設定するか、IGPを使用してネットワーク内のネットワークセグメントをアドバタイズします。

最適化されたキャプティブバイパスがイネーブルになっている場合でも、iOSクライアントは認証をトリガーできません。どうすればいいですか?

ポータルのcaptive-bypassoptimize delay secondsコマンドを実行して、captive-bypass検出タイムアウトを設定します。値の範囲は6～60秒で、デフォルト値は6秒です。
デバイスのパフォーマンスに影響を与えないようにするには、タイムアウトを大きな値に設定しないでください。

付録A デバイスの認証コマンド

このセクションでは、ワンキー、固定アカウント、WeChat公式アカウント、Facebook、ダム端末、ゲスト認証のデバイス上で実行する必要があるコマンドについて説明します。

アプリケーション認証およびFacebook認証の場合は、このセクションの設定を完了した後、”アプリケーション認証の設定”および”Facebook認証の設定”でそれぞれ設定を設定する必要があります。
デバイス上でこれらのコマンドをすばやく実行するには、必要に応じてグレー表示されているセクションを編集し、デバイスのユーザービューにすべてのコマンドを貼り付けます。

注意:

- これらのコマンドは、5405より前のバージョンでのみ実行してください。バージョン5405以降では、デバイスへの自動認証設定適用がサポートされているため、これらのコマンドを手動で設定する必要はありません。
- コマンドがデバイスに存在する設定と競合しないことを確認します。
- 設定前提条件のタスクが完了していることを確認します。詳細は”前提条件”を参照してください。

```
system-view
domain cloud
authentication portal none
authorization portal none
accounting portal none
quit
portal web-server cloud
url http://oasisauth.h3c.com/portal/protocol
server-type oauth
if-match user-agent CaptiveNetworkSupport redirect-url
http://oasisauth.h3c.com/generate_404
if-match user-agent Dalvik/2.1.0(Linux;U;Android7.0;HUAWEI redirect-url
http://oasisauth.h3c.com/generate_404
if-match original-url http://captive.apple.com user-agent Mozilla temp-pass redirect-url
http://oasisauth.h3c.com/portal/protocol
if-match original-url http://www.apple.com user-agent Mozilla temp-pass redirect-url
http://oasisauth.h3c.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.h3c.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 WeChat
portal safe-redirect user-agent iPhone
portal safe-redirect user-agent micromessenger
```