

H3C Cloud管理AP設定ガイド

Copyright © 2020, New H3C Technologies Co., Ltd. 及びその著作権所有者

全著作権所有

本書のいかなる部分も、New H3C Technologies Co., Ltd.の書面による事前の同意なしに、いかなる形式または手段によっても複製または更新することはできません。

商標

New H3C Technologies Co., Ltd.の商標を除き、本書に記載されているすべての商標は、それぞれの所有者の商標または登録商標です。

注意

本書に記載されている情報は、予告なしに変更されることがあります。このドキュメントに記載されているすべての内容(記述、情報、推奨事項を含む)は、正確であると考えられますが、明示的であるか黙示的であるかを問わず、いかなる種類の保証もなく提供されています。H3Cは、本書に含まれている技術的または編集上の誤りまたは脱落に対して責任を負わないものとします。

はじめに

このユーザーガイドでは、Cloudnetプラットフォームからクラウド管理APを設定する手順について説明します。

ここでは、マニュアルに関する次のトピックについて説明します。

- 対象者
- 表記規則
- ドキュメントに関するフィードバック

対象者

このマニュアルの対象読者:

- ネットワークプランナー
- 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
- H3Cアクセスコントローラを操作するネットワーク管理者

表記規則

ここでは、マニュアルで使用されている表記規則について説明します。

コマンドの規則





表記規則	説明
太字	太字のテキストは、表示されているとおりに入力したコマンドとキーワードを表します。
<i>Italic</i>	斜体テキストは、実際の値に置き換える引数を表します。
[]	角カッコは、オプションの構文選択(キーワードまたは引数)を囲みます。
{ x y ... }	中カッコは、必要な構文のセットを縦棒で区切って囲み、その中から1つを選択します。
[x y ...]	角かっこは、オプションの構文オプションのセットを縦棒で区切って囲み、その中から1つまたは何も選択しないようにします。
{ x y ... } *	アスタリスクでマークされた中カッコは、必要な構文の選択肢を縦棒で区切ったもので、その中から1つ以上を選択します。
[x y ...] *	アスタリスクの付いた角カッコは、オプションの構文の選択肢を縦棒で区切って囲みます。縦棒では、1つの選択肢、複数の選択肢、またはなしを選択できます。
&<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。
#	#記号で始まる行がコメントです。

GUIの規則













表記規則	説明
太字	ウィンドウ名、ボタン名、フィールド名およびメニューアイテムは太字で表示されます。たとえば、 新規ユーザー ウィンドウが開き、 OK をクリックします。

表記規則	説明
>	マルチレベルメニューは山括弧で区切られます。たとえば、File > Create > Folder

記号

表記規則	説明
	重要な情報への注意を喚起するアラートで、理解またはフォローしないと人身事故につながる可能性があります。
	重要な情報への注意を喚起するアラート。理解またはフォローしていないと、データの消失、データの破損、ハードウェアまたはソフトウェアの損傷につながる可能性があります。
	重要な情報への注意を促すアラート。
注:	追加情報または補足情報を含むアラート。
	有用な情報を提供するアラート。

ネットワークポロジアイコン

表記規則	説明
	ルーター、スイッチ、ファイアウォールなどの汎用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スイッチなどの一般的なスイッチ、またはレイヤー2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。
	全方向信号を表します。
	方向信号を表します。
	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、ロードバランシング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、ロードバランシング、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。

本書に記載されている例

このドキュメントの例では、使用しているデバイスと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異なるデバイスを使用している場合があります。通常、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、使用しているデバイスとは異なります。

ドキュメントに関するフィードバック

製品ドキュメントに関するご意見は、info@h3c.comまで電子メールでお寄せください。ご意見をいただければ幸いです。

目次

Cloudnetプラットフォームとクラウド管理APについて.....	1
第一部 ネットワーク.....	1
Cloudnetプラットフォームの構成.....	1
Cloudnetプラットフォームへ新規アカウントを作成.....	1
アカウントの削除.....	2
Cloudnetプラットフォームへサブアカウントを作成.....	4
サブアカウントを追加する.....	4
サブアカウントとは.....	6
サブアカウント例.....	6
サブアカウントの操作(表示、設定など)対象のブランチを設定する.....	6
Cloudnetプラットフォームへのアクセス.....	8
ブランチの設定.....	8
ブランチを追加する.....	8
ブランチの名前を変更する.....	8
ブランチを削除する.....	8
ブランチ作成のヒント.....	9
サイトを追加する.....	11
サイトにCloudAPを登録する.....	14
エリアを追加する.....	15
デバイスを追加する.....	17
デバイスをまとめて追加する.....	20
クラウドAPテンプレートを利用した設定.....	21
クラウド管理APの設定.....	26
エリアコードを指定する.....	26
Wi-Fi設定の構成.....	26
ワイヤレスサービスの設定.....	26
ドメイン名のホワイトリストまたはブラックリストの設定.....	39
無線帯域設定.....	39
ネットワーク最適化.....	43
SSIDに関連付けされたVLANの作成.....	46
クラウド管理されたコンフィグのローカルAPとの同期.....	47
ワイヤレス認証の設定.....	48
基本認証設定の構成.....	48
高度な認証設定の構成.....	51
再アソシエーションのための認証なしの設定.....	52
インターネットアクセスコントロールの設定.....	53
クラウド管理されたAPのモニタリング.....	54
クラウド管理APの統計情報サマリーの表示.....	54
クラウド管理APリストの表示.....	54
詳細なクライアント情報の表示(ネットワーク).....	57
第二部 スマートO&M.....	59
ダッシュボード.....	59
問題>問題分析.....	60
問題>アラーム.....	61
クライアント>無線端末.....	65
ネットワーク>AP.....	68
応用(アプリケーション)>応用統計.....	70
セキュリティ>攻撃検知.....	72
第三部 サービス.....	73
サービス>レポート管理.....	73
サービス>カスタム大画面.....	76

サービス>資産管理.....	79
第四部 デバイスの保守.....	84
ファームウェアのアップグレード.....	84
特定のデバイスのアップグレード.....	84
特定モデルのデバイスのアップグレード.....	85
アップグレードの詳細の表示.....	86
プライベートバージョンのアップロード.....	86
Cloudnet上にアップされたファームウェアが古い場合.....	87
装置への操作.....	91
システム.....	92
デバイスのバインド解除.....	92
付録1 Cloudnetサポートマトリックス.....	96
付録2 APのモード変更.....	101
APのモード.....	101
CLIからAPモードを変更する.....	101
BootWareメニューからAPモードを変更する.....	102
CloudnetからAPモードを変更する.....	104
付録3 SNMP及びsyslog設定.....	106
Syslogサーバーへのlog送信設定.....	106
SNMPでの管理設定.....	108
付録4 スマフォのCloudnetアプリ.....	109
付録5 トラブルシューティング.....	112
付録6 GUIへのアクセス方法.....	117
ローカルでの場合.....	117
管理用SSIDのセキュリティ強化.....	120
CloudnetからローカルのGUIへアクセスの場合.....	121
付録7 PoEとの接続.....	122

Cloudnetプラットフォームとクラウド管理APについて

H3C Cloudnetプラットフォームは、中小規模企業向けに設計された軽量マルチサービスプラットフォームであり、中小規模のオフィスネットワークや商用ネットワーク、本社+支社のシナリオに適用可能であり、デプロイメント、デバイスモニタリング、アシュアランスなどの機能を組み込んだシナリオベースのソリューションを提供します。

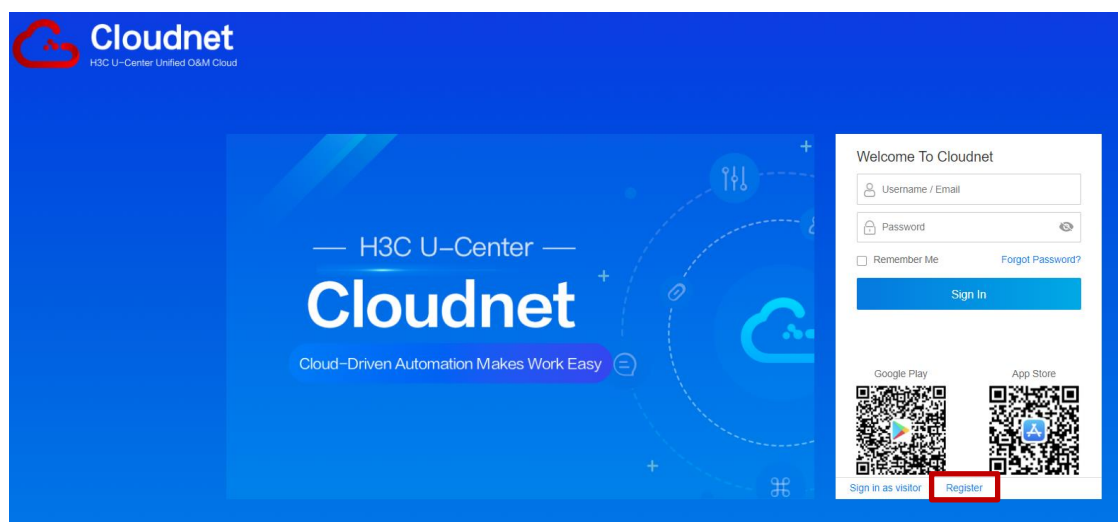
H3CクラウドマネージドAPは、Cloudnetプラットフォームをベースに開発されたもので、ネットワーク管理者がクラウドマネージドAPの状態をリアルタイムで確認して設定を展開するなど、クラウドマネージドAPを直接管理することで、ネットワーク効率を大幅に向上させ、セキュリティや安定性を向上させることができます。

第一部 ネットワーク

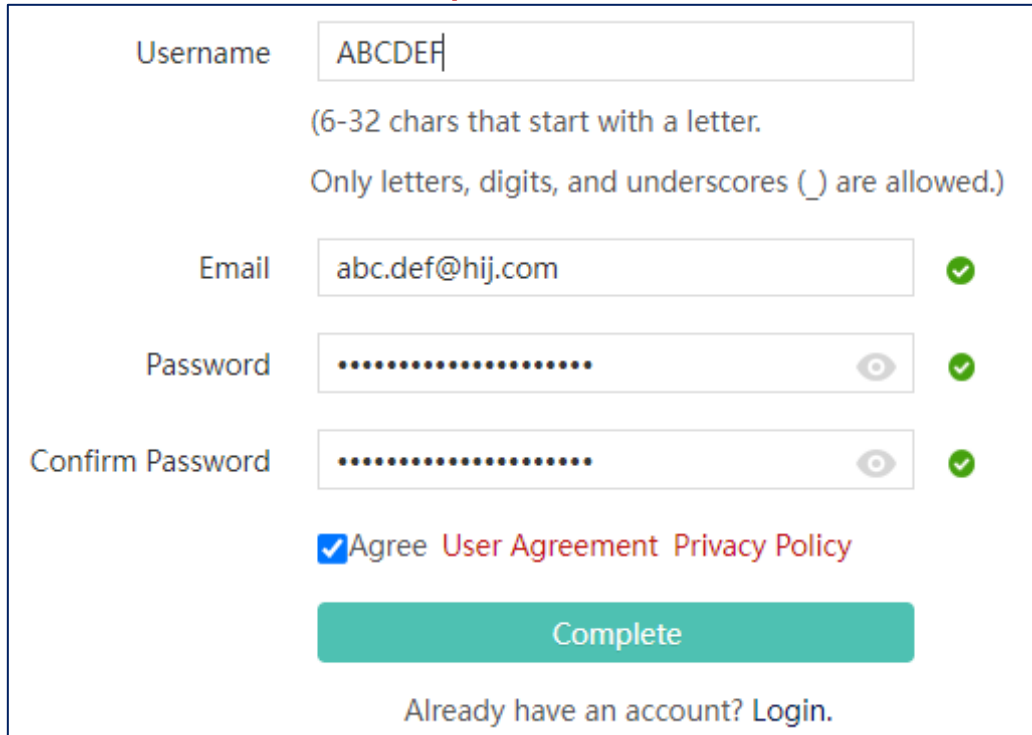
Cloudnetプラットフォームの構成

Cloudnetプラットフォームへ新規アカウントを作成

Cloudnetのサイトは**マルチテナント**方式を採用しており、独自のアカウントを作成し、**他のテナント**と隔離して管理することができます。新規アカウントを作成するには、パソコンをインターネットに接続し、ブラウザを開き、アドレスバーに<https://cloudnet.h3c.com>と入力します。表示されたログインページの右下の**register**をクリックします。



以下のように必要な項目を入力し**Complete**をクリックします。



The image shows a registration form with the following fields and elements:

- Username:** Input field containing "ABCDEF". Below it, text reads "(6-32 chars that start with a letter. Only letters, digits, and underscores (_) are allowed.)".
- Email:** Input field containing "abc.def@hij.com". A green checkmark is visible to the right.
- Password:** Input field with masked characters (dots). A green checkmark is visible to the right.
- Confirm Password:** Input field with masked characters (dots). A green checkmark is visible to the right.
- Agree:** A checked checkbox followed by the text "Agree User Agreement Privacy Policy".
- Complete:** A large green button.
- Footer:** Text that says "Already have an account? Login."

入力したEmailアドレスに確認のメールが届きますので、リンクをクリックすると上記アカウントが有効になります。

メールは以下のような形式で送信されます:

差出人: cloudnet@oasisinfo.h3c.com
日時: 2022年7月19日 10:31:09 JST
宛先: abc.def@hij.com
件名: New H3C Cloudnet Platform Email Binding

[Click here to activate account](#)

Effective within 24 hours, Please activate as soon as possible!

アカウントの削除

アカウントが不要になった場合、削除することができます。

削除はネットワーク > システム > アカウントで以下の画面を表示して、



The image shows the "Account Information" (基本情報) page with the following details:

- 顔写真 (Profile Picture):** A circular image of a sunset over water. Below it is a button labeled "アバターを変更する" (Change Avatar).
- アカウント名 (Account Name):** Input field containing "H3CTRAN". To its right is a link "パスワードを変更する" (Change Password) and a link "アカウントをキャンセルする" (Cancel Account), which is highlighted with a red box.
- メールボックス (Email Box):** Input field containing "training@h3c.com". To its right is a link "変更" (Change).

“アカウントをキャンセルする”をクリックすると、次の画面に推移します。

この画面でメール確認コードの**取得**ボタンをクリックすると、アカウントに登録されたメールアドレスにメール確認コードが送られてきますので、それをメール確認コード欄に入力して、**確定**をクリックし、アカウントを閉じるポップアップ画面が表示されますので、最終確認として**確定**をクリックするとアカウントは完全に削除されます。

ちなみに送られてくるメールは以下のような形式で送信されます。

差出人: cloudnet@oasisinfo.h3c.com

日時: 2022年11月21日 10:31:09 JST

宛先: abc.def@hij.com

件名: **New H3C Cloudnet Platform Email Binding**

The verification code for the account closing operation is123456. The code is valid in 5 minutes. If the message sending is not triggered by you, please ignore the message.

アカウント

アカウントを閉じる

アカウントの開鎖後は、そのアカウントを使用して、Cloudnet アプリを含む Cloudnet にログインし

アカウント: メール

* キャプチャ:

* メール認証コード:

アカウントを閉じる

アカウントの開鎖後、システムはアカウントの全てのデータを消去し、データを復元する事は出来ません。注意して操作してください。

Cloudnetプラットフォームへサブアカウントを作成

Cloudnetのアカウントは管理する役割によりサブアカウントを作成することができます。メインのアカウントは全ての管理権限を持ちますが、参照のみのアカウントを作成することができます。サブアカウントは最大500、アカウントの階層は5レベルまで作成することができます。

サブアカウントを追加する

1. トップナビゲーションバーで、**ネットワーク**をクリックします。
2. 左側のナビゲーションペインで、**システム > サブアカウント**を選択します。
3. 開いたページで、**ルートユーザー**を選択し、**追加**をクリックします。

ユーザ名	電話	メールボックス	アカウントタイプ	Branch Authorizator	Site Authorization	追加	修正	削除
H3CTRaining2	-	abc.def@ghi.com	Tenant	-	-	<input style="border: 2px solid red;" type="button" value="+"/>	-	-

4. 必須項目を入力して、**確定**をクリックします。

* サブアカウント名:	<input type="text" value="H3CTRaining3"/>
* パスワード:	<input type="password" value="....."/>
* パスワードを確認してください:	<input type="password" value="....."/>
* 役割:	<div style="border: 2px solid red; padding: 5px;"><input type="text" value="役割を選択してください"/> ^ Discretionary Account Watcher Account Maintenance Account Demo Account Operation Account Config Account</div>
Registration Method:	
* メールボックス:	
連絡先:	
	<input style="border: 2px solid red;" type="button" value="確定"/> <input type="button" value="キャンセル"/>

役割による権限は以下の通りです:

- Discretionary Account (フルオーソリティアカウント): テナントと同じ管理者権限を持ち、引き続きサブアカウントを作成できます。
- **Watcher Account** (監視アカウント): 主にネットワーク監視用で、構成管理権限がないのと、サブアカウントの作成ができません。
- **Maintenance Account** (運用および保守アカウント): ネットワーク構成および保守権限があり、サブアカウントを作成できます。
- Demo Account (デモアカウント): すべてのデバイスの読み取り専用機能があり、サブアカウントは作成できません。
- Operation Account (操作アカウント): 主にトラフィックフロー分析などを行い、サブアカウントを作成できます。
- **Config Account** (構成アカウント): ネットワーク構成権限があり、サブアカウントを作成できます。

Registration Methodはメールアドレスの登録か携帯番号の登録かを選択して設定します。
メールアドレス、携帯番号はCloudnet内で他のアカウントとの重複は許されません。
メインのアカウントの場合は、メールアドレスが正しいかの確認メールが届きましたが、サブアカウントの場合は確認メール、確認SMSなしで利用する事ができます。
補足: 携帯番号は中国国内の携帯電話番号のみで13、15、18、から始まる11桁。
アラームはメールアドレスを登録すれば、メールで、携帯番号を登録するとSMSで送信されます。

* サブアカウント名:	<input type="text" value="h3ctest123"/>
* パスワード:	<input type="password" value="....."/>
* パスワードを確認してください:	<input type="text" value="パスワードを確認してください"/>
* 役割:	<input type="text" value="役割を選択してください"/> ▼
Registration Method:	<input checked="" type="radio"/> メールボックス <input type="radio"/> 携帯番号
* メールボックス:	<input type="text" value="メールボックスを入力してくださいか"/>
連絡先:	<input type="text" value="長さは50文字を超えてはいけません"/>
<input type="button" value="確定"/> <input type="button" value="キャンセル"/>	

* サブアカウント名:	<input type="text" value="h3ctest123"/>
* パスワード:	<input type="password" value="....."/>
* パスワードを確認してください:	<input type="text" value="パスワードを確認してください"/>
* 役割:	<input type="text" value="役割を選択してください"/> ▼
Registration Method:	<input type="radio"/> メールボックス <input checked="" type="radio"/> 携帯番号
* 携帯番号:	<input type="text" value="携帯番号を入力してください"/>
連絡先:	<input type="text" value="長さは50文字を超えてはいけません"/>
<input type="button" value="確定"/> <input type="button" value="キャンセル"/>	

サブアカウントとは

サブアカウントとは、例えばあるネットワーク管理会社が複数の会社のネットワーク機器を監視、管理しているような場合に有益です。

管理している会社ごとにブランチを作成し、それぞれのブランチにその会社のネットワーク機器を登録します。

ネットワーク管理会社はすべてのブランチ、つまり管理している会社のネットワーク機器の状態を見ることができますし、コンフィグを変更することもできます。

管理されている会社にサブアカウントを与える(つまり、Cloudnetにアクセスする独自のアカウント(ユーザー名、パスワード)でログインできます)。このサブアカウントがアクセスできるのは許可されたブランチに作成されたサイトとルートのサイトとなります。

注意！！サブアカウントはルートに作成されたサイトにもアクセスできるため、ルートにはサイトは作成しないでください。ルートには必ずブランチを作成して、アクセスできる人を管理するようにしてください。

サブアカウント例

ユーザ名	電話	メールボックス	アカウントタイプ
▼ H3CTRaining3	-	test1@gmail.com	Tenant
TRAININGUSER01	-	test2@gmail.com	Demo Account
TRAININGUSER02	13090555566		Watcher Account

サブアカウントの操作(表示、設定など)対象のブランチを設定する

Site Authorizationは、サブアカウントが指定されたサイトのみを管理することを承認します。サブアカウントは、ここで指定したブランチ以外のブランチに対するアクセス特権がありません。

The screenshot shows a 'Site Authorization' dialog box. On the left, there is a list of users under 'H3CTRaining3': TRAININGUSER01 and TRAININGUSER02. The dialog box has a 'Search Branch' dropdown and an input field 'Enter a branch...'. Below this, a list of branches is shown: H3CLAB (checked), osaka (checked), STOCK (unchecked), and Tokyo (checked). At the bottom of the dialog are '確定' (Confirm) and 'キャンセル' (Cancel) buttons. In the background, a table shows account types: Tenant, Demo Account, and Watcher Account. The 'Demo Account' row has a red box around the 'Site Authorization' column icon.

Site Authorization ✕

① Site authorization authorizes the account to manage only the specified sites. The account does not have privileges over the branch to which the site belongs.

Search Branch ▼

- H3CLAB
 - > STORAGE
 - > TOKYO
 - > OSAKA

Cloudnetプラットフォームへのアクセス

パソコンをインターネットに接続し、ブラウザを開き、アドレスバーに<https://cloudnet.h3c.com>と入力します。表示されたログインページで、ユーザー名とパスワードを入力します。

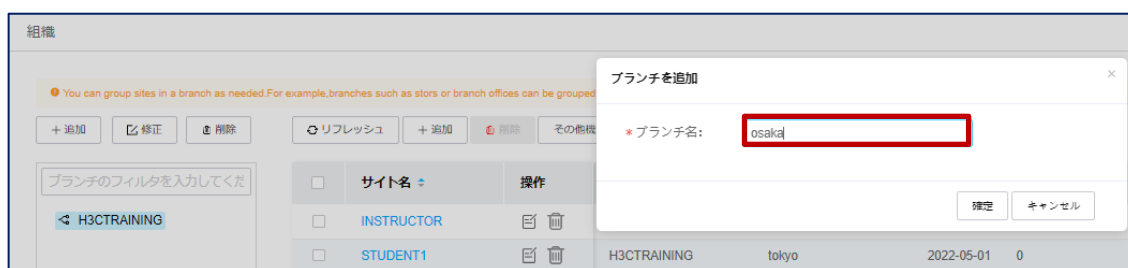
ブランチの設定

ブランチを追加、編集、または削除するには、次の作業を実行します。

ブランチを追加する

1. トップナビゲーションバーで、**ネットワーク**をクリックします。
2. 左側のナビゲーションペインで、**ネットワーク > 組織**を選択します。
3. 開いたページで、ルートブランチを選択し、**追加**をクリックします。
4. ブランチ名を入力します。

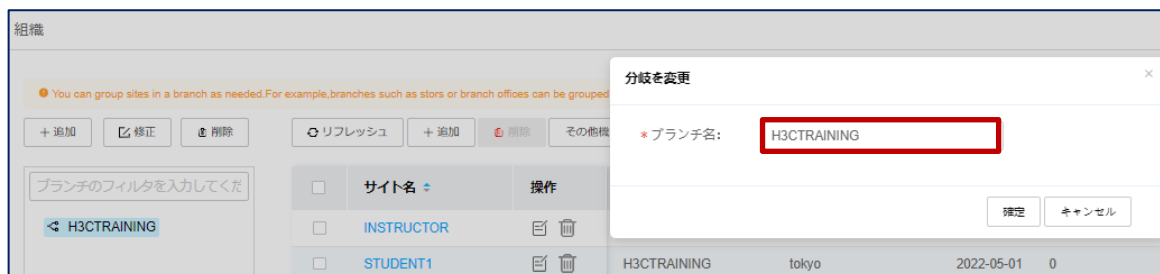
図1ブランチの追加



ブランチの名前を変更する

1. トップナビゲーションバーで、**ネットワーク**をクリックします。
2. 左側のナビゲーションペインで、**ネットワーク > 組織**を選択します。
3. 開いたページで、ターゲットブランチを選択し、**修正**をクリックします。
4. ブランチの名前を変更します。

図2ブランチ名の変更



ブランチを削除する

1. トップナビゲーションバーで、**ネットワーク**をクリックします。
2. 左側のナビゲーションペインで、**ネットワーク > 組織**を選択します。

- ターゲットブランチを選択し、削除をクリックします。ルートブランチは削除できません。
サイトまたはサブブランチを含むブランチを削除するには、まずサイトまたはサブブランチを削除します。

ブランチ作成のヒント

ダッシュボードはブランチ単位で表示されます。このダッシュボードではブランチ内のサイトがすべて表示されます。1つのブランチに24以上のサイトを登録すると全体を見渡して故障のCloudAPがどのサイトにあるのかが見つけづらくなります。そのため、24を超えるサイトがある場合、ブランチを増やしてそれぞれのブランチに分けて配置すると見やすくなります。以下の例ではCHIBA-EASTというブランチに20のサイトを配置しました。

これが24のサイトを超えるようであれば、CHIBA-EAST2のように新たなブランチを設けてそちらにサイトを作成します。

上の例のサイトは以下のように作成しております。

サイト名	操作	ブランチ
CHIBA-SHI-SITE1	[編集] [削除]	CHIBA-EAST
CHIBA-SHI-SITE10	[編集] [削除]	CHIBA-EAST
CHIBA-SHI-SITE11	[編集] [削除]	CHIBA-EAST
CHIBA-SHI-SITE12	[編集] [削除]	CHIBA-EAST
CHIBA-SHI-SITE13	[編集] [削除]	CHIBA-EAST
CHIBA-SHI-SITE14	[編集] [削除]	CHIBA-EAST
CHIBA-SHI-SITE15	[編集] [削除]	CHIBA-EAST
CHIBA-SHI-SITE16	[編集] [削除]	CHIBA-EAST

以下は上の例のCHIBA-EASTをCHIBA-EASTとCHIBA-EAST2に分割した例。

☒ CHIBA-EAST



☒ CHIBA-EAST2



サイトを追加する

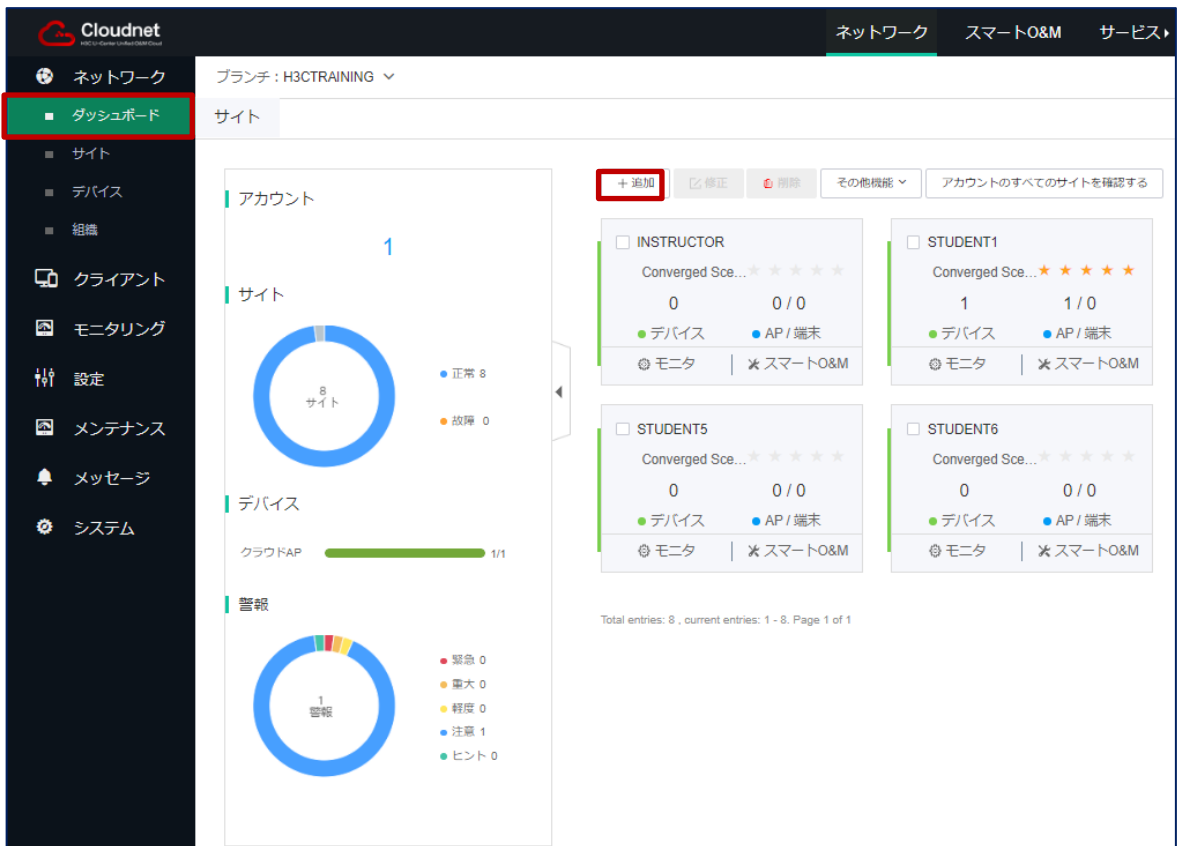
1. トップナビゲーションバーで、**ネットワーク**をクリックします。
2. 次のいずれかのタスクを実行します。
 - 左側のナビゲーションペインで、**ネットワーク > ダッシュボード**を選択します。作業ペインの左上隅から目的のブランチを選択し、**追加**をクリックします。
 - 左側のナビゲーションペインで、**ネットワーク > 組織**を選択します。組織ペインでターゲットブランチを選択し、サイトリストの上にある**追加**をクリックします。

図3と図4では、例として**ネットワーク > ダッシュボード**ページを使用しています。

図3 サイトを初めてブランチに追加する

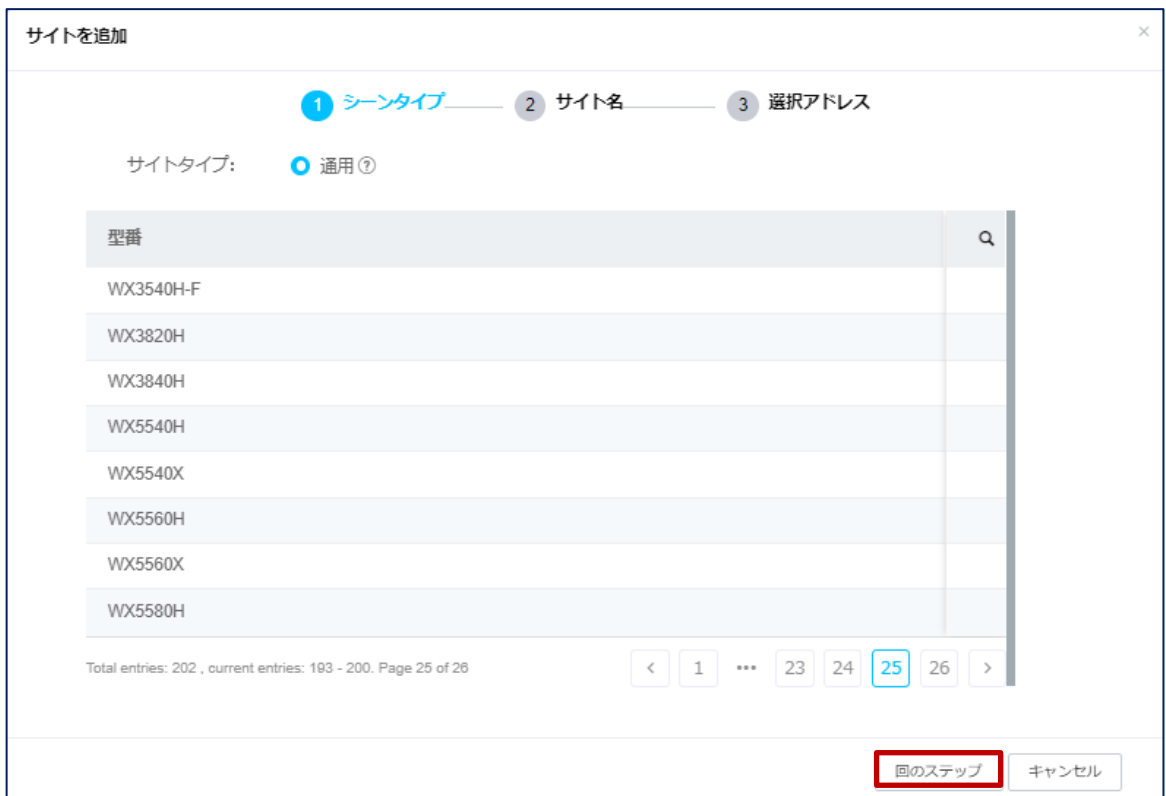


図4 サイトを含むブランチへのサイトの追加



3. ダッシュボードから+追加を選択し、シーンタイプフィールドから型番を選択して、回のステップ (nextの意味)をクリックします。

図5 シーンタイプ指定



4. サイト名を入力し、支店と所属業界を選択し、必要に応じて連絡先とサイト概要を指定して、**回のステップ**をクリックします。

図6 サイトの追加

サイトを追加

① シーンタイプ ② **サイト名** ③ 選択アドレス

*サイト名:

*分岐: Branch Management

*所属業界は:

連絡先:

サイト概要:

前のステップ **回のステップ** キャンセル

5. 現在位置の地図がでますので、確認して**確定**をクリックします。

サイトを追加

① シーンタイプ ② サイト名 ③ **選択アドレス**

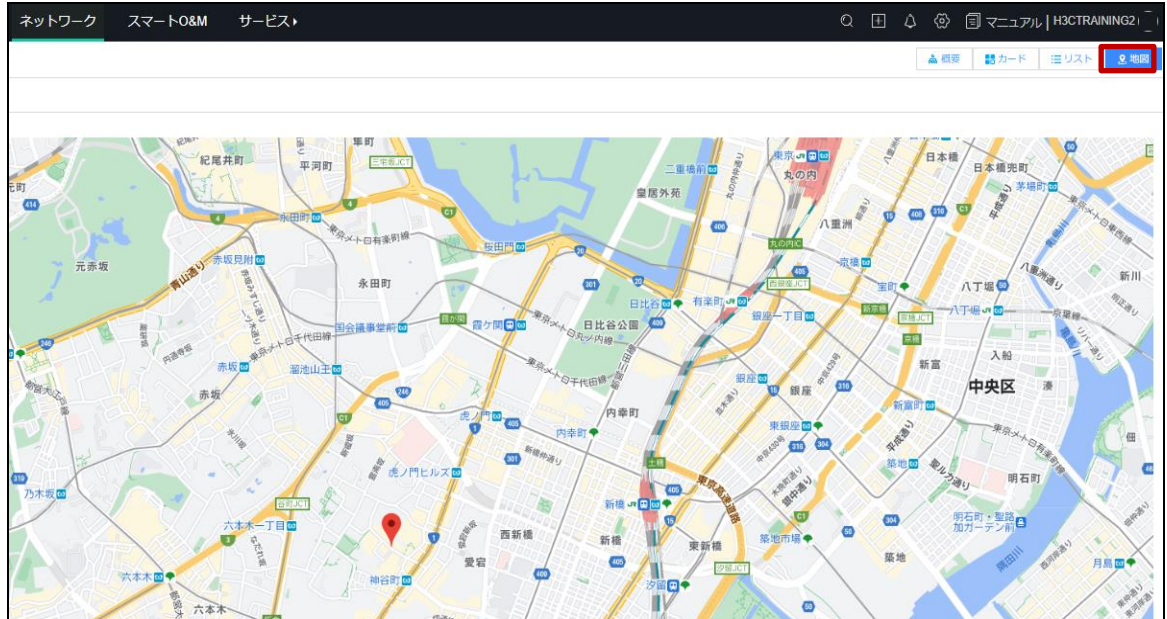
*詳細アドレス: 日本、〒105-0001 東京都港区虎ノ門4丁目3-10 虎ノ門きよしビル



位置アイコンをドラッグしたり、地図上で直接クリックして設定可能なサイトの住所を選択します。

前のステップ **確定** キャンセル

ちなみに、この地図はダッシュボードの右上の地図ボタンをクリックすると確認できます。



サイトにCloudAPを登録する

装置の登録は**サイト画面**では1台ずつ追加するのですが、**デバイス画面**(「デバイスをまとめて追加する」)ではExcelに装置一覧を作成して一括アップロードすることができます。

状態	デバイス名	シリアル番号	タイプ	型番	サイト名	デバイスバージョン	+/-
●	WA6638J	219801A2KF820BE000G6	Cloud AP	WA6638-JP	STUDENT8	Release 2459	
●	WA538J	219801A2959199G0000J	Cloud AP	WA538-JP	STUDENT8	Release 2449P11	

同じサイトに登録されたCloudAPは全て同じ設定(**設定 > クラウドAP > WiFi設定** で設定した項目)がコピーされます。

※例外: 先ほどのWiFi設定で設定した項目以外の機能を直接APにコンソールアクセスしてCLIで変更した項目はCloudnetでは関知しませんので、それぞれのCloudAPが異なる設定を持つことはあります。

エリアを追加する

ネットワーク上に多数のAPがあるシナリオでは、Cloudnetプラットフォームのエリア管理機能を使用して、APの場所、重要度、統計要件、またはその他の原則に基づいて、ネットワークをより小さな範囲に分割できます。

エリア管理では、ページにカードのようなエリアが表示されます。これにより、管理者は直観的な管理操作を使用して、すべてのエリアと特定のAPを管理できます。

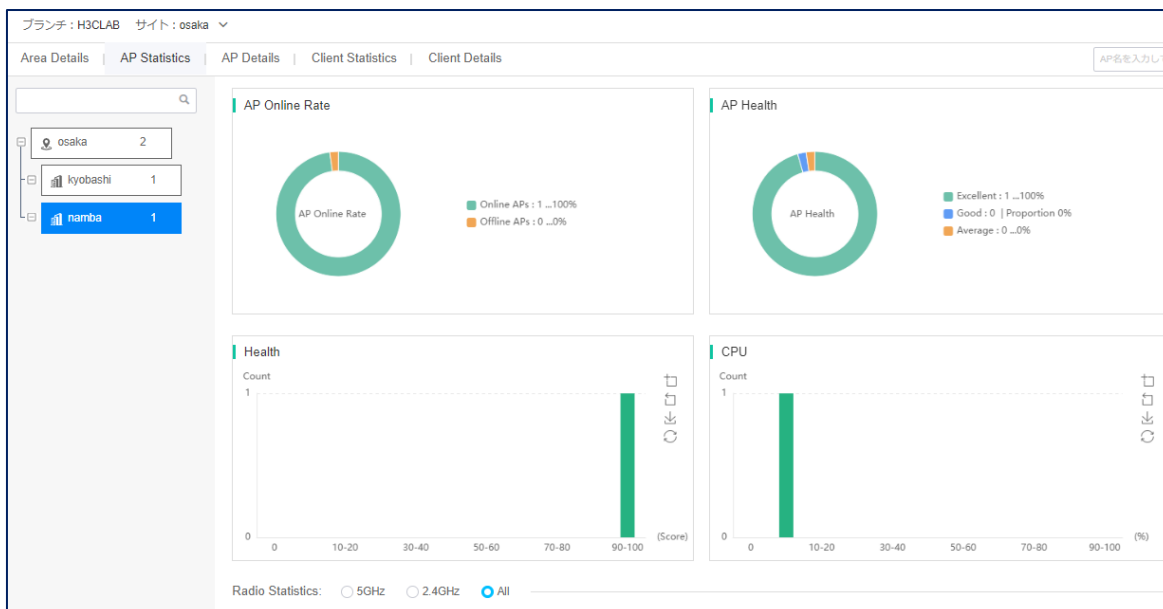
1. 画面中央上のメニューでネットワークを選択します。
2. 左のナビゲーションペインでサイト > エリア管理を選択します。
編集ボタンをクリックするとエリアを追加することができます。



エリア毎の健康状態を確認することができます。

1. 画面中央上のメニューで**スマートO&M**を選択します。
2. 左のナビゲーションペインで**ダッシュボード > Area Analysis**を選択します。

エリアごとの健康状態なので統計情報を表示することができます。



エリアを設定してある場合、後述の「**障害情報のメール通知**」によりエリアを限定(オープン)するとエリア内のAPの電波の利用状況のみを通知するようになり、その他の一切の状態の通知は行われませんので注意してください。

警報分類	警報タイプ	警告レベル	トリガーアラームの説明
Smart O&M	<input checked="" type="checkbox"/> High 2.4GHz channel usage	注意	AP 2.4 GHz無線周波数リアルタイムチャンネル利用率がを超えています (は60)
	<input checked="" type="checkbox"/> High 5GHz channel usage	注意	AP 5 GHz無線周波数リアルタイムチャンネル利用率はを超えています (0)
	<input checked="" type="checkbox"/> Too many clients on 2.4 GHz radios	注意	AP 2.4 GHz無線周波数リアルタイムアクセス端末数がを超えています (20)
	<input checked="" type="checkbox"/> Too many clients on 5 GHz radios	注意	AP 5 GHz無線周波数リアルタイムアクセス端末数がを超えています (0) ;

デバイスを追加する

❗重要:

- デフォルトでは、デバイスはDHCPを介してIPアドレスを取得します。デバイスがCloudnetプラットフォームに接続するには、IPアドレスを使用してインターネットにアクセスできることを確認してください。
- 追加するデバイスがCloudnetサーバーアドレスを正しく変換できることを確認します。
- **Firewallでは以下のポートがオープンである必要があります**
 - ログイン、認証のためのポート
TCP 80
TCP 443
 - Cloudnet通信用
TCP 19443 (デフォルト)変更するには以下のコマンドで行います
cloud-management server port port-number
 - NTPサーバーポート
UDP 123

サイトを作成した直後にデバイスをサイトに追加するか、次の手順を実行して既存のサイトにデバイスを追加します。

1. トップナビゲーションバーで、**ネットワーク**をクリックします。
2. 左側のナビゲーションペインで、**ネットワーク > デバイス**を選択します。
3. ページの左上隅から装置を登録するターゲットのブランチとサイトを選択し、**+デバイスの追加**をクリックします。
4. **デバイス名、シリアル番号、およびデバイスタイプ(一般デバイス,IRFデバイス)**を指定し、**デバイスの追加**をクリックします。

※装置のシリアル番号は装置のCLIコマンドで確認できます。

```
<CLOUDAP>dis device manuinfo  
DEVICE_NAME:WA6638  
DEVICE_SERIAL_NUMBER:219801A24F8201E0009X  
MAC_ADDRESS:F010-90F3-61A0  
MANUFACTURING_DATE:2020-02-29  
VENDOR_NAME:H3C
```


図7 デバイスの追加



デバイス情報

サイト: INSTRUCTOR

サイトがありませんか? 追加してください

* デバイス名 ①: 30ビット以下の文字を入力してください

* シリアル番号: 11-64桁の数字の下線または横棒で構成されています

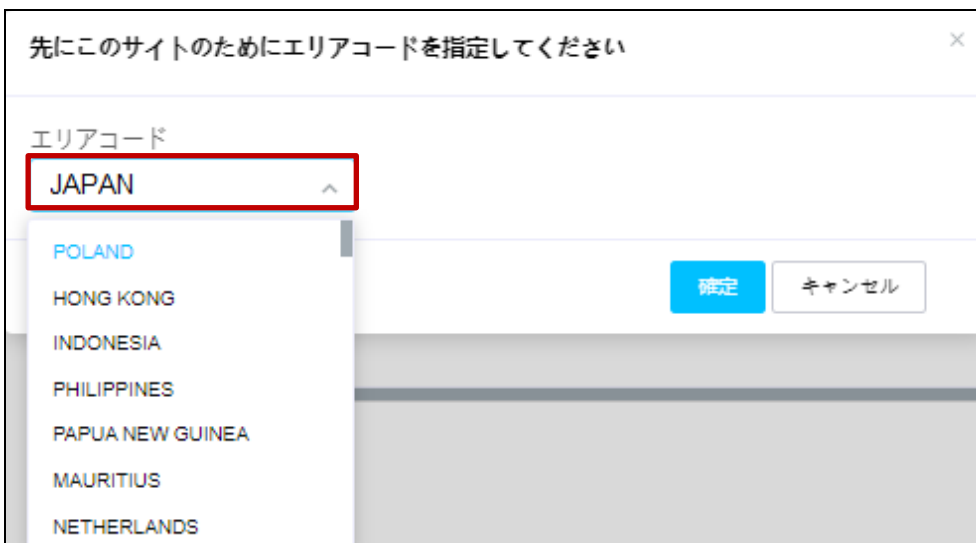
IRFデバイスですか: 一般 IRFデバイス

デバイスの追加

Cloudnetではデバイスはシリアル番号のみで装置と通信しますので、IPアドレスの入力は不要です。**Cloudnetとデバイスの間はhttps + tlsでの暗号化でトンネルを作成して通信**しており、デバイスからCloudnetへアクセスするパケットにシリアル番号の情報が含まれておりますので、装置を識別することができます。

デバイスを初めて追加する場合は、エリアコードを選択する必要があります。

図8 エリアコードの選択



先にこのサイトのためにエリアコードを指定してください

エリアコード

JAPAN

POLAND

HONG KONG

INDONESIA

PHILIPPINES

PAPUA NEW GUINEA

MAURITIUS

NETHERLANDS

確定 キャンセル

デバイスがオンラインになるまで数分かかる場合があります。後でページを更新して、デバイスがオンラインになったことを確認してください。

図9 デバイステータスの確認

The screenshot shows the Cloudnet management interface. The left sidebar contains navigation options: ネットワーク, ダッシュボード, サイト, デバイス (highlighted), 組織, クライアント, モニタリング, 設定, and メンテナンス. The main content area shows the 'デバイス' (Devices) page for branch 'H3CTRaining'. It includes a 'デバイスタイプ' (Device Type) filter set to 'クラウドAP' (Cloud AP) and a row of action buttons: リフレッシュ, 削除, 再起動, クラウド接続をreset, アップグレードバージョン, CLIヘルプ, ファイルシステム, and ローカル. Below this is a table with columns: 状態 (Status), 修正 (Edit), デバイス名 (Device Name), グローバルIP (Global IP), シリアル番号 (Serial Number), and タイプ (Type). The table contains one entry for 'FAT AP' with a green dot in the status column, indicating it is online. The footer shows 'Total entries: 1, current entries: 1 - 1. Page 1 of 1'.

状態	修正	デバイス名	グローバルIP	シリアル番号	タイプ
<input checked="" type="checkbox"/>		FAT AP	123.220.233.36	219801A2KF820BE0004H	Cloud AP

デバイスをまとめて追加する

①注意:

- 現在、以下の操作は日本語のページではExcelのテンプレートのダウンロードがエラーになりますので、この操作の際は言語をENのページにしてテンプレートをダウンロードしてください。現在一部中国語表記が残っておりますので、修正中です。

1. トップナビゲーションバーで、ネットワークをクリックします。
2. 左側のナビゲーションペインで、ネットワーク > デバイスを選択します。
3. ページの左上隅から装置を登録するターゲットのブランチとサイトを選択し、ページの右上のその他の機能から導入をクリックします。



ここで“[点击下载模板](#)”つまり、“クリックしてテンプレートをダウンロード”をクリックして、まとめて登録する装置を登録するExcelファイルをダウンロードし、そこへ装置を登録します。

4. ファイルアップロードの欄をクリックしてファイルを選択します。
5. アップロードが成功すると以下のメッセージが表示されます。



Excelの入力項目は以下の通りです。

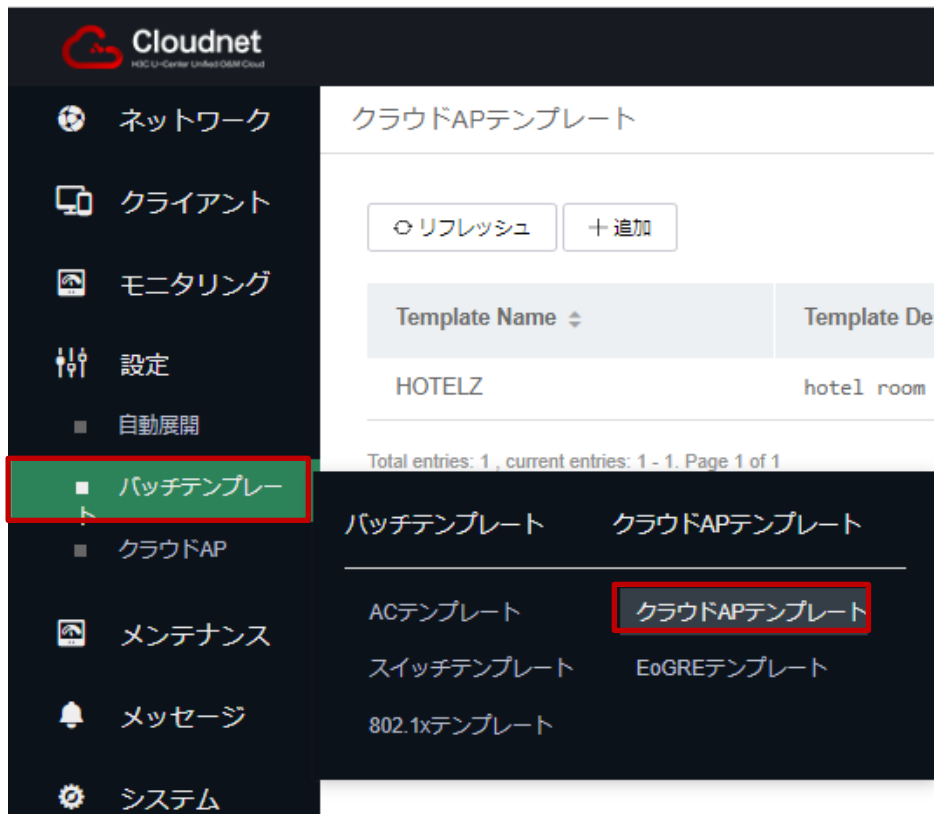
- ・サイト名(現在装置を登録しようとしているサイト名)
- ・装置名
- ・シリアル番号

	A	B	C
1	Site	Device Name	SN
2	サイト名を入力	装置名を入力	シリアル番号を入力
3			
4			

クラウドAPテンプレートを利用した設定

クラウド管理APを多く設置する際に、それぞれの設定のテンプレートを用意おくことにより、設定の手間が軽減されます。

1. トップナビゲーションバーで、ネットワークをクリックします。
2. 左側のナビゲーションペインで、設定 > バッチテンプレート > クラウドAPテンプレート > クラウドAPテンプレートを選択します。現れた画面で+追加をクリックします。



3. テンプレートの名前を設定し、エリアコードを選択します。

The screenshot shows the configuration form for a Cloud AP template. It includes a text input field for '* Template Name:' with the value 'HOTELZ' highlighted by a red box. Below it is a text area for 'Template Description:' containing 'hotel room AP configuration'. There are three tabs: 'エリアコード' (selected), 'Wi-Fi設定', and 'CLI'. A 'リスト' toggle switch is turned on. At the bottom, there is a dropdown menu for 'エリアコード:' with 'JAPAN' selected, highlighted by a red box.

4. CLIを選択して、以下の図の「を追加してください」をクリックします。

Cloudnet
KDC Li Center Limited OBM Cloud

クラウドAPテンプレート

Back

* Template Name: HOTELZ

Template Description: hotel room AP configuration

エリアコード Wi-Fi設定 **CLI**

リスト

データがありません, **を追加してください**

5. APの機種を選択して**確定**をクリックします。

Add

Device Model: All Select

<input type="radio"/> WA530-WW	<input type="radio"/> WA538-JP	<input type="radio"/> WA6636	<input type="radio"/> WA6330
<input type="radio"/> WA6320	<input type="radio"/> WA6320H	<input type="radio"/> WA6622	<input type="radio"/> WA6628
<input type="radio"/> WA6638	<input type="radio"/> WA6630X	<input type="radio"/> WA6628X	<input type="radio"/> WA6628E-T
<input type="radio"/> WA6620X	<input checked="" type="radio"/> WA6638-JP	<input type="radio"/> WA6630X-JP	<input type="radio"/> WA6320-JP
<input type="radio"/> WA6526E	<input type="radio"/> DH-AWA6220-W	<input type="radio"/> DH-AWA6220-C	<input type="radio"/> DH-AWA6220-O
<input type="radio"/> DH-AWA6330-C			

確定 キャンセル

6. Cloudモードで自動的に設定されるもの以外で、特別の設定が必要な場合、CLIコマンドを以下の編集の入力欄に入力します。そして**Save**をクリックします。

コマンドは10まで、それぞれのCLIコマンドの形式は以下の通りです：

return

system-view

CLIコマンド

エリアコード Wi-Fi設定 **CLI**

リスト

1. Perform CLI configuration under guidance of professionals. To avoid conflicts, do not add the same configuration repeatedly.
2. *例*のコマンド形式設定コマンドに従って、システムビューに入ってからコマンドを作成してください、すなわち、*例*のreturn system-viewの後
3. You can create a maximum of 10 Configlets in one bulk configuration template.

+追加

WA6638-JP ×

説明: LED setting

* CLI: 編集

```
return
system-view
wlan led-mode quiet
```

7. Cloudモードで自動的に設定されるもの以外で、特別の設定が必要な場合、CLIコマンドを以下の編集の入力欄に入力します。そして**Save**をクリックします。

8. **Wi-Fi設定**をクリックしてカスタマイズするSSIDを選択します。

番号 ⇅	SSID ⇅	サービス状態 ⇅
1	H3C_WiFi_1	オープン
2	H3C_WiFi_2	クローズ
3	H3C_WiFi_3	クローズ
4	H3C_WiFi_4	クローズ
5	H3C_WiFi_5	クローズ
6	H3C_WiFi_6	クローズ
7	H3C_WiFi_7	クローズ
8	H3C_WiFi_8	クローズ
9	H3C_WiFi_9	クローズ
10	H3C_WiFi_10	クローズ

Wi-Fi設定をクリックしてカスタマイズするSSIDを選択します。

一般的には、SSIDの表示名の変更、PSKによるパスワードの入力、同じWiFiに接続しているクライアント同士の通信を拒否するなどの設定を行います。設定したら**確定**をクリックします。

The screenshot shows a configuration page with two sections: '基本設定' (Basic Settings) and '高級な構成' (Advanced Configuration). In the '基本設定' section, the '自動SSID' (Auto SSID) is set to 'クローズ' (Closed), the 'SSID' is 'hotelz', and the 'サービス状態' (Service Status) is 'オープン' (Open). In the '高級な構成' section, 'AP転送モード' (AP Transfer Mode) is 'Bridgeモード', 'VLAN' is '1', '暗号化状態' (Encryption Status) is 'PSK', 'Security Mode' is 'WPA / WPA2-Compliant', 'Radioタイプ' (Radio Type) has both '2.4GHz' and '5GHz' checked, 'ユーザ分離' (User Separation) is 'オープン', 'ユーザ制限速度' (User Rate Limit) is 'クローズ', 'DHCP Option82' is 'クローズ', and 'EoGRE' is 'クローズ'. A red box highlights the 'SSID' field in the basic settings, and another red box highlights the '暗号化状態' (Encryption Status) section in the advanced settings. At the bottom, there are '確定' (Confirm) and 'キャンセル' (Cancel) buttons.

9. 全ての設定が完了したら**Save**をクリックして終了します。

The screenshot shows a template configuration page. The 'Template Name' is 'HOTELZ' and the 'Template Description' is 'hotel room AP configuration'. Below this, there are tabs for 'エリアコード', 'Wi-Fi設定', and 'CLI', with 'Wi-Fi設定' selected. A 'リスト' (List) toggle is turned on. A table displays the configuration for two templates:

番号	SSID	サービス状態
1	hotelz	オープン
2	H3C_WIFI_2	クローズ

At the bottom left, there is a red box around the 'Save' button.

10. テンプレートをCloudnetに登録されたAPIに適用するにはActionの**Apply**ボタンをクリックします。

Template Name	Template Description	Creator	Created At	Updated At	Action
HOTELZ	hotel room AP configuration	H3CTRaining2	2022-06-30 10:51:19	2022-06-30 11:54:26	

11. 適用するサイトを選択し、**Apply**をクリックするとAPIに適用されます。

Site	Branch	Cloud AP
<input checked="" type="checkbox"/> tokyo	TRAINING	1/1

クラウド管理APの設定

重要: CloudAPの設定は全てCloudnetで行います。ローカルで行うのはCloudAPがインターネットにアクセスできるようにすることのみです。SSIDの設定(15個のテンプレートが用意されておりますので、この範囲で利用してください)、VLANの作成、電波に関する設定などになります。従って、ローカルでの設定はCloudnetには現れませんので、管理が難しくなりますので、ローカルでの設定は基本的に行わないでください。

クラウドで管理されているAPを管理するには、トップナビゲーションバーのネットワークをクリックし、左側のナビゲーションページから設定 > クラウドAP > WLAN設定を選択して、ターゲットのブランチおよびサイトを選択します。必要に応じて、エリアコード、Wi-Fi設定、無線帯域設定およびネットワークの最適化を構成できます。

エリアコードを指定する

エリアコードタブで、エリアコードを選択し、確定をクリックします。

図10 エリアコードの指定

ブランチ: LABO サイト: FUNCTION_TEST ▾

エリアコード Wi-Fi設定 無線帯域設定 ネットワーク最適化

エリアコード: JAPAN ▾

確定

Wi-Fi設定の構成

ワイヤレスサービスの設定

ブランチ: LABO サイト: FUNCTION_TEST ▾

エリアコード **Wi-Fi設定** 無線帯域設定 ネットワーク最適化

無線サービス設定 ⓘ (Some cloud-managed AP models support only wireless)

目オープンサービス 目クローズサービス 目SSIDを隠す 目SSID表示

<input type="checkbox"/>	番号 ⇅	SSID ⇅	サービス状態 ⇅
--------------------------	------	--------	----------

❗重要:

- **WiFi設定はサイトに登録された全てのCloudAPで同じ設定が適用されます。特定のCloudAPで異なる設定をする場合は、別のサイトを作成して、装置をそこに移設します。移設はネットワーク > デバイス > 装置を選択します。移設をクリックして、確定し、移設するサイトを選択し、確定をクリックするとサイトを移動できます。**
 - **サイトに登録された装置がすべて削除された場合でも、再度新たな装置を登録すると以前のWiFi設定はそのまま残っておりますので、その設定が装置にダウンロードされます。**
-

1. **Wi-Fi設定タブをクリックし、下向き矢印📄 をクリックして無線サービス設定メニューを展開します。必要に応じて、全無線サービスを表示するまたは[オープンした無線サービスのみを表示する]をクリックして、すべてのサービスまたは有効なサービスを表示できます。**
2. **ワイヤレスサービスを一括して有効または無効にするには、対象サービスを選択し、オープンサービスまたはクローズサービスをクリックします。**
3. **ワイヤレスサービスで非表示になっているSSIDを一括して有効または無効にするには、対象サービスを選択し、SSIDを隠すまたはSSID表示をクリックします。**
4. **ワイヤレスサービスを編集するには、サービスのSSIDをクリックし、必要に応じて次のパラメータを設定します。**

図11 SSID設定の編集

基本設定

自動SSID ①: オープン クローズ

* SSID: (1-32個文字)

SSID説明: (50文字を超えてはいけません)

サービス状態: オープン クローズ

高級な構成

AP転送モード:

* VLAN:

SSIDを隠す ①: オープン クローズ

暗号化状態 ①: PSK 802.1X クローズ

* Radioタイプ ①: 2.4GHz 5GHz

ユーザ分離 ①: オープン クローズ

ユーザー制限速度 ①: オープン クローズ

認証: オープン クローズ

DHCP Option82 ①: オープン クローズ

EoGRE ①: オープン クローズ

Filter Client MACs ①: OFF

Denylist Allowlist

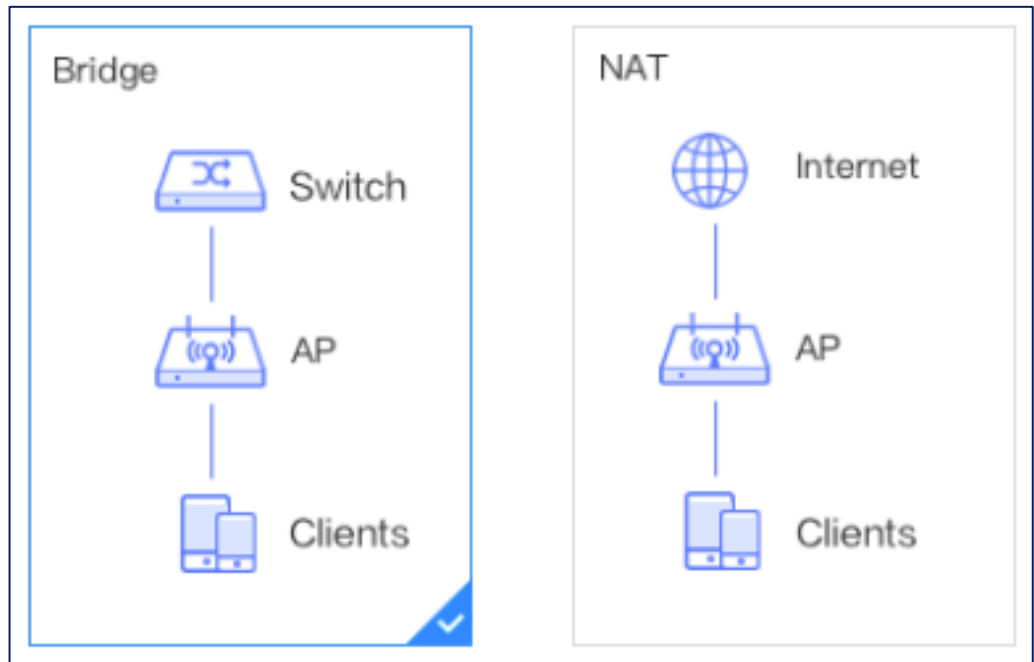
[Set Denylist](#) [Set Allowlist](#)

- **自動SSID:** システムは、構成されたSSIDとデバイス名を結合してSSID名を形成し、識別を容易にします。たとえば、構成されたSSIDがHotelでデバイス名が1103の場合、SSID名はHotel_1103になります。自動生成されるSSID名は32文字を超えることはできません。エラーを回避するため、長いSSIDは指定しないでください。

自動SSIDが有効になっている場合は、AP名を変更した後、またはAPをインポートした後に [Auto SSID Setting Sync] をクリックしてSSID設定をデバイスに展開する必要があります。

- **サービス状態:** オープンにするとこのSSIDが有効になります。
- **AP転送モード:**
 - **Bridgeモード:** VLANの設定をサポートし、APはワイヤレス端末アクセスの場合のレイヤー2転送にのみ使用され、DHCPサーバーは上位ゲートウェイデバイスです。APがPPPoEまたは静的IPアドレスでネットワークにアクセスする場合、ブリッジ転送方式はサポートされていません。

- **NATモード**: VLAN設定はサポートしておらず、APIは無線端末が接続される場合にDHCPサーバーとして機能します。



- **SSIDを隠す**: クライアントがアクティブスキャンによってSSIDを検出できないようにします。ネットワークにアクセスするには、ユーザーがSSIDを入力してパッシブスキャンを実行する必要があります。これにより、ネットワークセキュリティが強化されます。
- **暗号化状態**: システムでクライアントトラフィックを暗号化して、ネットワークセキュリティを強化できます。

- **PSKの場合**

暗号化状態 (?): PSK 802.1X クローズ

..... (説明: パスワー)

Security Mode (?): WPA / WPA2-Compliant ^

* Radioタイプ (?): WPA / WPA2-Compliant

ユーザ分離 (?): WPA2

WPA3

Security Modeの違いについて

WPA/WPA2-Compliant を選択

CloudAP に送信された設定 :

```
wlan service-template 1
ssid XXXX
cipher-suite ccmp          # AES
cipher-suite tkip         # TKIP
security-ie rsn           # WPA2
security-ie wpa           # WPA
```

WPA2 を選択

CloudAP に送信された設定 :

```
wlan service-template 1
ssid XXXX
cipher-suite ccmp          # AES
cipher-suite tkip         # TKIP
TKIP security-ie rsn      # WPA2
```

WPA3 を選択

CloudAP に送信された設定 :

```
wlan service-template 1
ssid XXXX
cipher-suite ccmp          # AES
security-ie rsn           # WPA
wpa3 personal optional    # WPA3 セキュリティモードをオプションに指定する
pmf optional              #保護管理フレーム機能をオプションモードに指定
```

● **802.1Xの場合**

暗号化状態 (?:) PSK 802.1X クローズ

配置RADIUS (?:) 内置服务器 (Built-In) 外置服务器 (External)

● **802.1xのRADIUSの配置がBuilt-in (CloudAP自身をRADIUSサーバーとして利用する場合) の場合のユーザー登録**

上部のナビゲーションバーネットワークをクリックし、左側のナビゲーションペインで **設定 > クラウドAP > ユーザー管理** をクリックします。そして、802.1x認証ユーザータブで **+** 追加をクリックします。必要なユーザー名、パスワードなどを入力し、**確定** をクリックします。

登録できるユーザーは最大512です。

設定情報が **permanent** の場合

Add Auth Account ×

* Account: ?

* Password: ?

Name:

Description:

Validity Period: Permanent Limited

設定情報が**Limited**の場合

Add Auth Account ×

* Account: ?

* Password: ?

Name:

Description:

Validity Period: Permanent Limited

Expire At: 📅

ユーザー登録は事前にインポートするExcelのテンプレートをダウンロードして、そこにユーザー名とパスワードを記入しておき、それをインポートします。



インポートするExcelの形式は以下の通り。

Account name	Password(6-32 characters without spaces)	Max Users (1-255)	MAC address binding	Remarks	Email	Send email	Effective time(integer day)
Each account Multiple MAC and Max Users can only fill in one of them. MAC address format: AA-BB-CC-DD-EE-FF. Multiple MAC addresses are comma separated. The upper limit is 255 for bound MAC addresses. The input value of valid time is 0~365, and no input and input "0" mean permanent validity . You can import a maximum of 1000 fixed accounts at a time .							

● 802.1xのRADIUSの配置がExternal場合

RADIUSサーバーをExternalとした場合、APから直接RADIUSサーバーへアクセスするので、APからRADIUSサーバーへのアクセスができるようになっている必要があります。

以下は上記画面を部分部分で拡大したもの。

認証サーバ

* ホストサーバIP: 10.10.11.27

スタンバイサーバIP: サーバIPを入力してください

課金サーバ

* ホストサーバIP: サーバIPを入力してください

スタンバイサーバIP: サーバIPを入力してください

* ISPドメイン名: ISPドメイン名を入力してください

ドメイン名の配布方法: ドメイン名を携帯して ドメイン名を持たない

* ポート号: 1812

ポート号: 1-65535

* ポート号: 1813

ポート号: 1-65535

* 認証共有鍵: 

* 課金共有鍵: 鍵を入力してください 

高級な構成 

応答タイムアウト時間: 秒

最大試行回数: 回

サイレント時間: 分

リアルタイム課金間隔: 秒

リアルタイム課金最大試行: 回

- Portal認証の場合のユーザー登録

上部のナビゲーションバーネットワークをクリックし、左側のナビゲーションペインで設定 > クラウドAP > ユーザー管理をクリックします。そして、Portal認証ユーザータブで+追加をクリックします。必要なユーザー名、パスワードなどを入力し、確定をクリックします。設定情報がバインディングMACの場合

アカウントを追加 ×

* アカウント名: (1-28ビット非スペース文字)

* パスワード: (6-32ビット非スペース文字) 🗨

* パスワードを確認してください: 🗨

備考:

メールボックス:

メールでアカウント名のパスワードを送信する

有効期間: 日
(空白または0は、永続的な有効性を意味します)

設定情報: バインディングMAC 人数制限

次のように入力してかつ英語コンマで区切られています

AA-BB-CC-DD-EE-FF,
GG-HH-II-JJ-KK-LL

設定情報が人数制限の場合

アカウントを追加

* アカウント名:

* パスワード:

* パスワードを確認してください:

備考:

メールボックス:

メールでアカウント名のパスワードを送信する

有効期間: 日
(空白または0は、永続的な有効性を意味します)

設定情報: バインディングMAC 人数制限

許可されたインターネット利用者数 (1-255) を入力してください

- **ユーザー分離**: 同じAPから提供された同じSSIDにアクセスするクライアントを分離します。
- **ユーザー制限速度**: Rateは、SSIDにアクセスするクライアントのデータ送受信を制限します。
- **認証**: オープンに設定して、**認証設定**をクリックすると後術の「**ワイヤレス認証の設定**」に移動し、そこでWeb認証画面の設定を行う。

認証: オープン クローズ

認証脱出: オープン クローズ

- **DHCP option82:** オプション82は、DHCPメッセージのオプションフィールドのリレーエージェントオプションです。DHCPクライアントの位置情報を記録します。DHCPリレーエージェントまたはDHCPスヌーピングデバイスは、クライアントの要求を受信すると、要求メッセージにオプション82を追加して、サーバーに送信します。
- **EoGRE(Ethernet over GRE):** Ethernet over GRE (EoGRE)は、イーサネットプロトコルをIPネットワーク上の仮想ポイントツーポイントトンネルにカプセル化できるトンネリングプロトコルです。イーサネットフレームは、一方のトンネルエンドでカプセル化され、もう一方のトンネルエンドでカプセル化が解除されます。
- **クライアントMACフィルタリング:**

クライアント MAC 許可リストを有効にすると、許可リストのクライアントのみがワイヤレス サービスにアクセスできます。クライアント MAC 拒否リストが有効になっていると、拒否リストのクライアントはワイヤレス サービスにアクセスできません。

一部のクラウド管理 AP モデルのみがこの機能をサポートしています。詳細については、Cloudnet リリース ノートを参照してください。

ブラックリストとホワイトリスト作成上の注意事項は、ホワイトリストの方がアクセス制限が強いいためリストに抜けが無いように気を付けてください。

ブラックリスト:

+追加を選択すると以下のようにMACアドレスを追加することができます。

The screenshot shows the 'MACアドレス拒否リスト' (MAC Address Deny List) tab selected. A modal window titled 'MACアドレスを追加' (Add MAC Address) is open, displaying a form with the following fields:

- MAC: 8C-55-4A-FD-69-8D
- MACマスク: ff-ff-ff-ff-ff
- 説明: 1-128文字

A warning message is displayed above the form: "ハイフン(-)またはセミコロン(;)で区切られた、大文字と小文字を区別しない数字または文字の形式がサポートされています: AA-cc-bB-67-e3-00、4532-AbCD-7FdC、AA:cc:BB:67:e3:00、及び AA-BB-CC".

追加された結果は以下のように表示されます。

MACアドレス許可リスト		MACアドレス拒否リスト	
<input type="checkbox"/>	MAC	MACマスク	説明
<input type="checkbox"/>	8c-55-4a-fd-69-8d	ff-ff-ff-ff-ff	

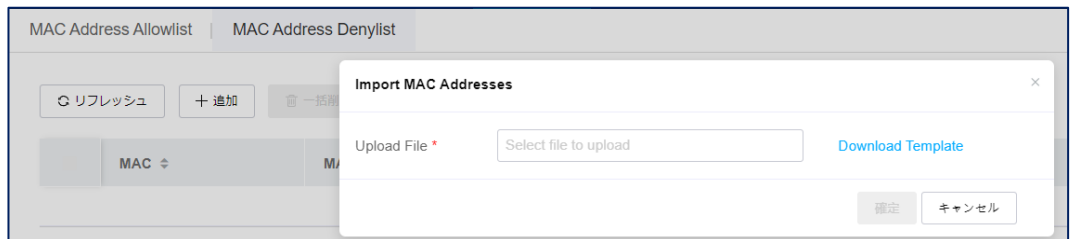
第 1 ~ 1 エントリーを表示する(総計 1 エントリー)

Client Type ⇅	ACL Number ⇅	Rule ID ⇅
	4000	0

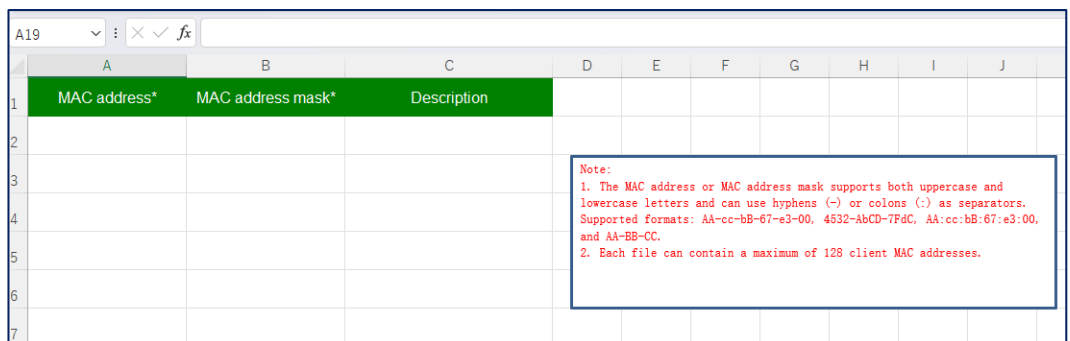
この結果は、CloudAPIには以下のように反映されます：

```
wlan service-template 1
ssid CLIENT
portal enable method direct
portal domain cloud
portal apply web-server 1
portal apply mac-trigger-server cloud
portal temp-pass enable
access-control acl 4000
#
service-template enable
acl number 4000
rule 0 deny source-mac 8c-55-4a-fd-69-8d ffff-ffff-ffff
rule 65534 permit
#
```

インポートを選択すると以下のようなファイル選択画面が表示されますが、“[Download Template](#)”をクリックすると以下のようにテンプレートをダウンロードすることができます。



クライアントのMACアドレス一覧を記入するアドレスリストのテンプレート



このテンプレートに許可するクライアントのMACアドレスを記述すると一度に多くのMACアドレスを入力することができます。

ホワイトリスト:

設定方法は上記のブラックリスト同様

ドメイン名のホワイトリストまたはブラックリストの設定

1. **Wi-Fi設定**タブをクリックし、下向きの矢印📄をクリックして**ドメイン名と白黒リスト**メニューを展開します。
2. **ドメイン名ホワイトリスト**または**ドメイン名ブラックリスト**を選択して、ホワイトリストまたはブラックリストを編集します。必要に応じてエントリを追加または削除できます。

オンラインクライアントは、ホワイトリスト内のドメインに認証なしで直接アクセスできます。ブラックリスト内のドメインにはアクセスできません。

ホワイトリストとブラックリストの両方にドメイン名が存在する場合、ブラックリストが有効になります。

図12 ドメイン名のホワイトリストまたはブラックリストの設定

ドメイン名	説明	操作
www.baidu.com		🗑️

無線帯域設定

1. **設定 > クラウドAP > WLAN設定 > 無線帯域設定**タブをクリックします。

高密度カバール

ホテル

2. シナリオを選択します。オプションは次のとおりです。
 - **高密度カバール**: 大規模な会議室、食堂、展示ホール、コロケーションオフィスなど、障害物の少ない高密度AP配置に適用できます。
 - **ホテル**: 1つのAPが1つまたは2つの部屋をカバーするシナリオに適用されます。
 - **独立したオフィス**: 1つのAPが1つまたは2つの部屋をカバーしているシナリオに適用できます。
 - **コマーシャルストア**: 十分なチャネルリソースがある低密度AP配置に適用できます。
 - **デフォルト**: デフォルトの展開方法。ほとんどのシナリオに適用できます。

- **カスタム:** 実際の環境に基づいて帯域幅と送信電力を設定できます。

高密度カバー (遮られていない空間APの設定が密集、人員密集、例えば大型会議室、食堂、ショールーム、集中事務)	ホテル (一つのAPは1から2つの部屋をカバーしています)	独立したオフィス (一つのAPは1から2つの部屋をカバーしています)
2.4G チャンネル: auto(デフォルト) 電力: 60% 周波数帯: 20	2.4G チャンネル: auto(デフォルト) 電力: 80% 周波数帯: 20	2.4G チャンネル: auto(デフォルト) 電力: 80% 周波数帯: 20
5GHz-1 チャンネル: auto(デフォルト) 電力: 80% 周波数帯: 20	5GHz-1 チャンネル: auto(デフォルト) 電力: 100%(デフォルト) 周波数帯: 40	5GHz-1 チャンネル: auto(デフォルト) 電力: 100%(デフォルト) 周波数帯: 40
5GHz-2 チャンネル: auto(デフォルト) 電力: 80% 周波数帯: 20	5GHz-2 チャンネル: auto(デフォルト) 電力: 100%(デフォルト) 周波数帯: 40	5GHz-2 チャンネル: auto(デフォルト) 電力: 100%(デフォルト) 周波数帯: 40

コマーシャルストア (エリア内のAPの総数が少なく、チャンネル資源が十分です)	デフォルト (デフォルト設定、大部分のシーンに適用されます)
2.4G チャンネル: auto(デフォルト) 電力: 80% 周波数帯: 20	2.4G チャンネル: auto(デフォルト) 電力: 100%(デフォルト) 周波数帯: 20
5GHz-1 チャンネル: auto(デフォルト) 電力: 100%(デフォルト) 周波数帯: 80(デフォルト)	5GHz-1 チャンネル: auto(デフォルト) 電力: 100%(デフォルト) 周波数帯: 80(デフォルト)
5GHz-2 チャンネル: auto(デフォルト) 電力: 100%(デフォルト) 周波数帯: 80(デフォルト)	5GHz-2 チャンネル: auto(デフォルト) 電力: 100%(デフォルト) 周波数帯: 80(デフォルト)

- 無線設定を編集します。クラウド管理APリストで、ターゲットAPの編集をクリックし、必要に応じて無線設定を行います。

Single-AP Configuration						
● You can adjust radio parameters for a single AP in this section.						
オンライン状態	AP名	AP>リアル番号	2.4GHz			
			状態	チャンネル	電力	周波数帯域
●	WA6638NOTJP	219801A24F8201E0000J	オープン	AUTO(デフォルト)	60%	20

5GHz-2				操作
状態	チャンネル	電力	周波数帯域	
オープン	AUTO(デフォルト)	80%	20	編集

図18 無線設定の編集

修正Radio状態

2.4GHz

状態: オープン クローズ

電力: 100%

チャンネル: AUTO

周波数帯域: 1, 2, 3, 4, 5, 6, 7

5GHz-1

状態:

電力:

チャンネル: AUTO

周波数帯域: 80

確定 キャンセル

←電力
30,40,50,60,70,80,90,100%

←チャンネル
AUTO,1 から
13

修正Radio状態

2.4GHz

状態: オープン クローズ

電力: 100%

チャンネル: AUTO

周波数帯域: 20

5GHz-1

状態: 周波数帯域を選択してください
20
40

電力: 100%

チャンネル: AUTO

周波数帯域: 80

確定 キャンセル

修正Radio状態

5GHz-1

状態: オープン クローズ

電力: 100%

チャンネル: AUTO

周波数帯域: 36, 40, 44, 48, 52, 56, 60

5GHz-2

状態:

電力:

チャンネル: AUTO

周波数帯域: 80

確定 キャンセル

←チャンネル
 AUTO,36,40,
 44,48,52,56,6
 0,64

修正Radio状態

5GHz-1

状態: オープン クローズ

電力: 100%

チャンネル: AUTO

周波数帯域: 80

5GHz-2

状態: 周波数帯域を選択してください

電力: 20, 40, 80

チャンネル: AUTO

周波数帯域: 80

確定 キャンセル

ネットワーク最適化

1. 設定 > クラウドAP > WLAN設定 > ネットワーク最適化タブをクリックして基本設定メニューが現れます。
2. 必要に応じて、次の設定を行います。

図13 基本設定の構成

基本設定		
5GHz優先 ?	<input checked="" type="radio"/> オープン	<input type="radio"/> 閉じる
ロードバランス ?	<input checked="" type="radio"/> オープン	<input type="radio"/> 閉じる
ローミングナビ ?	<input checked="" type="radio"/> オープン	<input type="radio"/> 閉じる
5GHz 無線ロードバランス ?	<input checked="" type="radio"/> オープン	<input type="radio"/> 閉じる
Broadcast Optimization ?	<input checked="" type="radio"/> オープン	<input type="radio"/> 閉じる
Broadcast Control ?	<input type="radio"/> オープン	<input checked="" type="radio"/> 閉じる

オープンは機能を有効にします。閉じるは機能を無効にします。

5 GHz優先:

本機能を有効にすると、デュアルバンドをサポートする無線端末は優先的に 5GHz 無線にアクセスします

ロードバランス:

本機能を有効にすると、施設内の AP が連携してアクセス端末の負荷を分散します

ローミングナビ:

本機能を有効にすると、AP は端末と連携して端末を誘導し、端末のシームレスなローミングを実現します

5 GHz無線ロードバランス:

本機能を有効にした後、5GHzラジオに接続している端末数が 40 台に達し、他の 5GHzラジオに接続している端末数を10台以上超えると、現在の5GHz無線SSIDはすぐに非表示になります。上記の条件のいずれかが満たされない場合にSSIDを再表示する

Broadcast Optimization :

ブロードキャストの最適化を有効にすると、AP がダウンリンクからブロードキャストまたはマルチキャスト パケットを受信すると、AP は ARP ブロードキャストおよび NS パケットにローカルで応答し、DHCP ブロードキャスト要求、RS パケット、および DHCPv6 ブロードキャスト パケットを破棄します。受信した IPv4 および IPv6 の基本ブロードキャストおよびマルチキャスト パケットは、通常どおり処理されます。

Broadcast Control :

ブロードキャスト制御を有効にすると、AP は受信したすべてのブロードキャストおよびマルチキャスト パケットを破棄します。同時にブロードキャストの最適化を有効にする必要があります。


詳細設定の  をクリックすると詳細設定項目が現れます。

図14 詳細設定の構成



設定項目	オープン	閉じる
弱い信号の拒否 ?	<input type="radio"/>	<input checked="" type="radio"/>
Channel Reuse-2.4GHz ?	<input type="radio"/>	<input checked="" type="radio"/>
Channel Reuse-5GHz ?	<input type="radio"/>	<input checked="" type="radio"/>
低レートを禁止にする-2.4GHz ?	<input type="radio"/>	<input checked="" type="radio"/>
低レートを禁止にする-5GHz ?	<input type="radio"/>	<input checked="" type="radio"/>
L3ローミング ?	<input type="radio"/>	<input checked="" type="radio"/>
無線プローブ ?	<input type="radio"/>	<input checked="" type="radio"/>

弱い信号の拒否 :

本機能を有効にした後、無線クライアントの信号強度が閾値を下回った場合、アクセスが禁止されます

Channel Reuse-2.4GHz :

この機能を有効にすると、APはノイズフロアを感知する能力を調整します。これにより、

複数のAPが5GHzの同じチャネルを使用する場合のチャネル使用率が向上します。設定値が小さい程、APがノイズフロアを感知する能力が弱くなります

Channel Reuse-2.4GHz :

この機能を有効にすると、APはノイズフロアを感知する能力を調整します。これにより、複数のAPが2.4GHzの同じチャネルを使用する場合のチャネル使用率が向上します。設定値が小さい程、APがノイズフロアを感知する能力が弱くなります

低レートを禁止にする-2.4GHz :

本機能を有効にすると、APは2.4Gに設定されたレートより低いレートの使用を禁止します

低レートを禁止にする-5 GHz :

本機能を有効にすると、APは5Gに設定されたレートより低いレートの使用を禁止します

L3ローミング :

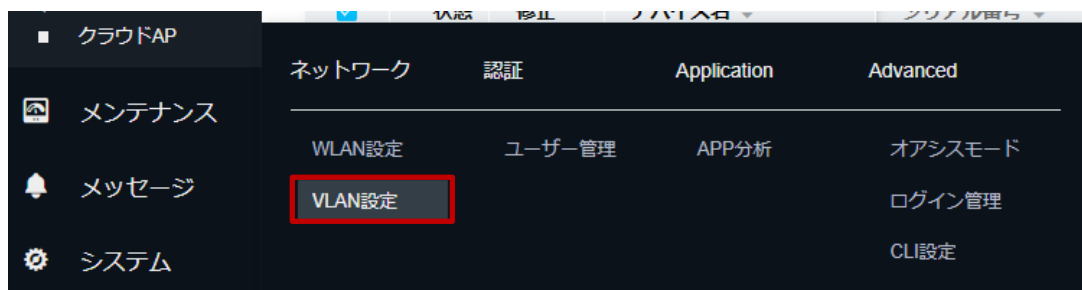
本機能を有効にすると、同一サイト内のAPが連携してアクセス端末でローミング操作を実行し、最大31のAP(異機種が混在していても可能。例えばWA6320-JPとWA6638-JP間でローミング)をサポートします

無線プローブ :

本機能を有効にすると、デバイスは無線パケットを監視して周囲の無線環境を検出します。

SSIDに関連付けされたVLANの作成

1. 設定 > クラウドAP > WLAN設定 > VLAN設定タブをクリックするとVLAN作成メニューが現れます。



2. 必要に応じて、作成するVLANのIDを指定します。

User Isolation: オープン(有効)にすると同一VLAN内の他のユーザーとの通信が行えないように設定します。

Forwarding MAC Address: User Isolationをオープンにしたときに、同一VLAN上にアクセスする必要のあるサーバー、プリンターなどの装置がある場合、ここで登録したMACアドレスの装置へはアクセスできるようになります。

図15 VLANの作成

* VLAN ID: 3

Description: sales.vlan

User Isolation (?): オープン クローズ

Forwardable MAC Address (?): + Add 削除

① MAC address/MAC address mask rule: Both Supported formats: AA-cc-bB-67-e3-00, AA:cc:bB:67:e3:00. The MAC address cannot be a broadcast or mcast address.

MAC Address

確定 キャンセル

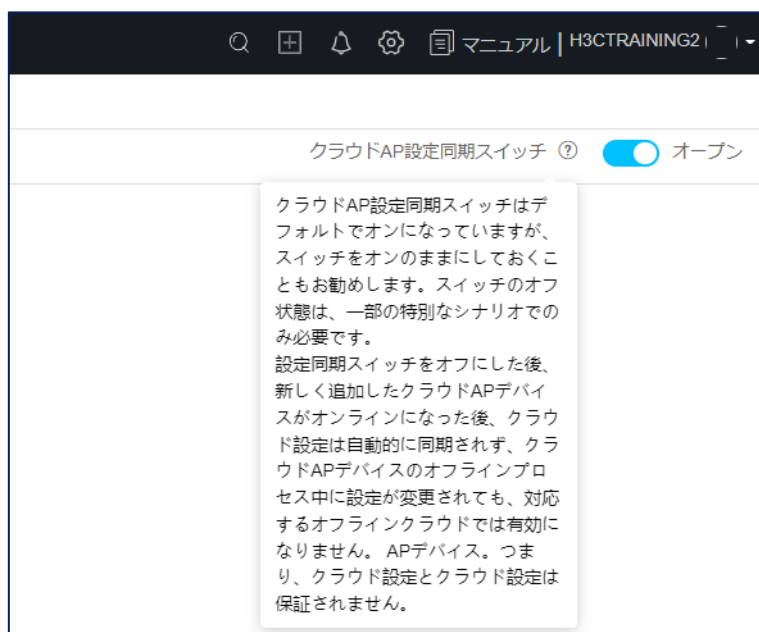
クラウド管理されたコンフィグのローカルAPとの同期

CloudAPIはクラウド上の設定メニューによりコンフィグを行います。このコンフィグはローカルAPへ同期されます。この同期はデフォルトで有効になっております。

1. トップナビゲーションバーで、**ネットワーク**をクリックします。
2. 左側のナビゲーションペインで、**設定 > クラウドAP > WLAN設定**を選択します。
3. 画面右上に**クラウドAP設定同期スイッチ**があり、デフォルトで有効になっております。

このスイッチをクローズに変更するとクラウド上での設定変更はローカルAPIには反映されないため、**クラウドとローカルの設定の不整合が生じる可能性があります。**

あえてクローズで使うシナリオとしては、Cloudで設定できない項目をローカルAPで設定したい場合には、**Cloudの設定がローカルAPIに上書きされてローカルAPで設定した項目が消えないようにする**場合となります。



ワイヤレス認証の設定

クラウド管理APIは、ワンタッチインターネット認証のみをサポートします。ワンタッチインターネット認証では、認証サーバーがMACアドレスでクライアントを認証します。ワンタッチインターネット認証は、監査や運用の要件が低いシナリオに適用でき、ユーザーは認証時にクライアントに広告をプッシュできます。

注意: 802.1X認証とポータル認証を同時に有効にすると802.1x認証に合格したのち、ポータル認証が現れますので、どちらか一方を有効にしてください。

基本認証設定の構成

1. トップナビゲーションバーでサービス > クライアント認証をクリックします。
2. 認証テンプレートフィールド+追加をクリックします。
3. カスタム, レストラン, ホテルのテンプレートから1つを選んでクリックします。
4. テンプレート名を設定して、応用をクリックします。



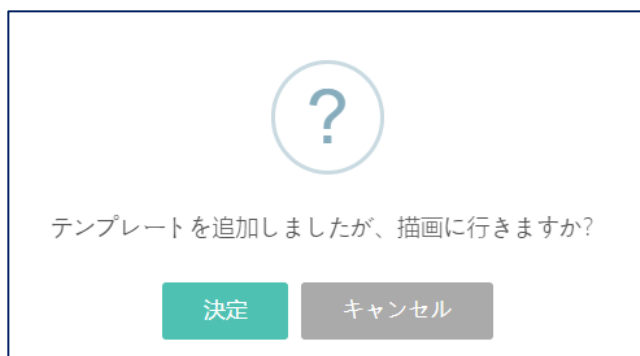
テンプレート情報

テンプレート名 * (1-32文字)

説明 (1-128文字)

応用 キャンセル

5. 決定をクリックします。



?

テンプレートを追加しましたが、描画に行きますか?

決定 キャンセル

6. ログインタブで認証設定メニューを展開し、必要に応じて基本的な認証設定を行います。設定したら完了をクリックして、確認をクリックすると有効になります。

図14 モバイル端末ページの基本認証設定の構成

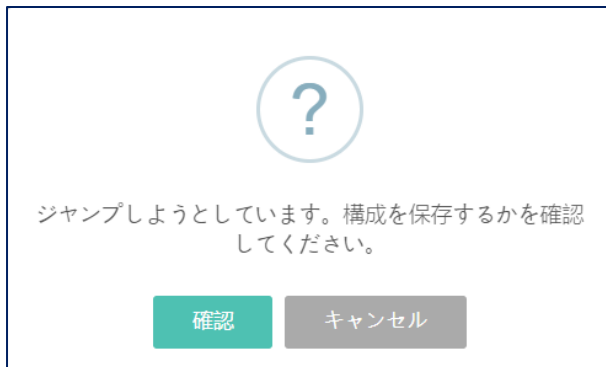


ログイン成功後に移行するページ(ホームページ)の設定





7. PC端末認証用のページを用意するには**PC端末ページをカスタマイズする**タブをクリックします。確認を求めてきますので**確認**をクリックします。



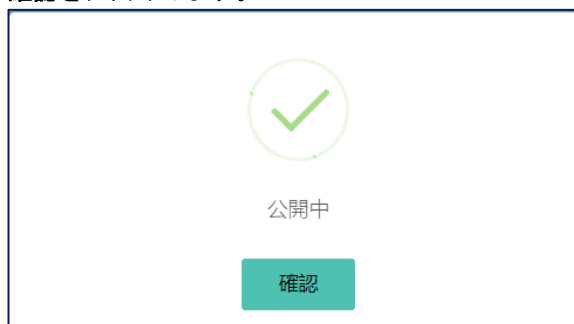
8. PC端末認証用のページに移動したら**PC端末認証をオンにする**をクリックして**ON**にします。そしてlogo、テキスト、バックグラウンド、左側エリアなどをカスタマイズできます。良ければ、**完了**をクリックします。



ログイン成功後に移行するページ(ホームページ)の設定



確認をクリックします。



高度な認証設定の構成

1. ログインタブで、**高度な構成**メニューを展開します。
2. インターネットアクセスの**アクセス制限**タブで、次の機能を設定します。
 - **1日のインターネット接続時間**
 - **毎日のインターネット接続時間**
 - **登録プロセスはHTTPSを有効にするか**: ランディングページとログインページにHTTPSを使用して、ネットワークセキュリティを強化します。
 - **PCのインターネット接続を許可するか**: ワイヤレスNICを搭載したラップトップおよびデスクトップがWLANIにアクセスできるようにします。

図15 高度な構成

認証設定
✕

認証方式
高級な構成

Xiaobeiルートは、次のような高度な設定をサポートしていません: 1回のインターネット接続時間、毎日のインターネット接続時間、アイドル時トラフィックのカットオフ、アイドル時カットオフ時間; ダム端末認証は高度な設定をサポートしていません、設定する必要はありません

インターネットのアクセス制限
認証なし
インターネット利用時間制限

1回のインターネット 接続時間 !

(0以上かつ1日のオンライン時間 分以下)、0以上かつ毎日のインターネット 接続時間以内の整数を入力してください

毎日のインターネット 接続時間 !

(1回のインターネット 接続時間より長く、かつ1440分より小さい)

登録プロセスはHTTPSを有効にする

PCのインターネット 接続を許可するか

完了

再アソシエーションのための認証なしの設定

1. 認証なしタブをクリックします。
2. 認証なし機能を有効にします。この機能を使用すると、クライアントがオフラインになり、指定された認証なし期間内にオンラインになった場合に、再認証なしでオンラインになることができます。

図16 再アソシエーションのための認証なしの設定

認証設定
✕

認証方式
高級な構成

Xiaobeiルートは、次のような高度な設定をサポートしていません: 1回のインターネット接続時間、毎日のインターネット接続時間、アイドル時トラフィックのカットオフ、アイドル時カットオフ時間; ダム端末認証は高度な設定をサポートしていません、設定する必要はありません

インターネットのアクセス制限
認証なし
インターネット利用時間制限

再度接続認証を免除する !

転送ページ

認証なし期間中 ! (1-355日)

開始時間 ! 初回認証 最終認証

完了

インターネットアクセスコントロールの設定

1. インターネット利用時間制限タブをクリックします。
2. インターネットアクセスコントロールを有効にします。
3. クライアントがインターネットにアクセスできる時間範囲を指定します。

開始時刻または終了時刻フィールドの各値は、24時間のタイムクロックを表します。時間範囲の終了時刻が開始時刻より後であることを確認してください。

終了時刻フィールドの値00は、24 p.m.を表します。00~00の時間範囲を指定すると、その範囲によって1日全体が定義されます。

1日に複数の時間範囲を追加するには、プラスアイコン+をクリックします。

図17 インターネットアクセス制御の設定

認証設定

認証方式
高級な構成

Xiaobeiルートは、次のような高度な設定をサポートしていません: 1回のインターネット接続時間、毎日のインターネット接続時間、アイドル時トラフィックのカットオフ、アイドル時カットオフ時間; ダム端末認証は高度な設定をサポートしていません、設定する必要はありません

インターネットのアクセス制限 認証なし インターネット利用時間制限

インターネット接続時間制限 ON

曜日	有効期間
月曜日	00 から 00 - +
火曜日	00 から 00 - +
水曜日	00 から 00 - +
木曜日	00 から 00 - +
金曜日	00 から 00 - +
土曜日	00 から 00 - +
日曜日	00 から 00 - +

完了

クラウド管理されたAPのモニタリング

クラウド管理APの統計情報サマリーの表示

1. トップナビゲーションバーで、**ネットワーク**をクリックします。
2. 左側のナビゲーションペインで、**モニタリング > クラウドAP > ダッシュボード**を選択します。
3. 作業領域の左上隅からターゲットのブランチおよびサイトを選択します。開いたページには、次の情報が表示されます。
 - **AP統計**: 合計AP数量、オンラインAP数量、およびオフラインAP数量を表示します。
 - **総フローの多いトップ5 AP**: 当日のダウンロードおよびアップリンクトラフィックが最も多い5つのAPを表示します。
 - **オンライン端末の多いトップ5 AP**: 当日のオンラインエンドポイント数が最も多い5つのAPを表示します。
 - **アラーム数の多いトップ5 AP**: サイト内でアラームが最も多い5つのAPを表示します。

図19 APの概要



クラウド管理APリストの表示

1. トップナビゲーションバーで、**ネットワーク**をクリックします。
2. 左側のナビゲーションペインで、**モニタリング > クラウドAP > APリスト**を選択します。
3. 作業ペインの左上隅からターゲットのブランチとサイトを選択します。
4. +/- 表示する列をカスタマイズするには、アイコンをクリックします。
5. リストを更新するには、**リフレッシュ**をクリックします。
6. APの名前をクリックすると、その情報が表示されます。
 - **状態**: 当日の基本的なAP情報、CPUとメモリーの使用状況、アップリンクとダウンロードのトラフィックを表示します。
 - **イベント**: APの動作ログとアラームを表示します。
 - **端末**: 当日のクライアント関連付けと、最新の統計収集期間に収集されたオンラインクライアント情報を表示します。**クライアント情報は5分ごとに収集されます**。クライアントの詳細情報を表示するには、Online Client InfoリストでクライアントのMACアドレスをクリックします。

図20 APと端末の情報

APリスト>FIT AP

状態 イベント 端末 ツール

基本情報

- 名: FIT AP
- AP 型番: WA6638
- オンライン状態: オンライン
- オンラインユーザ数: 1
- ローカルIP: 10.10.11.70
- シリアル番号: 219801A24F8201E0000J
- バージョン: Release 2454P01
- 運転時間: 05h07m52s
- メモリ使用率: 63%
- グローバルIP: 123.220.233.36

チャンネル情報

2.4GHz-1			5GHz-1		
チャンネル	チャンネル利用率	電力	チャンネル	チャンネル利用率	電力
1	28%	15dBm	36	5%	18dBm

CPU メモリトレンド

APリスト>FIT AP

状態 イベント 端末 ツール

操作ログ

	アカウント	IPアドレス	説明
✓	H3CTRaining2	123.220.233.36	save config: shopName-tokyo, devSN-219801A24F8201E0000J
✓	H3CTRaining2	123.220.233.36	Edit Oasis Mode: Site name - tokyo, SN-219801A24F8201E0000J, enable Oasis mode for an AP to act as an C
✓	H3CTRaining2	123.220.233.36	Oasis mode : Site name - tokyo, SN - 219801A24F8201E0000J, result - success
✓	H3CTRaining2	123.220.233.36	Add a device. Site: tokyo, device alias: FIT AP, device SN: 219801A24F8201E0000J, IRF device: No.
✓	H3CTRaining2	123.220.233.36	Delete a device. Site: tokyo, device SN: 219801A24F8201E0000J.

第 1 ~ 5 エントリーを表示する(総計 5 エントリー)

警報情報

アラーム深刻度	警報時間	状態	解除時間	警報タイプ	警報内容
● 注意	2022-06-23 18:28:00	解除されました	2022-06-24 09:21:33	Device offline	The device CLOUDAP of tokyo sit platform for more than 10 minutes
● ヒント	2022-06-24 10:00:57	解除されていません	-	Upgrade	The device CLOUDAP of tokyo si 7.1.064, Release 2454P01

APリスト>FIT AP

状態 | イベント | **端末** | ツール

オンライン端末トレンド ②

オンライン端末情報 ②

MAC	IP	ユーザ名	認証方式	メーカー	無線帯域	SSID
c8e2-6535-5d0e	10.10.11.34	-	Portal	PC	5GHz	CLOUDAP

第 1 ~ 1 エントリーを表示する(総計 1 エントリー)

7. AP名を変更するには、このページの上部にある編集アイコン をクリックします。

図21 クラウド管理されたAPリストの表示

APリスト

リフレッシュ | エクスポート | スクリーニング

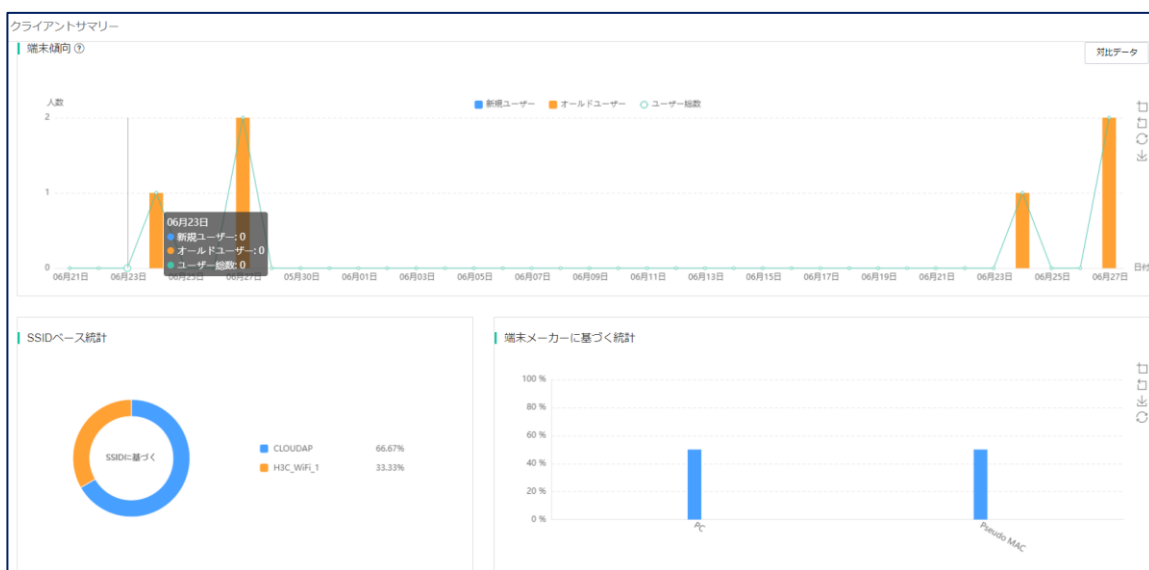
状態	APシリアル番号	AP名	MAC	ローカルIP	グローバルIP	型番	バージョン	稼働時間	端末	操作
オンライン	219801A24F8201E0000J	CLOUDAP	010-903e-f7e0	10.10.11.63	123.220.233.36	WA6638	Release 2454P01	03h10m27s	1	編集

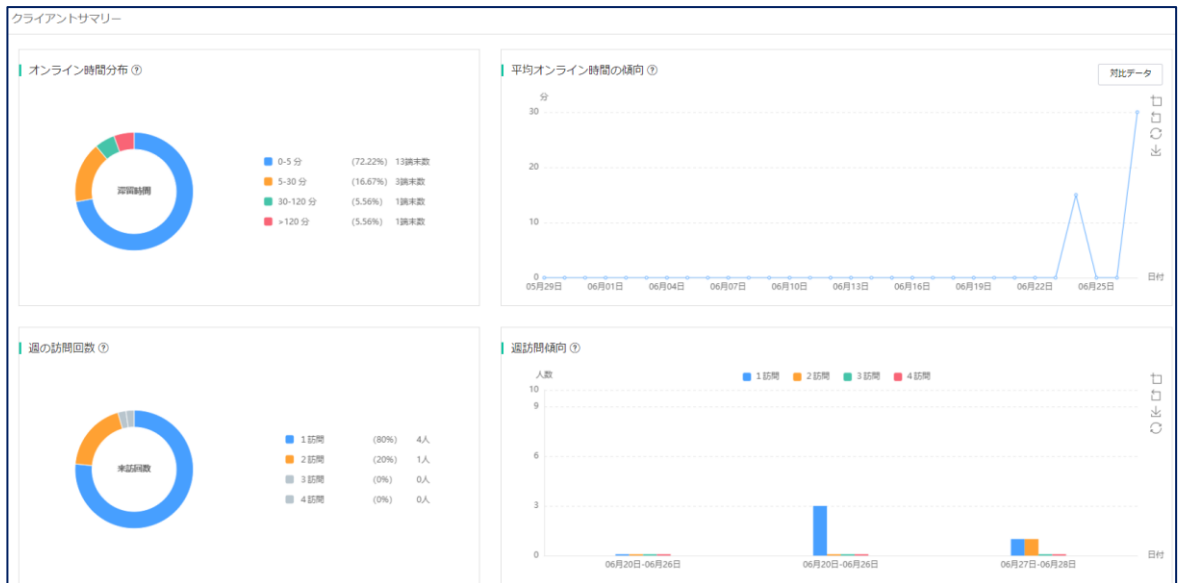
第 1 ~ 1 エントリーを表示する(総計 1 エントリー)

トップ頁 | 前頁 | 次頁 | 末页 | 10

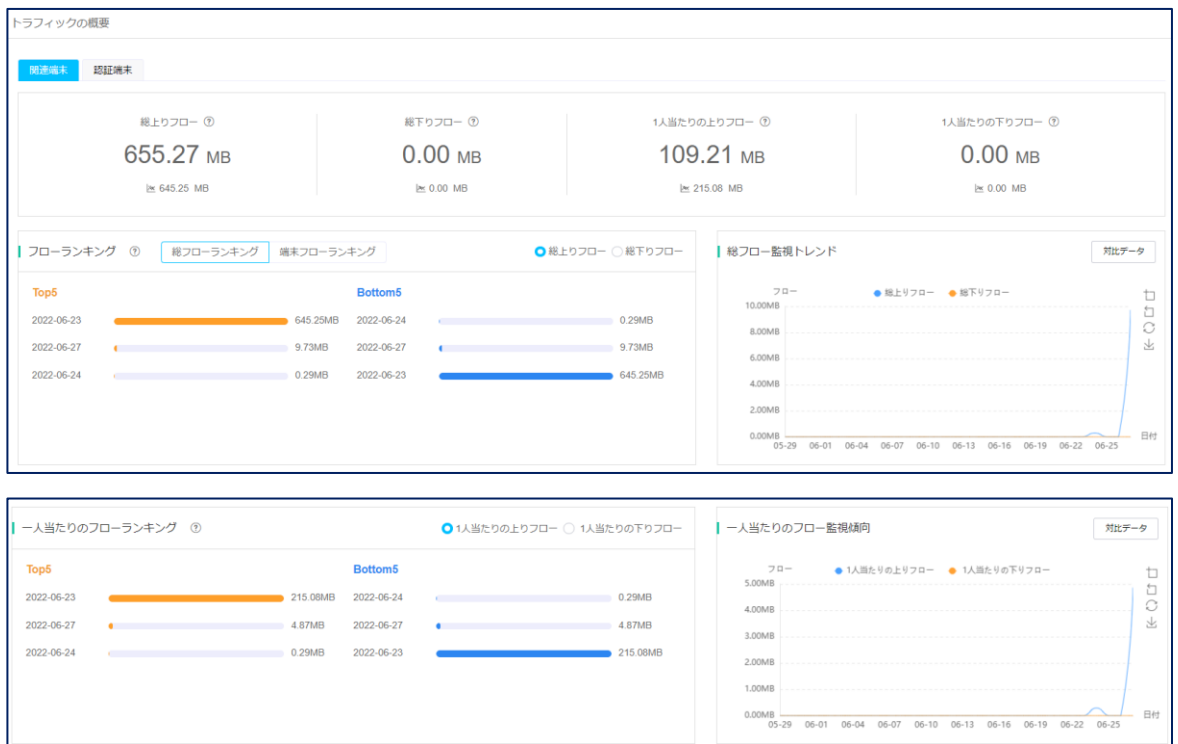
詳細なクライアント情報の表示(ネットワーク)

1. トップナビゲーションバーで、ネットワークをクリックします。
2. 左側のナビゲーションペインでネットワーク > クライアント > 端末統計 > クライアントサマリーを選択します。
3. 作業ウィンドウの左上隅からターゲットのブランチおよびサイトを選択します。開いたページには、サイト内のクライアントに関する詳細情報が表示されます。





4. 左側のナビゲーションペインでネットワーク > クライアント > 端末統計 > トラフィックの概要を選択します。
5. 作業ウィンドウの左上隅からターゲットのブランチおよびサイトを選択します。開いたページには、サイト内のトラフィックに関する詳細情報が表示されます。

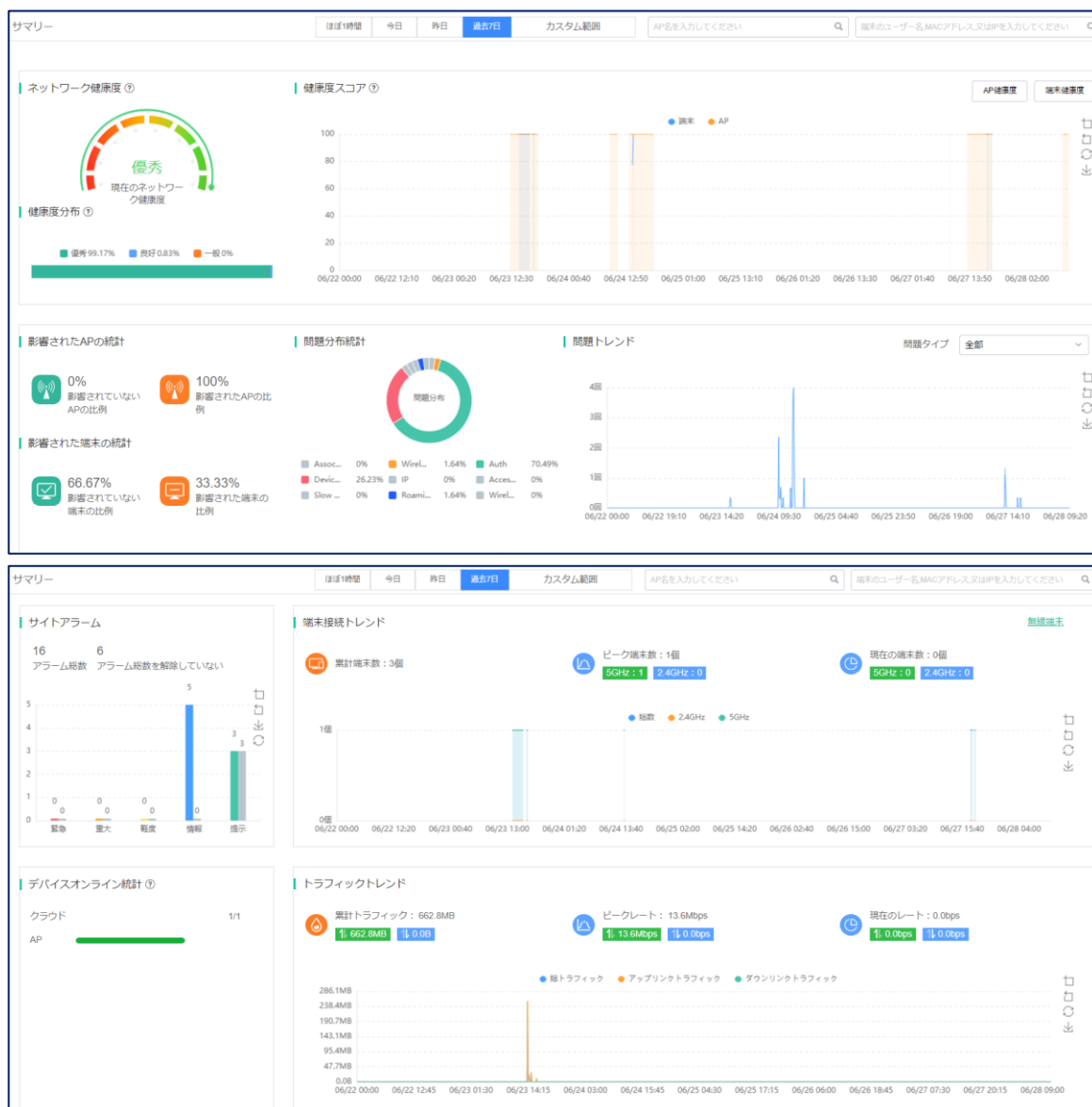


第二部 スマートO&M

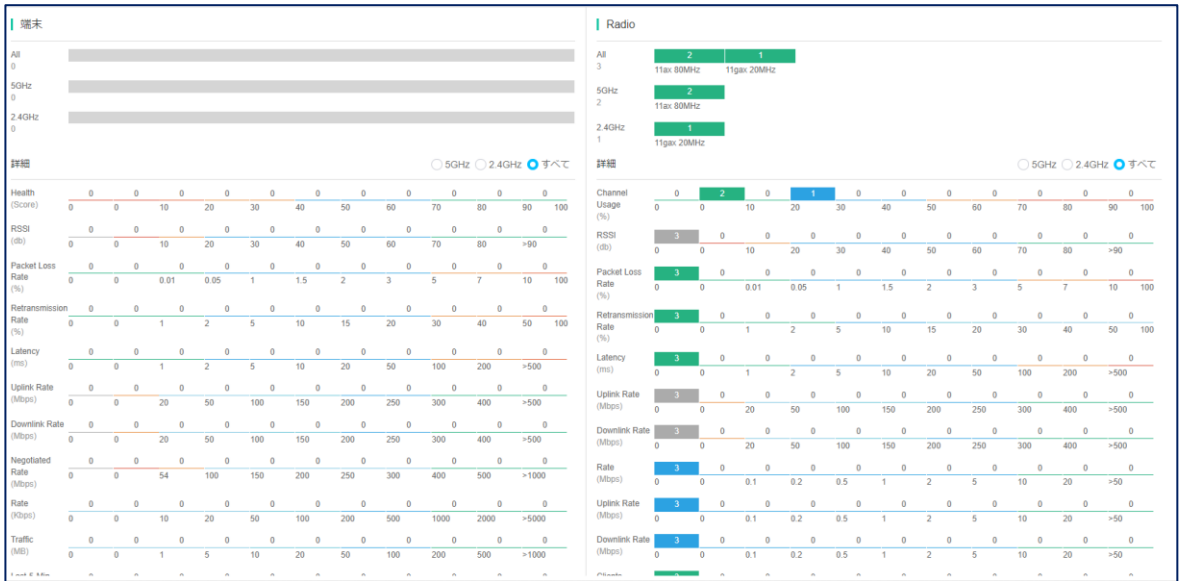
スマートO&Mは登録されたCloudAP及びCloudAPに接続されたクライアントの情報を過去7日間に渡って確認できます。

ダッシュボード

1. トップナビゲーションバーで、スマートO&Mをクリックします。
2. 左側のナビゲーションペインでダッシュボード > サマリーを選択します。ここではネットワークの健康度を見ることができます。



3. 左側のナビゲーションペインで**接続性**を選択します。ここでは2.4GHz、5GHzのチャンネルの利用状況を見ることができます。



問題>問題分析

1. トップナビゲーションバーで、**スマートO&M > 問題 > 問題分析**をクリックします。
2. **問題のカテゴリアイコン**をクリックします。

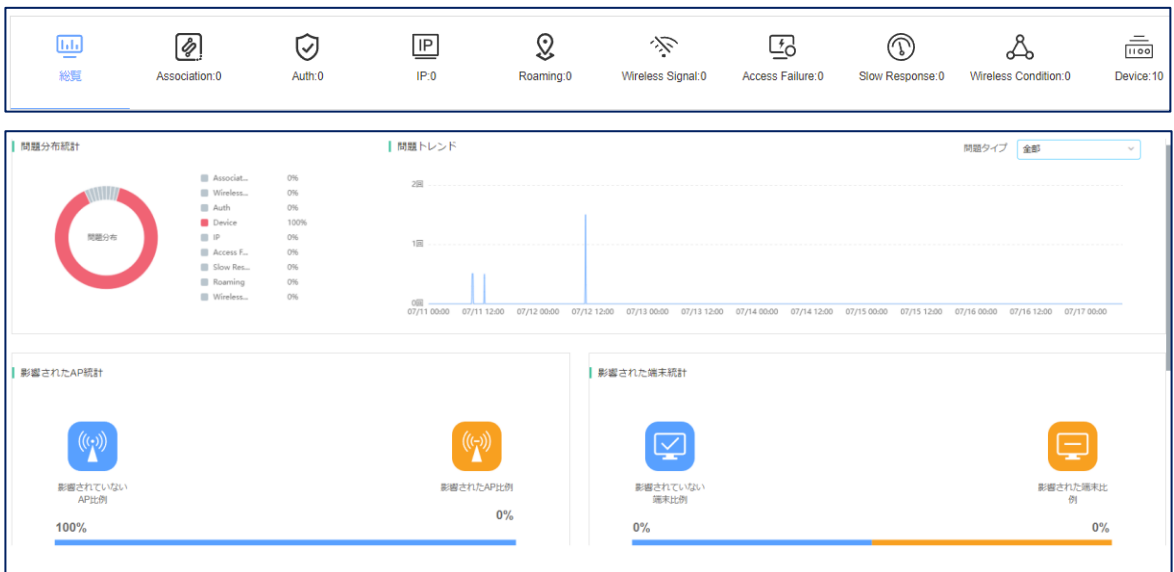


表1 問題のカテゴリと課題

カテゴリ	課題
関連付け	アクセスが遅い
	関連付けの失敗
	5Gが優先でない
	アクセスの異常
	802.1X認証の失敗

認証	802.1X認証パケット交換失敗
	低速802.1X認証
	低速MAC認証
	MAC認証の失敗
	MAC認証パケット交換失敗
	ポータル認証の失敗
IPアドレス	IP取得失敗
	IP取得タイムアウト
	IP取得が遅い
ローミング	ピンポン移動
	ローミングスティッキ性
無線信号	プール信号強度
アクセスエラー	不十分な無線リソース
反応が遅い	リンクレートが低い
	低いネゴシエーションレート
ワイヤレス状態	クライアントが多すぎる
	重大な干渉
	チャンネル使用率が高い
	高ブロードキャストおよびマルチキャスト伝送
	高ドロップレート
	高い再送信率
デバイス	APオフライン
	デバイスがオフライン
	CPU使用率が高い
	メモリー使用率が高い
	高い順方向CPU使用率

問題>アラーム

1. トップナビゲーションバーで、**スマートO&M > 問題 > アラーム**をクリックします。
2. **警報購読**タブを選択します。
3. **+追加**をクリックして、障害情報の対象となるエリア、メールの送り先を指定します。メールの送り先の登録は前のテーマの「**ネットワークトラフィックの日報、週報のメール通知**」と同様です。

メールは以下のような形式で送信されます：

差出人: cloudnet@oasisinfo.h3c.com

日時: 2022年7月19日 10:31:09 JST

宛先: abc.def@ghi.com

件名: Cloud platform-Alarm

Cloud platform-Alarm The device CLOUDAP of tokyo site has been restarted by H3C_TRAINING account at 09:31:02

* 名: fatal error

説明: only send fatal information

エリア ? : オープン クローズ

* 警報方式: メール警報

(説明: システムは毎日同じ場所に対して発生した警告を50通の警告メールに送ります; 全部の場所に対して発生した警告は全部の受信者に1000通の警告メールを送ります。特定の条件では制限値を超える可能性があります)

* 送り時間: 月曜日から金曜日まで 土曜日 日曜日

00:00 まで 23:59

* メンテナンスウィンドウ: クローズ


* Info sync ? : クローズ


* 警報アカウント:

アカウント	件数
<input type="checkbox"/> オプション警報アカウント	5
<input type="checkbox"/> SUBMAINTENANCE (test5@gmail.com)	
<input type="checkbox"/> SUBOPERATION (test1@gmail.com)	
<input type="checkbox"/> SUBWATCHER (test2@gmail.com)	
<input type="checkbox"/> SUBDEMO (test3@gmail.com)	
<input type="checkbox"/> SUBONFIG (test4@gmail.com)	

アカウント	件数
<input type="checkbox"/> 警告アカウントが選択されました	1
<input checked="" type="checkbox"/> H3CTRaining2 (training@h3c.com)	

4. 画面をスクロールダウンして、警報の対象となる場所、障害の程度などを指定します。

警報分類	<input type="checkbox"/> 警報タイプ	警告レベル	トリガーアラームの説明
<input checked="" type="checkbox"/>  Device state ^	<input checked="" type="checkbox"/> CPU Usage	注意	デバイスの平均CPU使用率が10分以内に超過 <input type="text" value="85"/> % (75-100の整数,デ
	<input checked="" type="checkbox"/> Memory Usage	注意	デバイスメモリの平均利用率が10分以内に超過 <input type="text" value="85"/> % (75-100の整数,デ
	<input checked="" type="checkbox"/> AP bulk dropped	重大	シングルまたは複数のAPを超えた場合,その前の <input type="text" value="0"/> 分以内にドロップ します ①
	<input checked="" type="checkbox"/> AP frequent dropped	注意	An AP dropped more than 5 times in 24 hours yesterday
	<input checked="" type="checkbox"/> Device offline	注意	Device offline from cloud platform for more than 10 minutes / 24 hours
	<input checked="" type="checkbox"/> Device frequently offline	重大	Device offline from cloud platform more than 7 times within 10 minutes
	<input checked="" type="checkbox"/> AP batch online	ヒント	シングルまたは複数のAPを超えた場合,その前の <input type="text" value="0"/> 分以内出現上線 (0
	<input checked="" type="checkbox"/> Port UP/DOWN	注意	Device port status changed
	<input checked="" type="checkbox"/> Port PoE	注意	Port PoE function status changed
	<input checked="" type="checkbox"/> IP Address Conflict	重大	IP address conflicts were detected on a switch interface
	<input checked="" type="checkbox"/> EoGRE Tunnel Interface Up/D own	ヒント	EoGRE Tunnel Interface State Change
	<input checked="" type="checkbox"/> Optical Transceiver Anti-Fake	注意	Transceiver is suspected to be a counterfeit/pirated/unauthorized H3C transceiver.

<input checked="" type="checkbox"/>  Device operation ^	<input checked="" type="checkbox"/> Device upgraded successfully	ヒント	Device upgraded successfully
	<input checked="" type="checkbox"/> Device upgraded failed	重大	Device upgraded failed
	<input checked="" type="checkbox"/> Device restart	注意	Device restart
	<input checked="" type="checkbox"/> Device unbinding	注意	Device unbound from the CLI

<input checked="" type="checkbox"/>	High forwarding CPU utilization	注意	The device's CPU usage is high because it forwards too many data packets
<input checked="" type="checkbox"/>	Broadcast multicast ratio is too high	ヒント	Broadcast / multicast messages take up too much channel resources
<input checked="" type="checkbox"/>	Excessive wired port traffic	ヒント	Excessive traffic on the physical interface
<input checked="" type="checkbox"/>	Device temperature alarm	ヒント	Device temperature abnormality detected
<input checked="" type="checkbox"/>	RF does not start	注意	RF is off
<input checked="" type="checkbox"/>	High noise floor	注意	AP noise floor is too high
<input checked="" type="checkbox"/>	Message congestion	注意	Message congestion
<input checked="" type="checkbox"/>	Channel radar avoidance	ヒント	The RF working channel has detected a radar and has evaded
<input checked="" type="checkbox"/>	Wired port receiving error packets continue to grow	ヒント	Continuously receiving error packets on the physical interface of the AP
<input checked="" type="checkbox"/>	AP wired port is Down	注意	AP physical interface status is set to DOWN
<input checked="" type="checkbox"/>	Wired port negotiation rate is low	ヒント	AP physical interface negotiation rate is low <input type="checkbox"/> Enable Periodic S
<input checked="" type="checkbox"/>	Wired port receiving resources are insufficient	ヒント	The AP physical interface peer sends packets too fast
<input checked="" type="checkbox"/>	Wired ports continue to send wrong packets	ヒント	The physical interface of the AP continues to send out error messages
<input checked="" type="checkbox"/>	Wired ports negotiate half-duplex	ヒント	AP physical interface duplex mode negotiation is half duplex
<input checked="" type="checkbox"/>	AP temperature alarm	注意	AP temperature abnormality detected
<input checked="" type="checkbox"/>	Insufficient sending resources	注意	Insufficient sending resources
<input checked="" type="checkbox"/>	Beacon frame sending failed	注意	Beacon frame sending failed
<input checked="" type="checkbox"/>	Beacon frame resource is insufficient	注意	Beacon frame resource is insufficient
<input checked="" type="checkbox"/>	Data message sending failed	注意	Data message sending failed
<input checked="" type="checkbox"/>	Insufficient message resources	注意	Insufficient message resources



Smart O&M



<input checked="" type="checkbox"/>	WAN port uplink bandwidth alarm	ヒント	WANポート上りブロードバンド検査、10分以内の上りブロードバンドピークは警報値	50	M (1-1000の整数で、デフォルトは50)
<input checked="" type="checkbox"/>	WAN port downlink bandwidth alarm	ヒント	WANポート下りブロードバンド検査、10分以内の下りブロードバンドピークが警報値	50	M (1-1000の整数で、デフォルトは50)
<input checked="" type="checkbox"/>	Large deviation in flow ratio in and out direction	ヒント	The proportion of the outgoing and incoming traffic of the device exceeds the preset th		
<input checked="" type="checkbox"/>	High 2.4GHz channel usage	注意	AP 2.4 GHz無線周波数リアルタイムチャンネル利用率を超えています	60	(は60)
<input checked="" type="checkbox"/>	High 5GHz channel usage	注意	AP 5 GHz無線周波数リアルタイムチャンネル利用率を超えています	60	0)
<input checked="" type="checkbox"/>	Too many clients on 2.4 GHz radios	注意	AP 2.4 GHz無線周波数リアルタイムアクセス端末数がを超えています	20	20)
<input checked="" type="checkbox"/>	Too many clients on 5 GHz radios	注意	AP 5 GHz無線周波数リアルタイムアクセス端末数がを超えています	40	0) ;
<input checked="" type="checkbox"/>	WAN port connectivity	重大	WAN口の接続性を検出し、パケットロス率は連続10分以内でお超える	10	10)
<input checked="" type="checkbox"/>	Loop detected on switch port	重大	Loop detected on switch port		
<input checked="" type="checkbox"/>	Too much Tx broadcast or multicast traffic	重大	Broadcast or multicast transmission rate exceeds	100	in the statistics collec
<input checked="" type="checkbox"/>	IRF split	重大	IRF split		
<input checked="" type="checkbox"/>	STP discarding detected on switch port	重大	STP discarding detected on switch port		
<input checked="" type="checkbox"/>	Fault Reports	<input checked="" type="checkbox"/> Add Fault Report	重大	A new fault report was submitted and needs processing	
		<input checked="" type="checkbox"/> Fault Report State Change	ヒント	The state of a fault report changed	

クライアント>無線端末

CloudAPIに接続したクライアントの情報を過去7日間に渡って表示できます。

1. トップナビゲーションバーで、**スマートO&M > クライアント > 無線端末 > 健康**をクリックします。
2. **表示範囲**を選択します。データは過去7日間が保持されていて、その間の特定の範囲はカスタム範囲で指定できます。

今日	昨日	過去7日	カスタム範囲
----	----	------	--------

図 表示範囲の指定

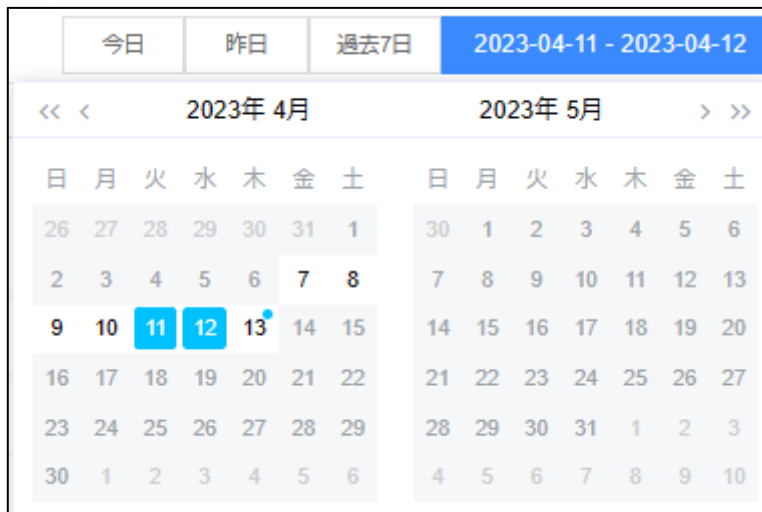
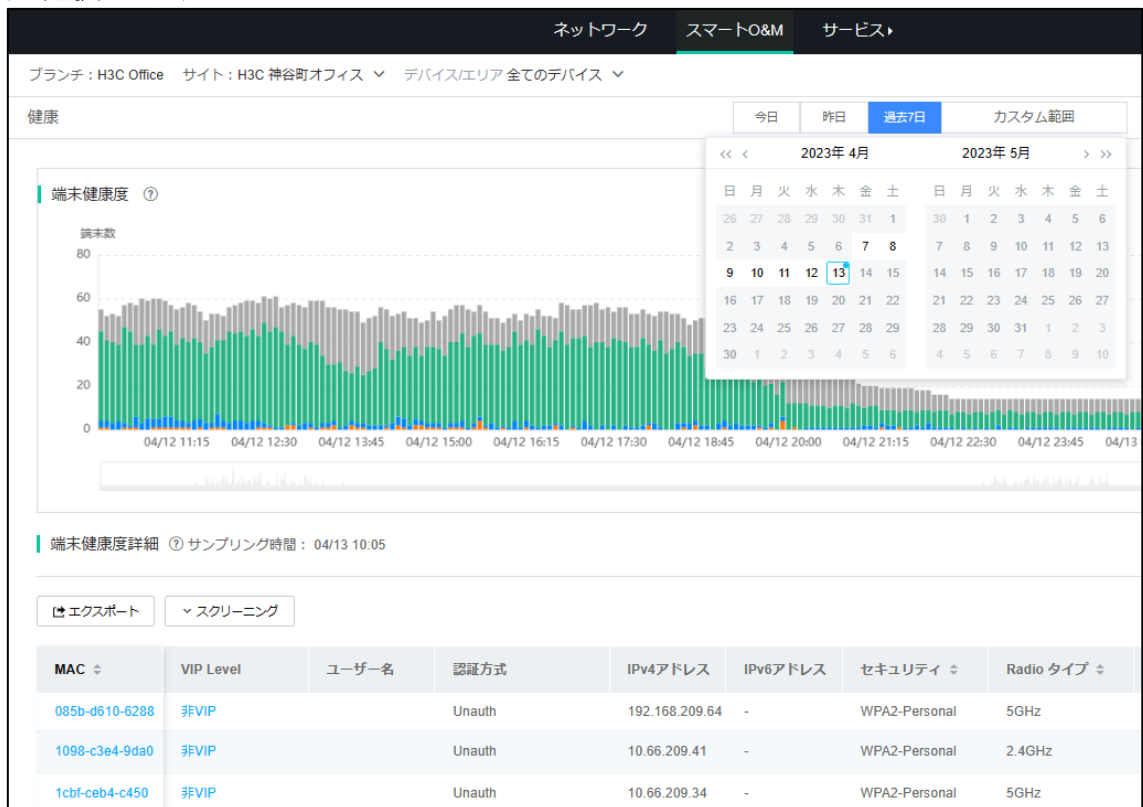


図 選択したクライアントデータ



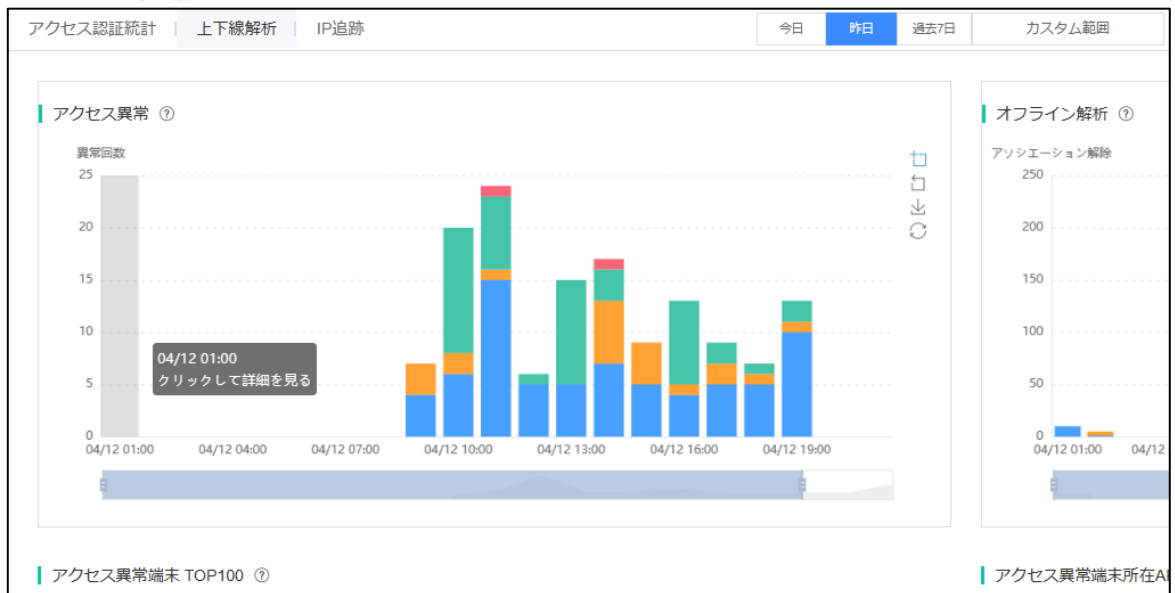
3. トップナビゲーションバーで、スマートO&M > クライアント > 無線端末 > オンラインリストをクリックします。

図 オンラインリスト

MAC	ユーザー名	認証方式	セキュリティ	レート	上り流量	アップリンクARP	上りレート	下り流量
f4a4-753f-7a32		Unauth	WPA2-Personal	47.0Kbps	890.7KB	13	24.3Kbps	831.2KB
3032-35ad-f69c		Unauth	WPA2-Personal	3.4Kbps	103.8KB	58	2.8Kbps	20.1KB
389d-92ff-ac5a		Unauth	WPA2-Personal	5.8Kbps	133.3KB	49	3.6Kbps	78.7KB
f4d1-08b8-c5d6		Unauth	WPA2-Personal	34.3Kbps	366.5KB	6	10.0Kbps	889.4KB
8c45-00dd-bb8d		Unauth	WPA2-Personal	2.3Kbps	53.7KB	2	1.5Kbps	31.9KB
1098-c3e4-9da0		Unauth	WPA2-Personal	0.3Kbps	11.6KB	1	0.3Kbps	1.4KB
4c1d-963c-3d63		Unauth	WPA2-Personal	123.8Kbps	3.1MB	7	87.4Kbps	1.3MB

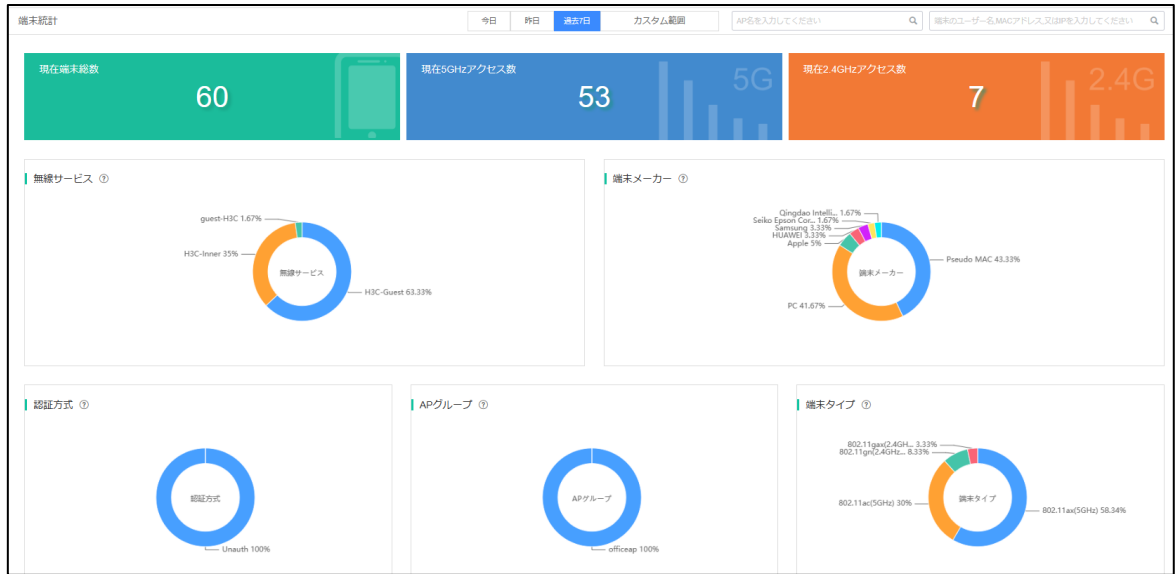
4. トップナビゲーションバーで、スマートO&M > クライアント > 無線端末 > アクセス分析をクリックします。

図 アクセス分析



5. トップナビゲーションバーで、スマートO&M > クライアント > 無線端末 > 端末統計をクリックします。

図 端末統計



ネットワーク>AP

CloudAP自身の情報を過去7日間に渡って表示できます。

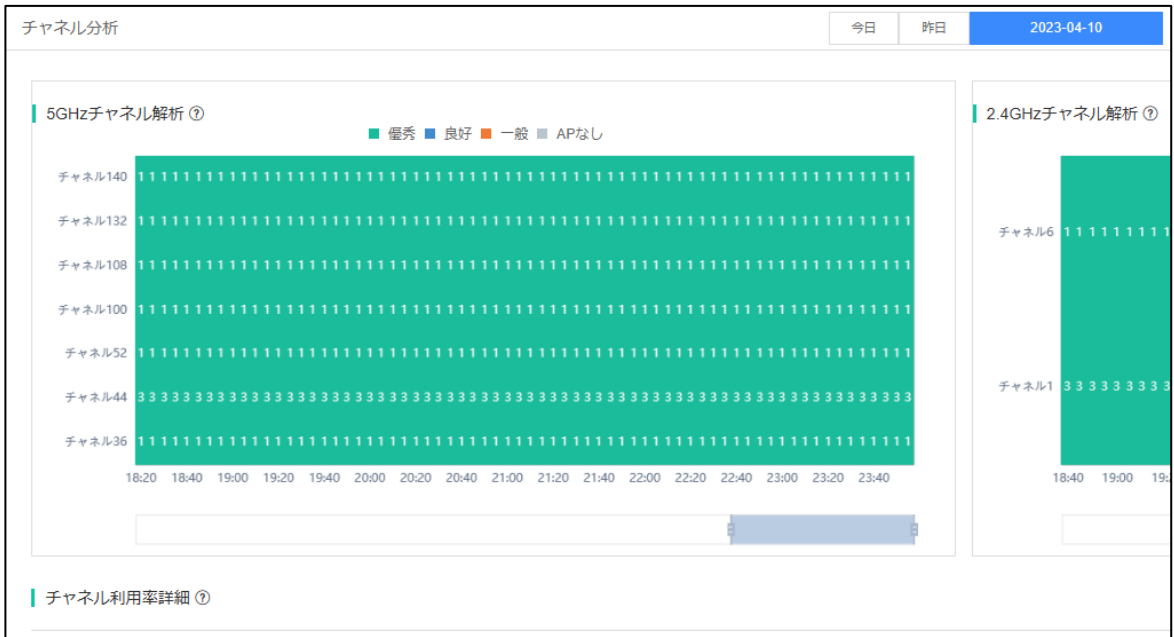
1. トップナビゲーションバーで、スマートO&M > ネットワーク > AP > 健康をクリックします。

図 APの健康状態



2. トップナビゲーションバーで、スマートO&M > ネットワーク > AP > チャンネル分析をクリックします。

図 チャンネル分析



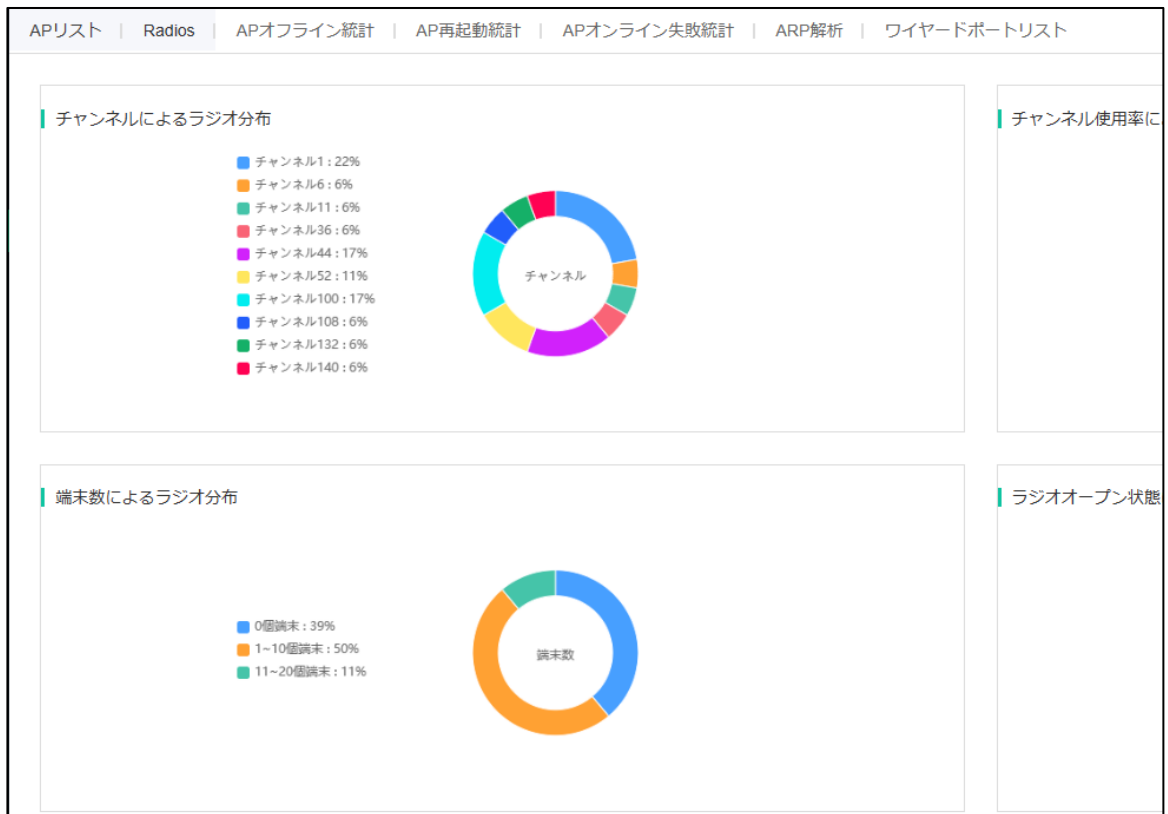
3. トップナビゲーションバーで、スマートO&M > ネットワーク > AP > AP統計をクリックします。



図 APリスト



☒ Radios



応用(アプリケーション)>応用統計

CloudAPIにアクセスするクライアントが利用しているアプリケーションの統計情報を表示できます。

1. トップナビゲーションバーで、**スマートO&M > 応用 > 応用統計**をクリックします。

図 応用統計



2. トップナビゲーションバーで、スマートO&M > 応用 > 応用分析をクリックします。

図 応用統計分析



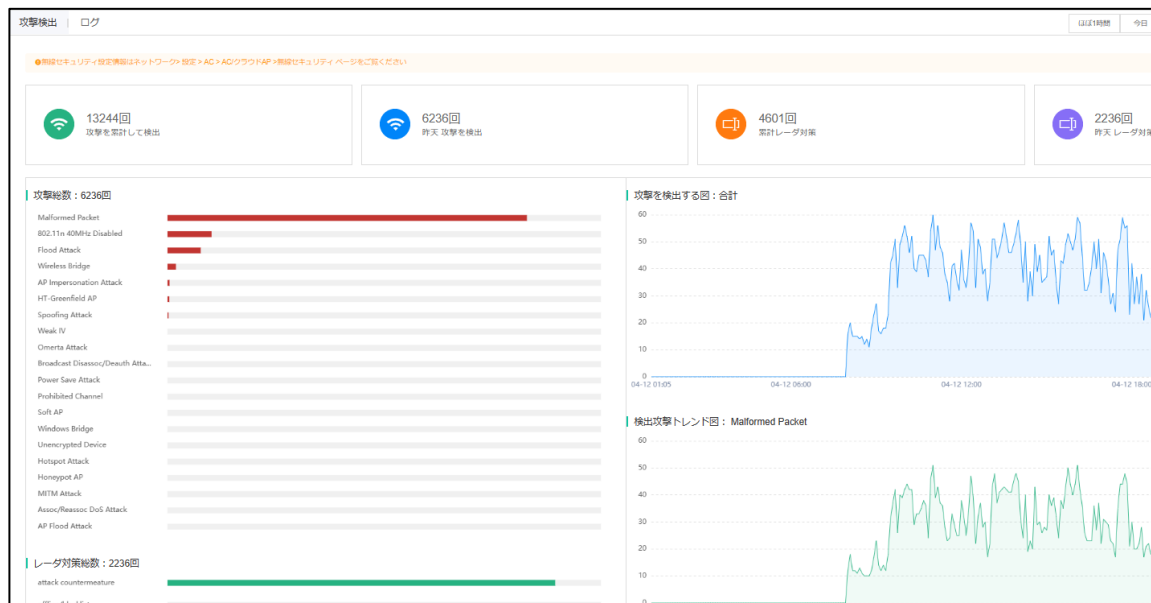
セキュリティ>攻撃検知

CloudAPIに対する侵入攻撃をWIPS機能で検知、対策した結果を過去7日間に渡って表示できます。

※無線セキュリティ設定情報はネットワーク>設定>AC>AC/クラウドAP>無線セキュリティ ページをご覧ください

1. トップナビゲーションバーで、スマートO&M > セキュリティ> 攻撃検知をクリックします。

図 APの攻撃検知の状況



2. トップナビゲーションバーで、スマートO&M > セキュリティ> SSID検知をクリックします。

図 APのSSIDへの攻撃検知の状況

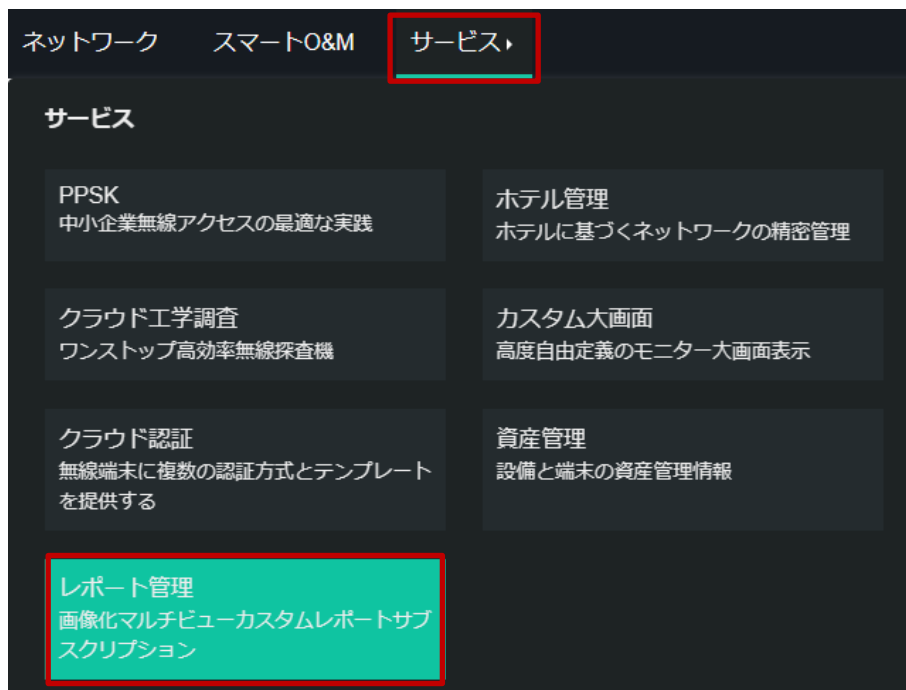


第三部 サービス

CloudAPIに接続したクライアントの情報を過去7日間に渡って表示できます。

サービス>レポート管理

1. トップナビゲーションバーで、サービス > Report Managementをクリックします。



2. 追加をクリックします。



3. 必要な情報を入力して**セーブ**をクリックします。

* レポート名:	<input type="text" value="CLOUDAP_Weekly"/>
* サイト名:	<input type="text" value="tokyo"/>
レポートタイプ:	<input type="text" value="Network O&M"/>
プッシュサイクル:	<input type="text" value="週ごとに押して送り"/> ?
レポートフォーマット:	<input type="text" value="PDF"/> レポートプレビュー
アカウントを押して送ります:	<input type="button" value="+ メールボックス追加"/> <input type="text" value="koshiro X"/>
備考:	<input type="text" value="1~255文字"/>
	<input type="button" value="セーブ"/> <input type="button" value="キャンセル"/>

4. レポートの送り先のメールアドレスは、予め登録しておきます。
トップナビゲーションバーで、**サービス > Users**を選択して**+追加**をクリックします。

Cloudnet
ネットワーク スマートO&M **サービス**


O&M Reports
Users

ブランチ: TRAINING サイト: tokyo

Users

メールボックス設定 ?

5. レポートの送り先のメールアドレスは、予め登録しておきます。
トップナビゲーションバーで、サービス > Usersを選択して+追加をクリックします。



The screenshot shows a dialog box titled "新規設定" (New Setting) with a close button (X) in the top right corner. The dialog contains three input fields:

- A text input field labeled "* アカウント名:" (Account Name) containing the text "CLOUDAPSTS".
- A text input field labeled "* メールボックスアドレス:" (Mailbox Address) containing the text "test2@gmail.com".
- A text area labeled "備考:" (Remarks) containing the text "report mail address".

At the bottom right of the dialog, there are two buttons: "確定" (Confirm) and "キャンセル" (Cancel). The "確定" button is highlighted with a red border.

6. 必要な項目を入力して**確定**をクリックします。
このアドレスが有効になるには、登録アドレス宛に確認のメールが届き、そこにあるリンクをクリックすることで有効になります。

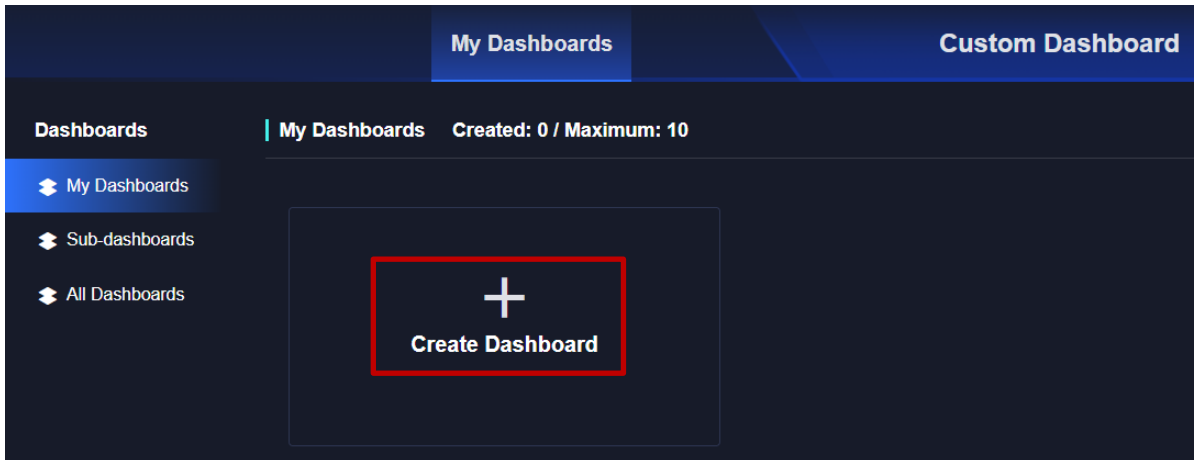
サービス>カスタム大画面

カスタムダッシュボードサービスを使用すると、ネットワーク画面にネットワーク統計グラフを追加して、ネットワークの状態、問題の分布、APの数量、APの負荷統計、クライアントアクセスの傾向、クライアント/トラフィックの傾向、およびアラームの内容などの最新のネットワーク情報を表示できます。




各アカウントは最大10のダッシュボードを作成でき、親アカウントはサブアカウントによって作成されたダッシュボードを表示できます。



1. トップナビゲーションバーで、サービス > カスタム大画面を選択します。My Dashboardsページが表示されます。

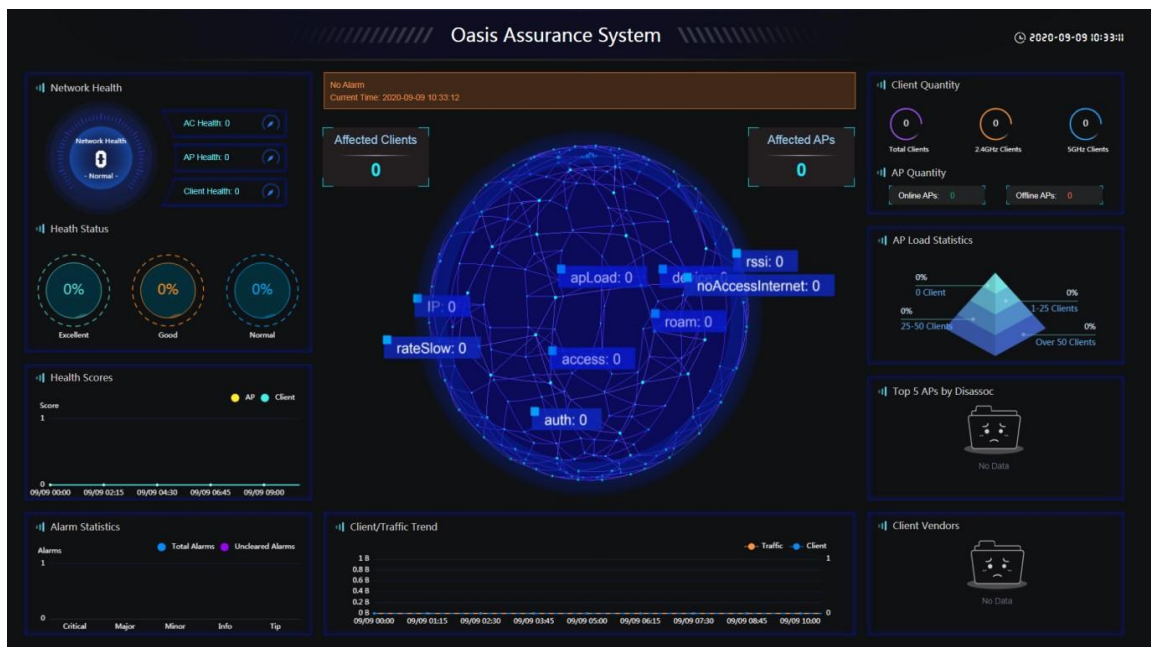


2. **Create Dashboard**をクリックします。
3. Assurance template、empty template又はCommercial templateを選択し、**Create Dashboard**をクリックします。
4. ダッシュボードの名前を指定し、**OK**をクリックします。

ダッシュボードのカスタマイズページが開きます。このページには、タイル領域、サービス領域、ダッシュボード領域、ダッシュボード/タイル設定領域が左から右に表示され、上部にツールバーが表示されます。
5. ダッシュボードにタイルを追加します。Services、text、picture、time、assistantなど、さまざまな種類のタイルを使用して、カスタムコンテンツをダッシュボードに配置できます。
6. **Tile**領域でタイルを管理します。
 - タイルの表示順序を調整するには、タイルを選択してからアクションを選択します。最上部のタイルは、ダッシュボードの最初に表示されます。
 - タイルを表示または非表示にするには、タイルの左側にあるアイコンをクリックします。
 - タイルのデータソースを表示するには、タイルをクリックします。
 - ダッシュボードからタイルを削除するには、タイルを選択し、アイコンをクリックします。
7. ダッシュボード領域でレイアウトを管理します。
 - タイルのサイズを変更するには、タイルをクリックし、マウスポインタをハンドルの1つに移動してからマウスをドラッグします。
 - タイルの位置を調整するには、タイルを選択し、キーボードの矢印キーを押します。
 - 表示順序を調整したり、ダッシュボードからタイルを削除したりするには、タイルを右クリックしてアクションを選択します。
 - 垂直または水平のガイドを作成するには、ルーラーをクリックします。
 - ガイドを目的の位置に移動するには、ガイドをドラッグします。
 - ガイドを削除するには、ガイドをダブルクリックします。
 - ガイドの表示と非表示を切り替えるには、左上隅の定規の交点にあるアイコンをクリックします。
8. ダッシュボード設定を構成するには、ダッシュボードの空白領域をクリックします。**Dashboard Settings**領域がページの右側に表示されます。設定は、ダッシュボード上のすべてのタイルに適用されます。

- **Style**タブでは、ダッシュボードのテーマ、タイトルスタイル、タイトルタイトル、背景画像、およびダッシュボードカバーを構成できます。 .jpg、.png、および.jpegファイルのみがサポートされており、ファイルサイズは2MBを超えることはできません。
 - 期間や更新間隔などのデータソース設定を構成するには、**Data**タブをクリックします。ダッシュボードのすべてのタイトルの既定の設定に戻すには、**Restore Default Settings**をクリックします。
9. タイルの設定を構成するには、**Tile**または**Dashboard**領域でタイトルをクリックします。**Tile Settings**領域がページの右側に表示されます。
- **Style**タブでは、選択したタイトルに応じて、タイトルのタイトル名、タイトルの配置、フォントサイズ、タイトルの位置、タイトルの表示スタイルを調整できます。
 - **Data**タブでは、選択したタイトルに応じて、デバイスの選択、期間の設定、更新間隔の設定を行うことができます。
10. ダッシュボードをプレビューするには、ダッシュボードにタイトルを配置した後、右上隅にある**Save & Preview**をクリックします。

ダッシュボードを全画面モードで表示するには、使用するオペレーティングシステムまたはブラウザに応じて、キーボードのショートカットキー(F11など)を押します。



サービス>資産管理

資産タイプ(ルーター、スイッチ、AC,APなどのタイプ)、装置のシリアル番号、資産番号、資産状態(使用中、故障、未使用など)、EOL(製品のサポート終了日)、保証の終了日、登録されているサイト、資産のラベルなどを管理する**管理台帳機能**です。

例えば、予備品として倉庫に保管している装置の資産管理をする場合にも使えます。予備品ですからサイト情報は空白のまま登録します。サイトを指定すると、装置が倉庫にあつてネットワークにつないでいない状態でも、オフラインと認識されダッシュボードには故障とカウントされています。勿論、装置を倉庫から出してネットワークにつながるとこの資産はオンラインと表示され、以降オフラインになればダッシュボードには故障と表示されます。

1. トップナビゲーションバーで、サービス > 資産管理をクリックします。



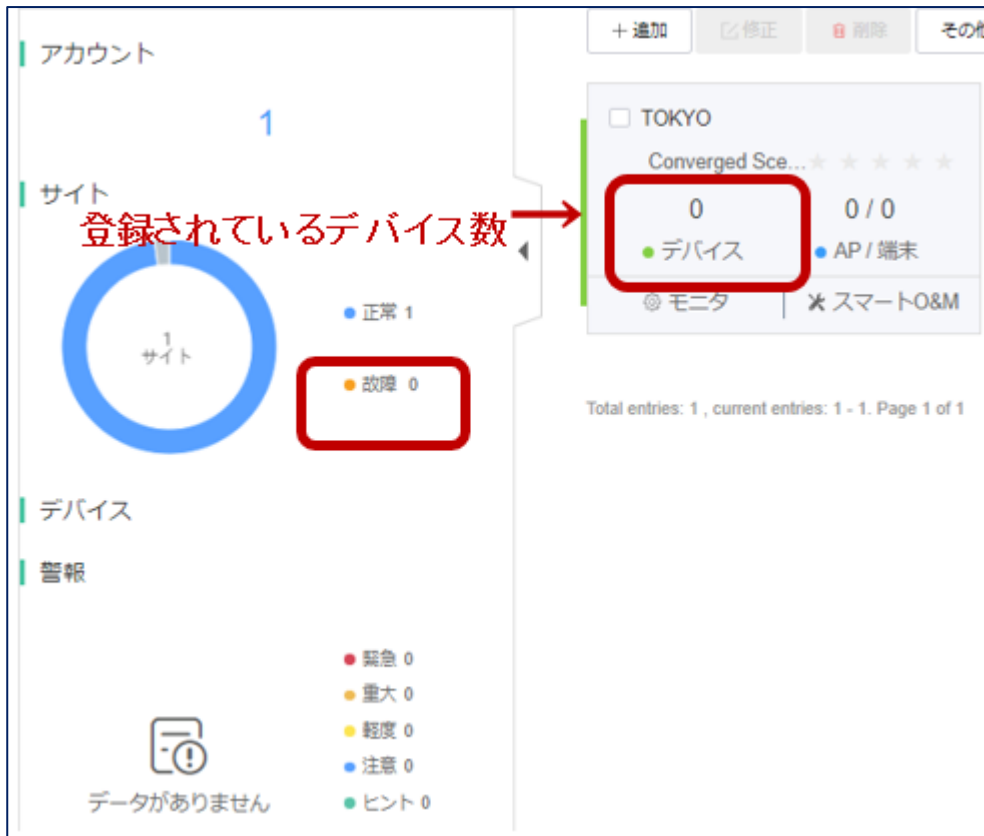
2. 資産管理タブを選択します。



ちなみに最終資産とはCloudnetに登録できないPCなどの端末装置をMACアドレスで管理する場合に利用いたします。

資産登録と装置登録の関係を説明いたします。

サイトを作成した直後の装置が何も登録されていない状態は以下のようになります。




3. **+追加**をクリックして、CloudAPを登録します。

Asset registration form with the following fields:

- 資産タイプ: Cloud AP
- 資産SN: 219801A24F8201E0000J
- 資産番号: 101
- 資産状態: Not In Use
- 停产时间: YYYY-MM-DD 应用到其型番下所有资产
- 停保时间: YYYY-MM-DD 应用到其型番下所有资产
- 所属サイト: サイトを選んでください **全て空欄にします**
- 資産ラベル: ラベルを選んでください (資産ラベルは最大3つまで指定)
- コメント: 100文字以内

Buttons: 確定 (Confirm), キャンセル (Cancel)

4.  オンライン状態を同期する をクリックして資産状況を更新します。所属サイトを空白のままにしておくと資産に登録してもオンライン状態はチェックされません。

資産番号	資産シリアル番号	所属サイト名	資産モデル	資産状態	資産ラベル	オンライン状態
101	219801A24F8201E0000J	-	WA6638	Not In Use	-	-

ダッシュボードにも登録された資産は“故障”にカウントされません



アカウント: 1

サイト: 1

デバイス: 1

● 正常 1

● 故障 0

登録されているデバイス数 → 0

0 / 0

● デバイス

● AP / 端末

● モニタ

● スマートO&M

Total entries: 1, current entries: 1 - 1. Page 1 of 1

5. 装置をオンラインにして、サイトに登録しました



云简网络 - Cloudnet -

クラウドAP

1

1

● オンラインデバイス数

● デバイス総数

デバイスリスト


デバイス情報

リフレッシュ 削除 再起動 クラウド接続をreset アップグレードバージョン

状態	デバイス名	シリアル番号	タイプ
●	CLOUDAP	219801A24F8201E0000J	Cloud AP

ダッシュボードには以下のように表示されます。



6.  オンライン状態を同期する をクリックして資産状況を更新します。

資産番号	資産シリアル番号	所属サイト名	資産モデル	資産状態	資産ラベル	オンライン状態
101	219801A24F8201E0000J	-	WA6638	Not In Use	-	オンライン

エントリーを表示する(総計 1 エントリー)

所属サイトは反映されないまま、かつ資産状態もNot In Useのままでもオンラインになったことが確認されました。操作欄で編集アイコンをクリックしてオンラインにしたサイトを選択し資産状態をIn Useに変更します。
この状態でこの装置に障害が発生してオフラインになるとダッシュボードには故障と表示されま



サイト情報は以下ようになります。

クラウドAP

0 オンラインデバイス数 1 デバイス総数

デバイスリスト

デバイス情報

リフレッシュ 削除 再起動 クラウド接続をreset アップグレードバージョン

状態	デバイス名	シリアル番号	タイプ
●	CLOUDAP	219801A24F8201E0000J	Cloud AP

Total entries: 1 , current entries: 1 - 1. Page 1 of 1

7. オンライン状態を同期する をクリックして資産状況を更新します。装置の状態がオフラインと認識されたことが確認されました。

資産番号	資産シリアル番号	所属サイト名	資産モデル	資産状態	資産ラベル	オンライン状態
101	219801A24F8201E0000J	-	WA6638	Not In Use	-	オフライン

結論として、サイトを空白にして登録すると、装置がオンラインになるまでは、オンライン状態がチェックされないの、ネットワークに接続していない装置をあらかじめ資産として登録しても、ダッシュボード上には故障としてカウントされません。

- そして、装置がオンラインになった後、オンライン状態を同期する をクリックして資産状況を更新すると資産管理台帳にもオンライン状態反映されますので、資産管理台帳の編集ボタンでオンラインになったサイトの選択、使用状態をIn Useにします。

資産番号	資産シリアル番号	所属サイト名	資産モデル	資産状態	資産ラベル	オンライン状態
101	219801A24F8201E0000J	TOKYO	WA6638	In Use	-	オンライン

第四部 デバイスの保守

ファームウェアのアップグレード

この機能でアップグレードできるのはオンラインデバイスだけです。オフラインデバイスをアップグレードするには、イメージをローカルディレクトリにダウンロードし、デバイスをローカルにアップグレードします。イメージをダウンロードするには、図23を参照してください。

特定のデバイスのアップグレード

1. トップナビゲーションバーで、ネットワークをクリックします。
2. 左側のナビゲーションペインで、メンテナンス > ソフトウェアの更新を選択します。
3. 作業ペインの左上隅からターゲットの分岐とサイトを選択します。
4. デバイス別にアップグレードタブで、スクリーニングメニューを展開し、必要に応じてデバイスをフィルタします。
5. ターゲットデバイスを選択し、アップグレードをクリックします。

図22 特定のオンラインデバイスのアップグレード



The screenshot shows a web interface for software upgrades. At the top, it displays 'Branch: TRAINING' and 'Site: tokyo'. Below this, there are tabs for 'Software Upgrade' and 'Upgrade Details'. Under 'Upgrade Details', there are two sub-tabs: 'Upgrade by Device' (selected) and 'Upgrade by Model'. A 'Screening' dropdown menu is visible. Below the menu, there are two buttons: 'Upgrade Version' and 'Offline Download'. A table lists the devices available for upgrade.

<input type="checkbox"/>	状態	デバイス名	シリアル番号	型番	サイト	ブランチ	現在ソフトウェアバージョン
<input type="checkbox"/>	●	CLOUDAP	219801A24F8201E0000J	WA6638	tokyo	TRAINING	Release 2454P01

Total entries: 1, current entries: 1 - 1, Page 1 of 1

6. アップグレード方法を選択し、確定をクリックします。

図23 アップグレード方法の選択

確認メッセージ ×

● システムのアップグレードはデバイスを再起動し、再起動の過程で業務が中断され、非業務の忙しい時間帯にアップグレードすることを提案する

説明: 現在デバイスがアップグレードされている場合、このデバイスは今回のアップグレード操作を実行しません

アップグレードと再起動
 アップグレードし、設定を保存し、再起動する
 アップグレードのみ再起動しない (次回再起動後に有効になります)

確定
キャンセル

アップグレードの進捗状況は以下のように確認できます。

ソフトウェアアップグレード | アップグレード詳細

アップグレード中のデバイス:

デバイス名	シリアル番号	サイト	現在ソフトウェアバージョン	バージョンアップグレード進捗	アップグレード日時
CLOUDAP	219801A24F8201E0000J	tokyo	Version 7.1.064, ESS 2444P01	<div style="width: 31%; background-color: #007bff; height: 10px;"></div> 31%	2022-06-24 09:57:43

Total entries: 1, current entries: 1 - 1. Page 1 of 1

アップグレード済みデバイス:

デバイス名	シリアル番号	サイト	現在ソフトウェアバージョン	アップグレード状態	失敗原因	前回アップグレード日時
データなし						

特定モデルのデバイスのアップグレード

1. トップナビゲーションバーで、ネットワークをクリックします。
1. 左側のナビゲーションペインで、メンテナンス > ソフトウェアの更新を選択します。
2. 作業ペインの左上隅からターゲットの分岐とサイトを選択します。
3. 型番別にアップグレードタブをクリックし、スクリーニングメニューを展開して、必要に応じてデバイスをフィルタします。
4. 特定モデルのすべてのデバイスをアップグレードするには、次のタスクを実行します。
 - a. ターゲットデバイスのモデルを選択し、アップグレードをクリックします。

図24 特定モデルのオンラインデバイスのアップグレード

ブランチ: TRAINING | サイト: tokyo

ソフトウェアアップグレード | アップグレード詳細

デバイス別にアップグレード | 型番別にアップグレード

<input checked="" type="checkbox"/>	型番	デバイス数量	デバイスタイプ
<input checked="" type="checkbox"/>	WA6638	1	クラウドAP

Total entries: 1, current entries: 1 - 1. Page 1 of 1

- b. アップグレード方法を選択し、確定をクリックします。

図25 アップグレード方法の選択

The screenshot shows a dialog box titled "確認メッセージ" (Confirmation Message) with a close button (X) in the top right corner. The main text reads: "● システムのアップグレードはデバイスを再起動し、再起動の過程で業務が中断され、非業務の忙しい時間帯にアップグレードすることを提案する" (● System upgrade requires device restart, and business operations will be interrupted during the restart process, so we recommend upgrading during non-business busy hours). Below this is a note: "説明: 現在デバイスがアップグレードされている場合、このデバイスは今回のアップグレード操作を実行しません" (Note: If the device is currently being upgraded, this device will not be upgraded in this operation). There are three radio button options: "アップグレードと再起動" (Upgrade and restart), "アップグレードし、設定を保存し、再起動する" (Upgrade, save settings, and restart) - which is selected with a blue dot, and "アップグレードのみ再起動しない (次回再起動後に有効になります)" (Upgrade only, no restart (effective after next restart)). At the bottom right, there are two buttons: "確定" (Confirm) and "キャンセル" (Cancel).

5. デバイスモデルの特定のデバイスをアップグレードするには、モデルのデバイス数量リンクをクリックします。表示されるウィンドウでターゲットデバイスを選択し、**アップグレード**をクリックします。

アップグレードの詳細の表示

1. トップナビゲーションバーで、**ネットワーク**をクリックします。
2. 左側のナビゲーションペインで、**メンテナンス > ソフトウェアの更新**を選択します。
3. 作業ペインの左上隅からターゲットの分岐とサイトを選択します。
4. **アップグレード詳細**タブをクリックします。
 - **アップグレード中のデバイス**: 現在のバージョン、進行状況、およびアップグレード時刻情報が含まれます。
 - **アップグレード済デバイス**: 現在のバージョン、アップグレード状態、および障害理由情報が含まれています。

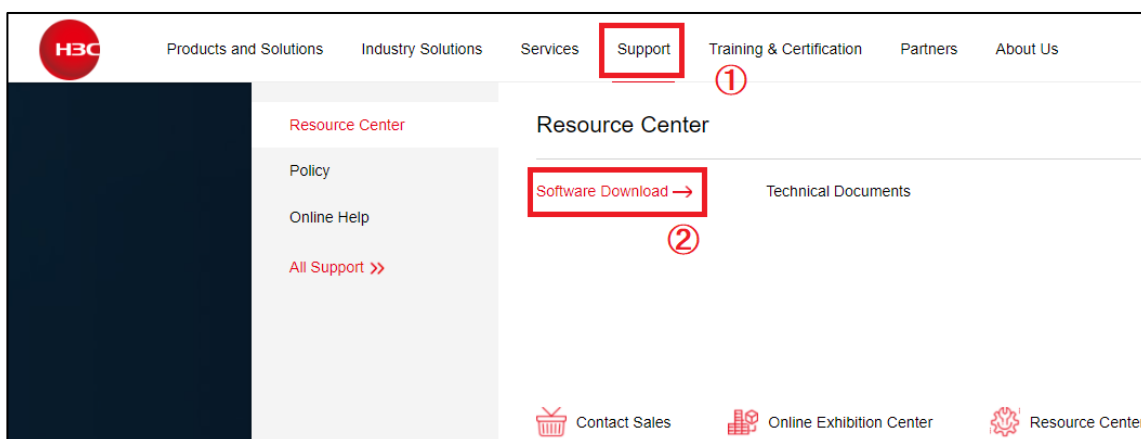
プライベートバージョンのアップロード

1. トップナビゲーションバーで、**ネットワーク**をクリックします。
2. 左側のナビゲーションペインで、**メンテナンス > ソフトウェアの更新**を選択します。
3. 作業ペインの左上隅からターゲットの分岐とサイトを選択します。
4. **アップグレード詳細**タブをクリックします。
 - **アップグレード中のデバイス**: 現在のバージョン、進行状況、およびアップグレード時刻情報が含まれます。
 - **アップグレード済デバイス**: 現在のバージョン、アップグレード状態、および障害理由情報が含まれています。

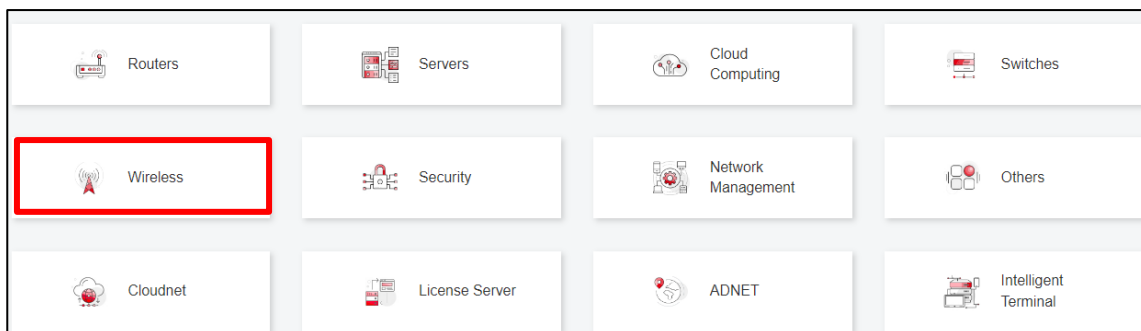
Cloudnet上にアップされたファームウェアが古い場合

Cloudnet上に最新のファームウェアがアップされているとは限りません。その場合、新しいファームウェアでのバージョンアップを希望される場合、弊社ソフトウェアのダウンロードサイトからダウンロードして頂き、Cloudnetを経由して装置にファームウェアをコピーした後、装置のCLIに入ってバージョンアップのコマンドを実行致します。

1. 弊社のダウンロードサイトへアクセスします。



2. 装置のタイプを選択します。



3. 装置のシリーズを選択します。



4. Downloadタブをクリックします。

装置によってはRecommendが提示されているバージョンがあります。このバージョンは最新ではありませんが、多くのお客様で安定して使われているバージョンですので、特に最新のバージョンの機能が必要な場合以外はRecommendのバージョンをお使いください。

WA6320			
	Title	Date	Downloads
→	WA6300-CMW710-R2459	07-11-2022	
→	WA6300-CMW710-R2457	08-08-2022	
→	WA6300-CMW710-R2453P01	12-04-2022	
→	WA6300-CMW710-R2444P01	30-06-2021	

5. ダウンロードにはアカウントが必要です。弊社パートナー様はアカウントをお持ちですので、パートナー以外のエンドユーザーの方は購入されたパートナー様から入手してください。

User **H3C Partner** H3C Employee

XXXXXXXXXX

.....

551F 5 5 1 F

Log In

[Forgot Password](#) [Partner Register](#) [User Register](#)

I agree to the use of my personal information according to the [H3C Privacy Statement](#). I understand that my personal information may be transferred for processing outside my country of residence.

I agree to the use of my contact data like email to keep me informed of products, services and offerings

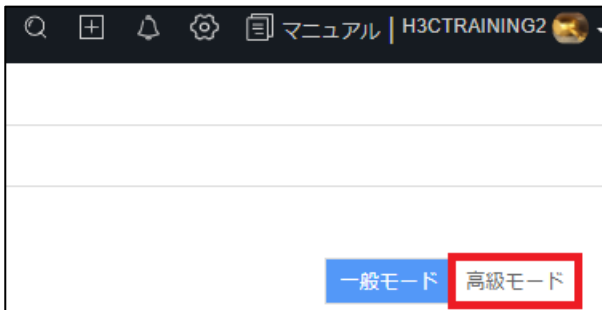
6. ファームウェアの圧縮ファイルはzip形式、またはrar形式で用意されております。また、当該バージョンで新規の機能や、解決されたバグなどの情報はリリースノートから確認できます。

Download	
Title	
WA6300-CMW710-R2459.zip	
WA6300-CMW710-R2459 Release Notes (Software Feature Changes).pdf	
WA63206300-CMW710-R2459 Release Notes.pdf	

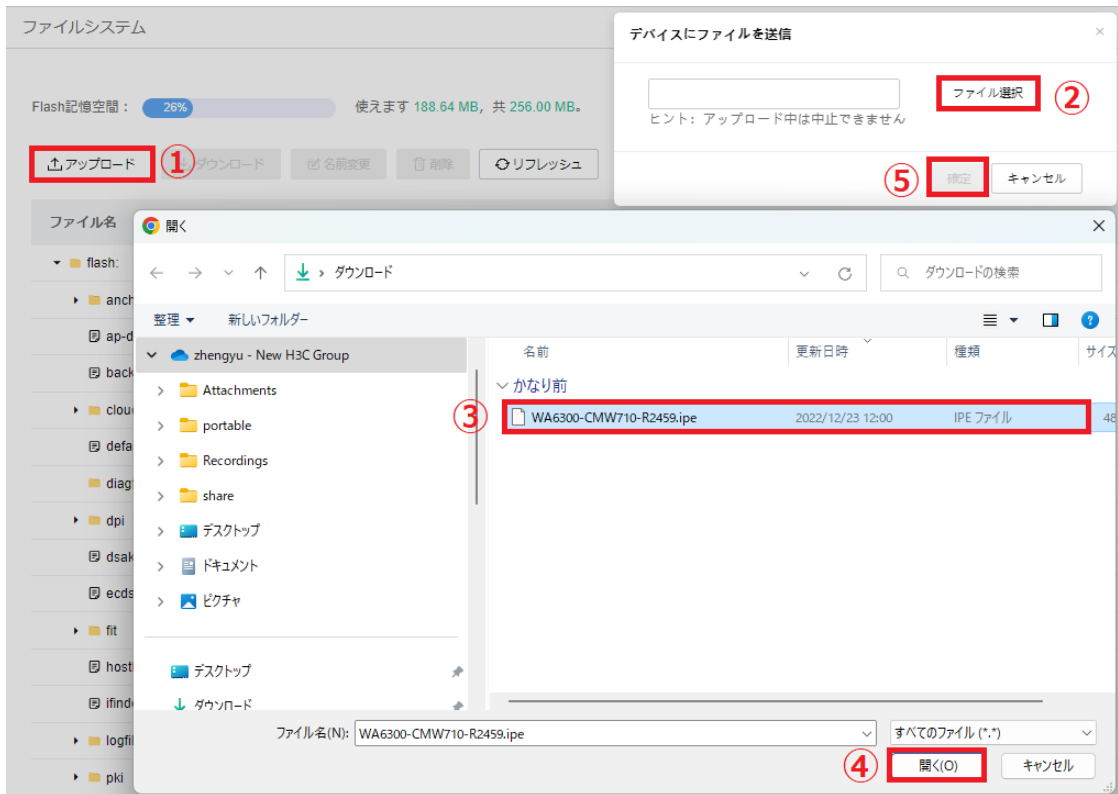
7. ダウンロードされたファームウェアをCloudnetを経由してAPへアップロードします。
 デバイスメニューから装置を選択するとファイルシステムのメニューにアクセスできるようになりますので、ここをクリックします。



8. 右上の高级模式を選択します。



9. アップロードをクリックしてアップロードするファイルを選択、そして確定をクリックします。
 Flash記憶容量の空きが25%程度と少ない場合、アップロード及びバージョンアップに失敗しますので、前のバージョンの.ipeファイルを削除(画面上からファイルを選択し削除ボタンで削除します)



10. アップロードしたファイルを使ってCLIでバージョンアップします。
 デバイスマニューから装置を選択しCLIヘルパーからCLIにアクセスします。



11. バージョンアップのコマンドを実行後、rebootコマンドでリブートさせます。リブートが完了すると新しいバージョンで稼働しております。

<WA6320-JP>**boot-loader file flash:/ファームウェアのファイル名 main**

Verifying the file flash:/ファームウェアのファイル名 on the device...Done.

H3C WA6320 images in IPE:

wa6300-boot.bin

wa6300-system.bin

wa6300-freeradius.bin

This command will set the main startup software images. Please do not reboot the device during the upgrade.
 Continue? [Y/N]:**y**

Add images to the device.

File flash:/wa6300-boot.bin already exists on the device.

File flash:/wa6300-system.bin already exists on the device.

File flash:/wa6300-freeradius.bin already exists on the device.

Overwrite the existing files? [Y/N]:**y**

Decompressing file wa6300-boot.bin to flash:/wa6300-boot.bin.....Done.

Decompressing file wa6300-system.bin to flash:/wa6300-system.bin.....Done.

Decompressing file wa6300-freeradius.bin to flash:/wa6300-freeradius.bin...Done.

Verifying the file flash:/wa6300-boot.bin on the device...Done.

Verifying the file flash:/wa6300-system.bin on the device.....Done.

Verifying the file flash:/wa6300-freeradius.bin on the device...Done.

The images that have passed all examinations will be used as the main startup software images at the next reboot on the device.

Decompression completed.

You are recommended to delete the .ipe file after you set startup software images for all slots.

Do you want to delete flash:/ファームウェアのファイル名 now? [Y/N]:**y**

<WA6320-JP>**reboot**

Start to check configuration with next startup configuration file, please wait.....DONE!

This command will reboot the device. Continue? [Y/N]:**y**

Now rebooting, please wait...

装置への操作

このタスクを実行して、オンラインデバイスを再起動したり、デバイス設定を保存したりできます。デバイスを操作するには:

1. トップナビゲーションバーで、**ネットワーク**をクリックします。
2. 左側のナビゲーションペインで、**メンテナンス > デバイス操作**を選択します。
3. 複数のデバイスを一括して再起動するには、ターゲットデバイスを選択し、再起動または構成を保存して再起動をクリックします。
4. 1つのデバイスを操作するには、必要に応じてデバイスの次のボタンをクリックします。
 - **コンフィグ保存**: 実行コンフィギュレーションを保存します。
 - **設定を保存して再起動する**: 実行コンフィギュレーションを保存して、デバイスを再起動します。
 - **再起動**: デバイスを直接再起動します。この操作により構成が失われる可能性があります。注意して使用してください。

図26 装置操作

<input checked="" type="checkbox"/>	状態	デバイス名 ⇅	タイプ	シリアル番号 ⇅	サイト名	最近一回再起動時間	最近一回再起動状態
<input checked="" type="checkbox"/>	●	CLOUDAP	クラウドAP	219801A24F8201E0000J	tokyo	なし	なし

Total entries: 1, current entries: 1 - 1. Page 1 of 1

システム

デバイスのバインド解除

どこかのサイトへ既に登録されている装置を新たなサイトへ登録しようとする、既に登録されているというメッセージが表示され登録できません。その時の解除方法がバインド解除という手順になります。

例えば、以下のようにCloudAPを登録しようとしたら、既にどこかのサイトへ登録されているというメッセージが表示されました。

デバイスの追加

デバイス情報

サイト:

[サイトがありませんか? 追加してください](#)

* デバイス名 (?):

* シリアル番号:

IRFデバイスですか: 一般 IRFデバイス

追加失敗, デバイス 219801A2959199G0001G クラウドプラットフォームに登録されました, [リリースするにはここをクリック](#), もし何か質問があれば、メールで連絡してください h3c_oasis@126.com

この時はメッセージの“[リリースするにはここをクリック](#)”をクリックします。

そうすると下図のような画面に遷移します。

デバイスのバインド解除

説明：現在はAC製品のみがデバイスの拘束操作をサポートしており,Release 5420及び以降のソフトウェアバージョンでなければならない
一日に最大5回まで

縛り解除ステップ：
1、接続解除装置のシリアル番号を入力し,取得したアンロックコードをコピーする
2、このデバイスのコマンドコンソールにおいて,システムビューでコピーされたコマンドを実行する
3、現在のページに戻ってリフレッシュボタンをクリックして,縛りの結果を確認します

シリアル番号

シリアル番号	リリースコード	解除状態
データなし		

そこで、**获取リリースコード**、英語の原文では"Obtain Unbinding Code"、つまりバインド解除コードの取得をクリックします。

すると、バインド解除コードが表示されます。

デバイスのバインド解除

説明：現在はAC製品のみがデバイスの拘束操作をサポートしており,Release 5420及び以降のソフトウェアバージョンでなければならない
一日に最大5回まで

縛り解除ステップ：
1、接続解除装置のシリアル番号を入力し,取得したアンロックコードをコピーする
2、このデバイスのコマンドコンソールにおいて,システムビューでコピーされたコマンドを実行する
3、現在のページに戻ってリフレッシュボタンをクリックして,縛りの結果を確認します

シリアル番号

装置上にこのコマンドを設定して,装置を縛り(24時間以内有効)解除してください: cloud-management unbinding-code 4B54z034cF85DYE3 **コピーコマンド**

シリアル番号	リリースコード	解除状態
219801A2959199G0001G	4B54z034cF85DYE3	まだ解りません

Total entries: 1, current entries: 1 - 1. Page 1 of 1

ここで上図の“コピーコマンド”をクリックすると、以下のようにデバイスのバインド解除コマンドが解除コードとともにテキストとしてコピーされます。

cloud-management unbinding-code 4B54z034cF85DYE3

このコマンドを登録しようとしていた装置で実行します。この時、この装置はCloudnetに接続できるインターネット接続がされているものとします。

<H3C>sys

System View: return to User View with Ctrl+Z.

[H3C]cloud-management unbinding-code 4B54z034cF85DYE3

[H3C]

これで、この装置はCloudnetへの登録が解除されるはずですが、上図の画面で“リフレッシュ”ボタンを

クリックして、解除状態をみます。“解除成功”であれば解除が成功しました

デバイスのバインド解除

説明：現在はAC製品のみがデバイスの拘束操作をサポートしており,Release 5420及び以降のソフトウェアバージョンでなければならない
一日に最大5回まで

縛り解除ステップ：
1、接続解除装置のシリアル番号を入力し,取得したアンロックコードをコピーする
2、このデバイスのコマンドコンソールにおいて,システムビューでコピーされたコマンドを実行する
3、現在のページに戻ってリフレッシュボタンをクリックして,縛りの結果を確認します

シリアル番号

シリアル番号	リリースコード	解除状態
219801A2959199G0001G	4B54z034cF85DYE3	解除成功

Total entries: 1 , current entries: 1 - 1. Page 1 of 1

では、改めて登録してみましょう。

デバイスの追加

デバイス情報

サイト:

[サイトがありませんか? 追加してください](#)

* デバイス名 (?):

* シリアル番号:

IRFデバイスですか:

デバイスを追加しました

● 注: 新しいデバイスが追加されたら、[更新]ボタンをクリックしてステータスを更新できます

リフレッシュ 削除 CLIヘルパー ファイルシステム その他機能

<input type="checkbox"/>	状態	修正	デバイス名	シリアル番号	タイプ
<input type="checkbox"/>	●		OFFICEAP	219801A2959199G0001G	Cloud AP

Total entries: 1 , current entries: 1 - 1. Page 1 of 1

デバイスの登録が完了したことが確認できました。

付録1 Cloudnetサポートマトリックス

Cloudnetはスイッチ、ルーター、無線LANコントローラー(AC)、無線アクセスポイント(AP)などを総合的に管理するツールのため、CloudAPではサポートされていない機能のメニューにアクセス出来てしまうので、以下にサポートマトリックスを掲載しました。

表2 ネットワーク管理メニュー

注:黄色で塗られた部分はCloudApではサポートしていません

レベル1	レベル2	レベル3	ブランチ	サイト
ネットワーク	テナント		√	√
	ダッシュボード		√	×
	サイト		√	√
	デバイス		√	√
	組織		√	√
クライアント	端末統計	クライアントサマリー	√	√
		クライアント詳細	√	√
		トラフィックの概要	√	√
		トラフィックの詳細	√	√
	スマート端末	重要端末	×	×
		監視カメラ	×	×
設定	自動展開		×	×
	バッチテンプレート	ACテンプレート	×	×
		スイッチテンプレート	×	×
		802.1xテンプレート	×	×
	クラウドAPテンプレート	クラウドAPテンプレート	√	√
		EoGREテンプレート	√	√
	クラウドAP	WLAN設定	√	√
		ユーザー管理	√	√
		オアシスモード	√	√
		ログイン管理	√	√
CLI設定		√	√	
メンテナンス	ソフトウェアの更新		√	√
	プライベートバージョン		√	√
	コマンドヘルプ		×	√
	ファイルシステム		×	√
	コンフィグの復元		×	√
	コンフィグ比較		√	√
	デバイス操作		√	√
	ヘルスチェック		×	×
	ツール		√	√
	デバイス交換		√	√

メッセージ	アラーム	警報ログ	√	√
		警報購読		
	SMS Details		×	×
	操作ログ		√	√
	システムメッセージ		√	√
システム	障害報告情報		√	√
	SMS Gateway		×	×
	サービススイッチ		√	√
	タグ		√	√
	サブアカウント		√	√
	オープンプラットフォーム		√	√
	アカウント		√	√
デバイスのバインド解除		×	×	

表3 スマートO&Mメニュー

注:黄色で塗られた部分はACの機能なのでCloudApではサポートしておりません

レベル1	レベル2	レベル3	ブランチ	サイト	
ダッシュボード	サマリー		√	√	
	接続性		√	×	
	Area Analysis	Area Detail		√	√
		AP Statistics		√	√
		AP Details		√	√
		Client Statistics		√	√
Client Details		√	√		
問題	問題分析		√	√	
	アラーム	警報ログ	√	√	
		警報購読	√	√	
クライアント	無線端末	健康	√	√	
		オンラインリスト	√	√	
		アクセス分析	√	√	
		端末統計	√	√	
ネットワーク	AP	健康	√	√	
		チャネル分析	√	√	
		AP統計	√	√	
		リポートAP	√	√	
最適化	ワンキー最適化	最適化設定	×	√	
		最適化進捗	×	√	
		最適化履歴	×	√	
	ワンキー診断		×	√	
セキュリティ	攻撃検知	攻撃検出	×	√	
		ログ	×	√	
	SSID検知		×	√	
	偽MAC検知		×	√	
Safeguard	Doctor AP	tests	×	×	
		Critical APS	×	×	
VIP	VIP AP		×	×	
	VIP端末		×	×	
AI-Driven Tasks	AI Analytics		×	×	
	Optimization		×	×	

レベル1	レベル2	レベル3	分岐	サイト
Power Saving	Power Save Mode		×	×
	Auto Shutdown	Area Summary	×	×
		Plan Detail	×	×
		Plan Logs	×	×

表4 サービスメニュー

注:黄色で塗られた部分はCloudApではサポートしておりません

レベル1	レベル2	レベル3	ブランチ	サイト
PPSK	ユーザーリスト		×	×
	パスワードリスト		×	×
	パスワードプッシュ		×	×
	パスワード要求		×	×
	監査記録		×	×
	特徴設定		×	×
ホテル管理	ネット最適化		×	×
	ルーム管理		×	×
	ラベル管理		×	×
クラウド工学調査	Engineering		×	×
	Basic Data	Device management	×	×
		Obstacle settings	×	×
		Scene settings	×	×
カスタム大画面	My Dashboards		√	√
	Sub-dashboards		×	×
	All dashboard		√	√
クラウド認証	認証テンプレート		√	√
	アカウント管理		√	√
資産管理	最終資産(PCなどの資産)		√	√
	資産管理(H3C製品)		√	√
Report Management	O&M Reports		√	√
	Users		√	√

付録2 APのモード変更

APのモード

APのモードには**FITモード**(工場出荷時)、**Anchor-acモード**(仮想無線LANコントローラー)、**Cloudモード**(Cloudnetで管理する)、**FATモード**(Cloudモードの特殊形でCloudnetモードのような機能を持つがCloudnetに管理されないモード)があります。

CloudnetでAPを管理するには、**ACに管理されたFITモード**、もしくは**個々に管理されるCloudモード**でなければなりません。以下はAPの動作モードの変更方法について説明いたします。

CLIからAPモードを変更する

APのCLIにアクセスしsystem-viewでap-mode cloudコマンドを実行します。そうすると新しいモードを有効にするためにAPが再起動しCloudモードに変更されます。

```
# syste-view|に入る
<H3C>system-view
System View: return to User View with Ctrl+Z.
# APの現在のモードを確認する(工場出荷時のFITモード)
<H3C>display wlan device role
Current running mode: FIT AP.
# APのモードをCloudモードに変更する
[H3C]ap-mode cloud
Changing working mode will reboot system. Continue? [Y/N]:y
# Cloudモードを有効にするために自動的にrebootします
System is starting...
Press Ctrl+D to access BASIC-BOOTWARE MENU...
Booting Normal Extended BootWare
The Extended BootWare is self-decompressing.....Done.

*****
*                                     *
*           H3C WA6638 BootWare, Version 7.14           *
*                                                         *
*****

Copyright (c) 2004-2021 New H3C Technologies Co., Ltd.
System image is starting...
Press ENTER to get started.

# syste-view|に入る
<H3C>system-view
System View: return to User View with Ctrl+Z.
# APの現在のモードを確認する(Cloudモード)
<H3C>display wlan device role
Current running mode: Cloud AP.
<H3C>
```

BootWareメニューからAPモードを変更する

APの起動時にBootWareが最初に起動し、インストールされているファームウェアをメモリーにロードして、そのファームウェアを起動しますが、BootWareメニューにアクセスすることによりAPの動作モードを選択することができます。

APをリブートします。出力例を次に示します。

System is starting...

Press Ctrl+D to access BASIC-BOOTWARE MENU...

Booting Normal Extended BootWare

The Extended BootWare is self-decompressingDone.....

```
*****
*                                                                 *
*           H3C WA6638 BootWare, Version 7.14                   *
*                                                                 *
*****
```

Copyright (c) 2004-2021 New H3C Technologies Co., Ltd.

Compiled Date: Jan 28 2021

CPU L1 Cache: 32KB

CPU L2 Cache: 256KB

CPU Clock Speed: 2200MHz Memory

Type: DDR3 SDRAM

Memory Size: 1024MB

Memory Speed: 933MHz

Flash Size: 256MB

PCB Version: Ver.A BootWare

Validating...

Press Ctrl+B to access EXTENDED-BOOTWARE MENU...

上記プロンプトで**Ctrl+B**を入力して、EXTENDED-BOOTWAREメニューに入ります。

Password recovery capability is enabled.

Note: The current operating device is flash

Enter < Storage Device Operation > to select device.

```
=====<EXTENDED-BOOTWARE MENU>=====
|<1> Boot System |
|<2> Enter Serial SubMenu |
|<3> Enter Ethernet SubMenu |
|<4> File Control |
|<5> Restore to Factory Default Configuration |
|<6> Skip Current System Configuration |
|<7> BootWare Operation Menu |
|<8> Skip Authentication for Console Login |
|<9> Storage Device Operation |
|<0> Reboot |
=====
```

Ctrl+Z: Access EXTENDED ASSISTANT MENU

Ctrl+F: Format File System

Ctrl+C: Display Copyright

Ctrl+Y: Change AP Mode

Enter your choice(0-9):

Ctrl+Yキーを押してAPモードを変更します。

Please select the new mode Current mode is Fit

```
=====
|NO. Mode                                                    |
|1  Fit Mode                                                  |
|2  Anchor-AC (Virtual AC Mode)                             |
|3  Cloud Mode                                              |
|0  Exit                                                      |
=====
```

Enter your choice(0-3):**3**

Changed to cloud mode successfully!

```
=====<EXTENDED-BOOTWARE MENU>=====
|<1> Boot System                                             |
|<2> Enter Serial SubMenu                                   |
|<3> Enter Ethernet SubMenu                                 |
|<4> File Control                                           |
|<5> Restore to Factory Default Configuration              |
|<6> Skip Current System Configuration                     |
|<7> BootWare Operation Menu                               |
|<8> Skip Authentication for Console Login                |
|<9> Storage Device Operation                             |
|<0> Reboot                                                 |
=====
```

Ctrl+Z: Access EXTENDED ASSISTANT MENU

Ctrl+F: Format File System

Ctrl+C: Display Copyright

Ctrl+Y: Change AP Mode

Enter your choice(0-9): **0**

System is starting...

Press Ctrl+D to access BASIC-BOOTWARE MENU...

Booting Normal Extended BootWare

The Extended BootWare is self-decompressing.....Done.

```

*****
*
*           H3C WA6638 BootWare, Version 7.14           *
*
*****

Copyright (c) 2004-2021 New H3C Technologies Co., Ltd.
System image is starting...
Press ENTER to get started.

# syste-view|に入る
<H3C>system-view
# APの現在のモードを確認する(Cloudモード)
<H3C>display wlan device role
Current running mode: Cloud AP.

```

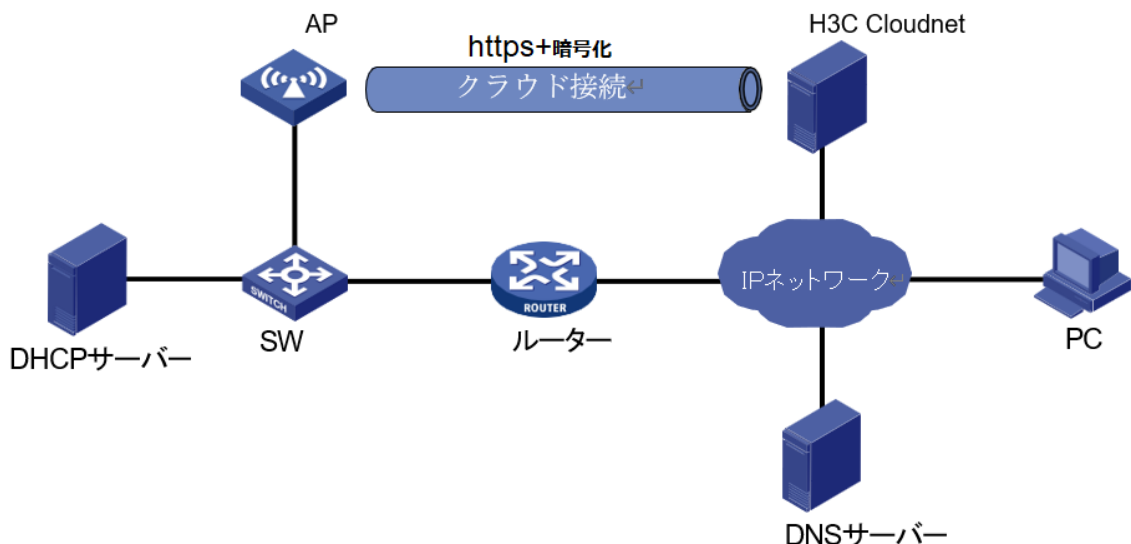
CloudnetからAPモードを変更する

図28に示すように設定環境を設定し、DHCP経由でIPアドレスを取得するようにAPを設定します。

次の条件が満たされていることを確認してください。

- APはどのACにも登録されていません
- APは、DHCPサーバーによって割り当てられたIPアドレスを使用してパブリックネットワークに到達できます。
- DNSサーバーはCloudnetのドメインアドレスを名前解決できます。

図27 構成環境のセットアップ



ブラウザでoasiscloud.h3c.comにアクセスし、ユーザー名とパスワードを入力します。
CloudnetにAPを追加します。

1. 上部のナビゲーションバーネットワークをクリックし、左側のナビゲーションペインでネットワーク > デバイスを選択します。

2. ページの左上隅からターゲットのブランチとサイトを選択し、+デバイスの追加をクリックします。
3. デバイス名、シリアル番号、およびデバイスタイプ(一般デバイス,IRFデバイス)を指定し、デバイスの追加をクリックします。

図28 デバイスの追加

デバイス情報

サイト:

サイトがありませんか? 追加してください

* デバイス名 [?]:

* シリアル番号:

IRFデバイスですか:

4. APを起動します。APが起動してACの検出に失敗すると、Cloudnetとの最初の関連付けで動作モードがCloudに変わります。
5. APモードを手動で変換するには、トップナビゲーションバーのネットワークをクリックし、左ナビゲーションペインで設定 > クラウドAP > オアシスモードを選択します。次に、ターゲットAPのモード切替を許可にします。

図29クラウドモードの許可

オアシスモード

● 説明: 許可に設定、禁止に設定デバイスが自動的にクラウドAPモードをオンにするかどうかを設定します

	デバイス名	シリアル番号	APモード	モード切り替え
<input type="checkbox"/>	FIT AP	219801A24F8201E0000J	Fit Ap	<input checked="" type="checkbox"/> 許可

第 1 ~ 1 エントリーを表示する(総計 1 エントリー)

付録3 SNMP及びsyslog設定

ネットワーク管理のアプリケーションとしてSNMPマネージャーが使われている場合、CloudAPに設定する方法と、エラーログの管理にsyslogサーバーが使われている場合の設定方法はCLIコマンドで設定する必要があります。

Syslogサーバーへのlog送信設定

Cloudnetではsyslogサーバーへのlog送信機能はサポートしておりません。syslogサーバーへのログ送信の必要があれば、GUIにアクセスして設定する必要があります。

GUIへのアクセス方法は「付録4トラブルシューティング」を参照してください。

1. System-view|に入ってinfo-centerコマンドでホストと記録するエラーのレベルを指定します。

```
<H3C> system-view
```

```
[H3C] info-center loghost syslogサーバーのIPアドレス
```

```
[h3c] info-center source default loghost level critical
```

レベルは以下の通り

Alert 推奨アクションはすぐに行う必要があります (severity=1)

Critical 危機的な状態 (severity=2)

Debugging デバッグレベルのメッセージ (severity=7)

Emergency システムが動作していません (severity=0)

Error エラー状態 (severity=3)

Informational 情報メッセージ (severity=6)

Notification 正常だが重大な状態 (severity=5)

Warning 警告状態 (severity=4)

又はGUIではsyslogサーバーのアドレスは指定できますが、sourceにあたる指定はできません。

System View > Network Configuration > Management Protocols > Settings

System > Network Configuration > Management Protocols > Settings

HTTP/HTTPS Telnet SSH NTP LLDP **Settings**

Dashboard

Network Configuration

Network Interfaces

VLAN

Network Routing

Network Services

Management Protocols

Network Security

System

Log to buffer

Output logs to the log buffer

Maximum Buffered Logs 512

Log to hosts

Hostname or IP	Port	VRF
10.10.11.48	514	Public network
1 - 253 chars.	1-65535,514 for default	Public network

* Up to 4 log hosts.

Hostname or IP	Port	VRF
10.10.11.48	514	Public network
1 - 253 chars.	1-65535,514 for default	Public network

syslogサーバーのログの例

3CDaemon

File View Help

Time	IP Address	Msg Type	Message
Jul 26 09:59:28	10.10.11.44	local7.info	Jul 26 08:59:27 2022 WA538-JP2 %%10STAMGR/6/STAMGR_CLIENT_OFFLINE: Client c8e2-6535-5d0e went o
Jul 26 09:59:28	10.10.11.44	local7.notice	Jul 26 08:59:27 2022 WA538-JP2 %%10IFNET/5/LINK_UPDOWN: Line protocol state on the interface Vlan-in
Jul 26 09:59:28	10.10.11.44	local7.err	Jul 26 08:59:27 2022 WA538-JP2 %%10IFNET/3/PHY_UPDOWN: Physical state on the interface Vlan-interfac
Jul 26 09:59:07	10.10.11.41	local7.info	Jul 26 08:59:06 2022 WA538-JP1 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:59:06	10.10.11.41	local7.info	Jul 26 08:59:05 2022 WA538-JP1 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:59:06	10.10.11.41	local7.info	Jul 25 08:44:00 2022 WA538-JP1 %%10SYSLOG/6/SYSLOG_RESTART: System restarted -- H3C Comware Soft
Jul 26 09:58:42	10.10.11.44	local7.info	Jul 26 08:58:41 2022 WA538-JP2 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:58:30	10.10.11.44	local7.info	Jul 26 08:58:30 2022 WA538-JP2 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:58:13	10.10.11.52	local7.info	Jul 26 08:58:12 2022 WA538-JPX %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:58:11	10.10.11.52	local7.info	Jul 26 08:58:10 2022 WA538-JPX %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:58:08	10.10.11.52	local7.info	Jul 26 08:58:07 2022 WA538-JPX %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:58:08	10.10.11.52	local7.info	Jul 26 08:58:05 2022 WA538-JPX %%10SYSLOG/6/SYSLOG_RESTART: System restarted -- H3C Comware Soft
Jul 26 09:56:55	10.10.11.44	local7.info	Jul 26 08:56:54 2022 WA538-JP2 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:56:15	10.10.11.44	local7.info	Jul 26 08:56:15 2022 WA538-JP2 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:56:11	10.10.11.44	local7.info	Jul 26 08:56:10 2022 WA538-JP2 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:56:06	10.10.11.44	local7.info	Jul 26 08:56:05 2022 WA538-JP2 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:55:58	10.10.11.44	local7.info	Jul 26 08:55:58 2022 WA538-JP2 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:55:55	10.10.11.44	local7.info	Jul 26 08:55:54 2022 WA538-JP2 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:55:47	10.10.11.44	local7.info	Jul 26 08:55:46 2022 WA538-JP2 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:55:37	10.10.11.44	local7.info	Jul 26 08:55:36 2022 WA538-JP2 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:55:30	10.10.11.44	local7.info	Jul 26 08:55:30 2022 WA538-JP2 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:55:21	10.10.11.44	local7.info	Jul 26 08:55:20 2022 WA538-JP2 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:55:04	10.10.11.44	local7.info	Jul 26 08:55:04 2022 WA538-JP2 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:54:39	10.10.11.44	local7.info	Jul 26 08:54:38 2022 WA538-JP2 %%10SHELL/6/SHELL_CMD: -Line=con0-IPAddr=""-User=""; Command is
Jul 26 09:54:39	10.10.11.44	local7.info	Jul 25 09:15:12 2022 WA538-JP2 %%10SYSLOG/6/SYSLOG_RESTART: System restarted -- H3C Comware Soft

For Help, press F1

SNMPでの管理設定

CloudnetではSNMPとの連携はサポートしていません。SNMPマネージャーとの連携の必要があれば、GUIにアクセスして設定する必要があります。

GUIへのアクセス方法は「付録4トラブルシューティング」を参照してください。

1. System-viewに入ってsnmpコマンドでコミュニティ名やSNMPのバージョンの設定をします。

```
<H3C> system-view
```

```
[H3C] snmp-agent community write simple xxxxxxx
```

```
[H3C] snmp-agent community read simple xxxxx
```

```
[H3C] snmp-agent sys-info version all
```

2. 前の項目でCloudAPやクライアントなどでエラーなどの事象が発生した場合にSNMPのtrapメッセージを送る場合は以下のような設定をします。Securitynameは固有の設定をし、v2cはtrapのバージョンを指定します。

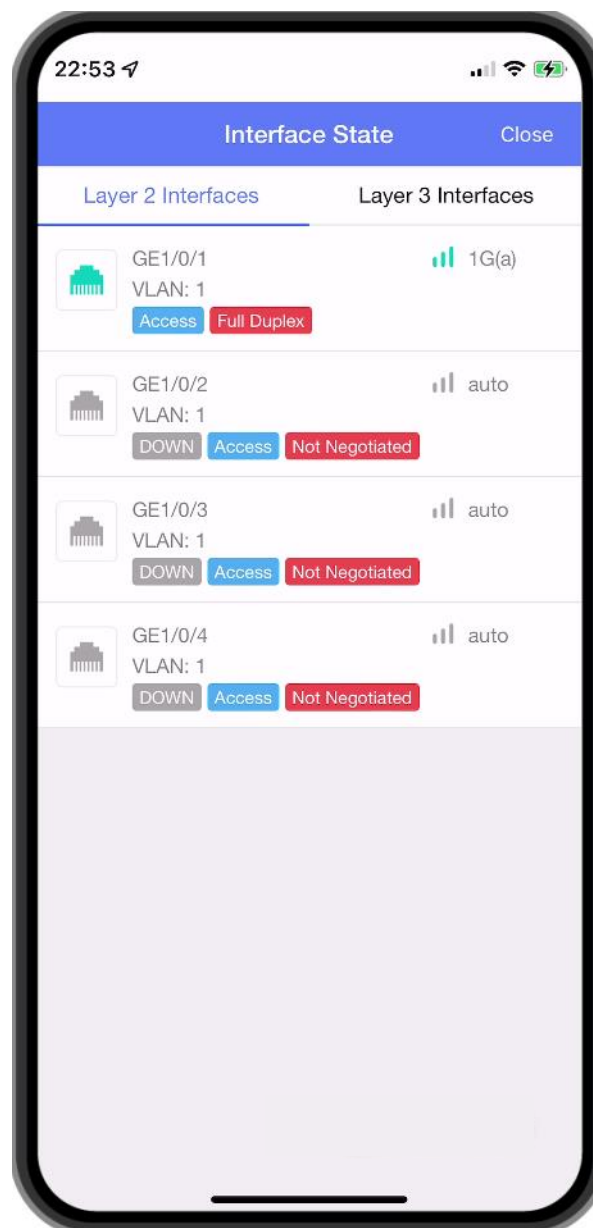
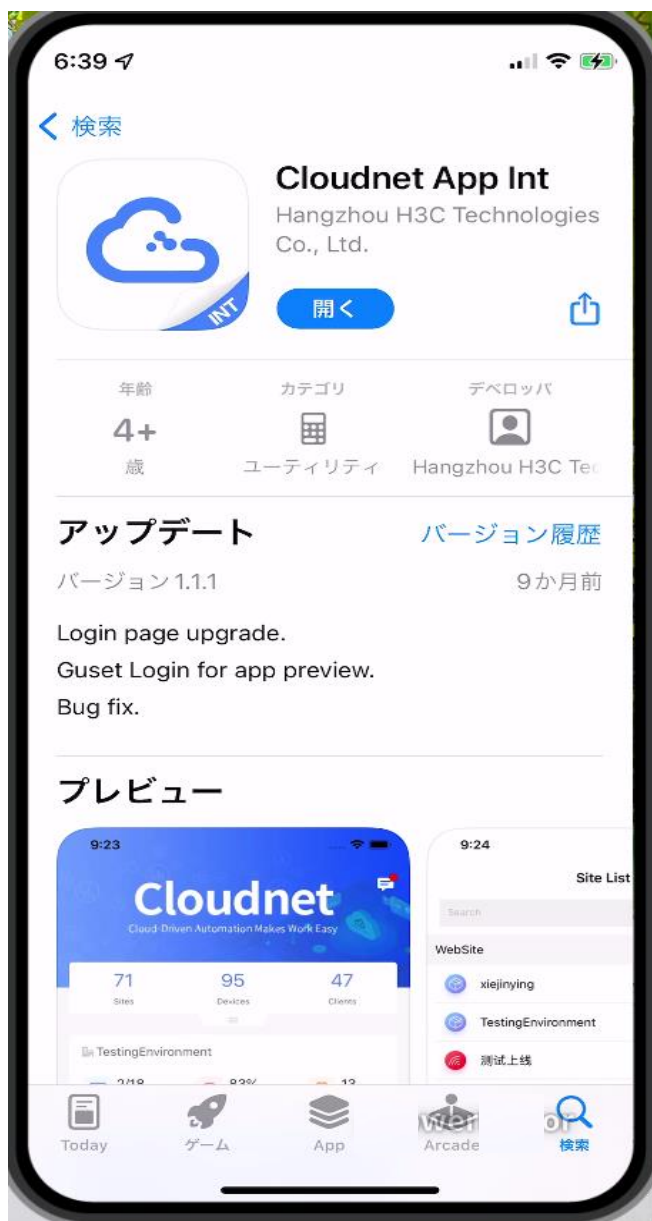
```
[H3C] snmp-agent trap enable syslog
```

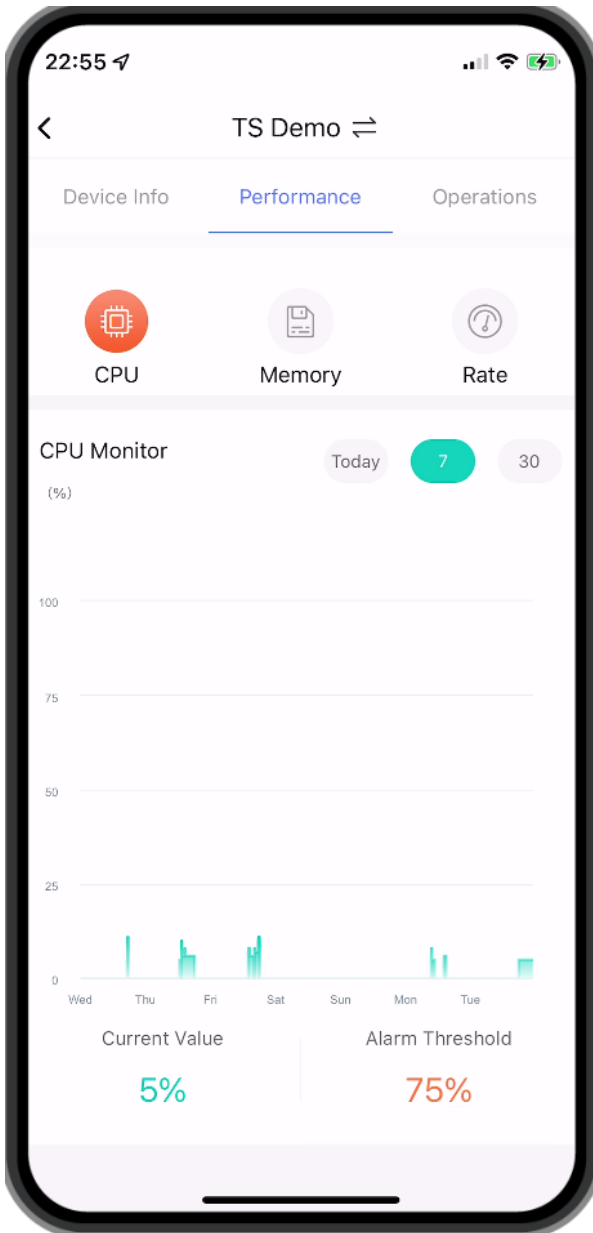
```
[H3C] snmp-agent target-host trap address udp-domain トラップを受信するip-address params
```

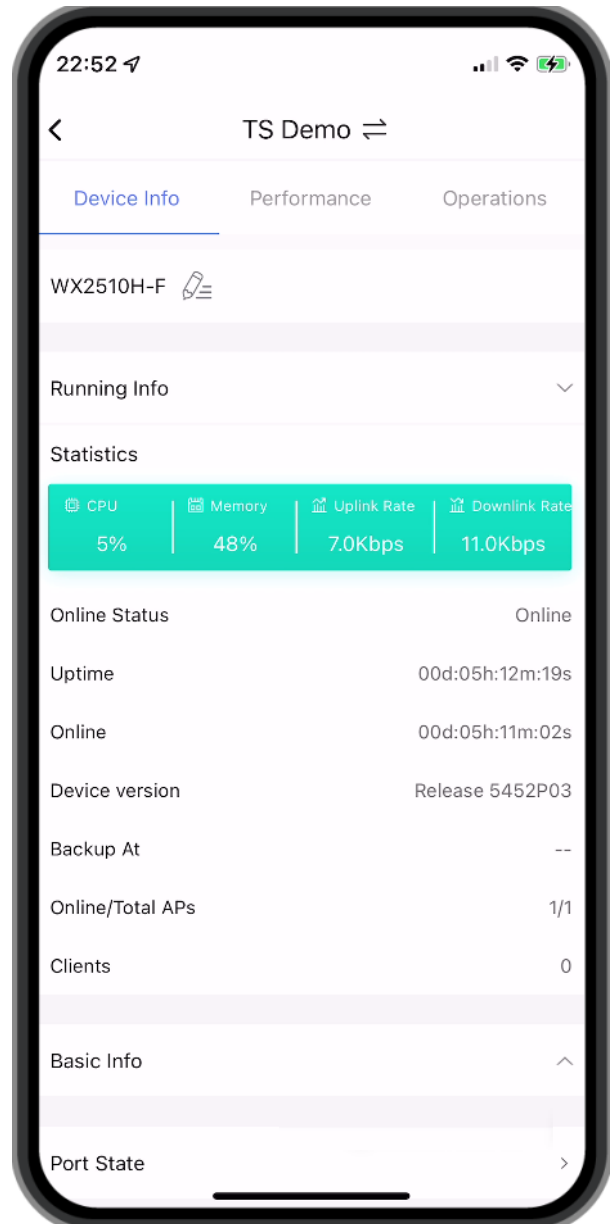
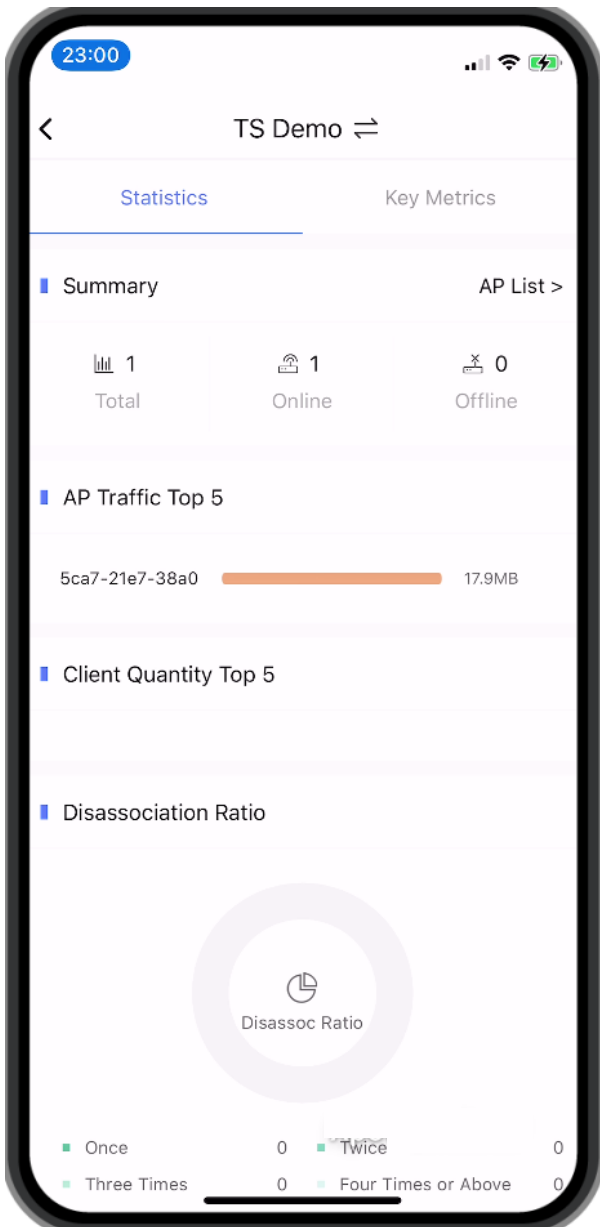
```
securityname WA6638_01 v2c
```

付録4 スマホのCloudnetアプリ

Cloudnetはスマホのアプリが提供されております。







付録5 トラブルシューティング

トラブルの状況が自身では解決できない場合は、テクニカルサポートへ必要な情報を取得してメールにて連絡して頂きます。

1. CloudAPのログインパスワードを既にデフォルトから変更されている場合は以下の手順3に進んでください。
2. CloudAPのログインパスワードを変更するためにGUIへアクセスします。そのために以下のようにネットワーク > サイト > デバイス情報を選択します。
そして、ローカル管理をクリックします。

デバイス情報

リフレッシュ 削除 再記録 **ローカル管理** CLIヘルパー ファイルシステム その他機能

<input checked="" type="checkbox"/>	状態	デバイス名	シリアル番号	タイプ	型番
<input checked="" type="checkbox"/>	●	WA6638NOTJP	219801A24F8201E0000J	Cloud AP	WA6638

Total entries: 1, current entries: 1 - 1. Page 1 of 1

ブラウザが開いて以下のログイン画面が現れます。

H3C WLAN Management Platform

WA6638

Remember username English

Login

Internet Explorer 10, Firefox 30.0.0.5269, Chrome 35.0.1916.114, Safari 5.1, and their higher versions are supported.

ユーザー名 **admin**、パスワードにフェフォルトのパスワード**h3capadmin**を入力するとパスワードの変更が求められます。

Change Password ✕

The default password is not secure. A qualified password must meet the following requirements: It must contain a minimum of 10 characters. It must contain a minimum of 2 types, and a minimum of 1 character for each type. It can't contain the username or the reversed letters of the username.

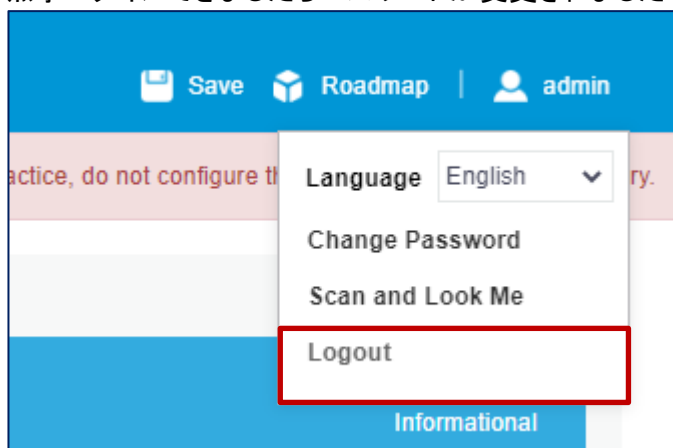
Old Password

New Password

Confirm Password

Apply
Cancel

無事ログインできましたらパスワードが変更されましたので、ログアウトして結構です。



3. ネットワーク > サイト > デバイス情報を選択して、CLIヘルパーを選択します。

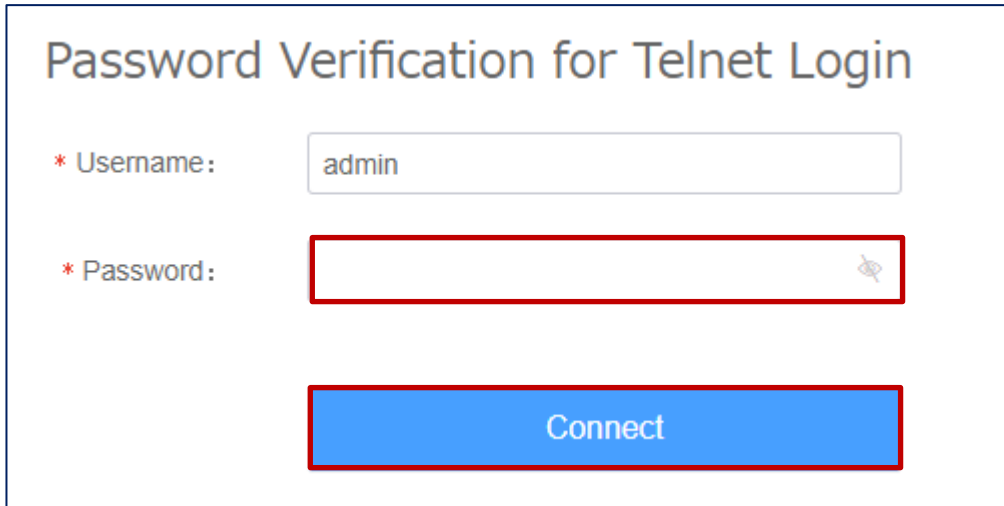
デバイス情報

リフレッシュ
削除
再認識
ローカル管理
CLIヘルパー
ファイルシステム
その他機能

<input checked="" type="checkbox"/>	状態	デバイス名	シリアル番号	タイプ	型番
<input checked="" type="checkbox"/>	●	WA6638NOTJP	219801A24F8201E0000J	Cloud AP	WA6638

Total entries: 1, current entries: 1 - 1. Page 1 of 1

4. 表示された画面に先ほど設定したログインパスワードを入力します。



Password Verification for Telnet Login

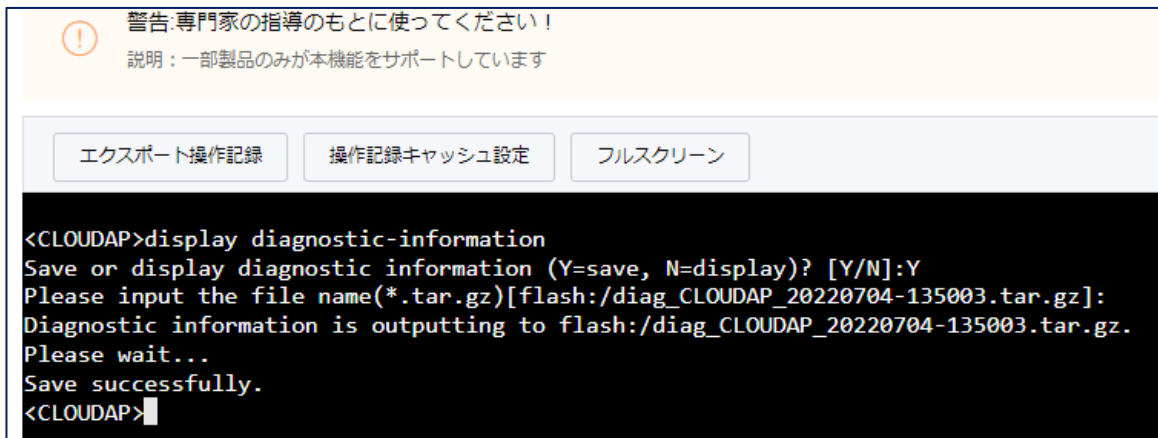
* Username:

* Password:

Connect

5. コマンド入力画面が表示されますので、以下のように診断情報を取得するコマンドを入力してください。なお、取得した情報は装置上のflashドライブに保存されます。

```
<CLOUDAP>display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name(*.tar.gz)[flash:/diag_CLOUDAP_20220704-
135241.tar.gz]: [enterキー]
Diagnostic information is outputting to flash:/diag_CLOUDAP_20220704-
135241.tar.gz.
Please wait...
Save successfully.
<CLOUDAP>
```




警告:専門家の指導のもとに使ってください!
説明:一部製品のみが本機能をサポートしています

エクスポート操作記録 操作記録キャッシュ設定 フルスクリーン

```
<CLOUDAP>display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:Y
Please input the file name(*.tar.gz)[flash:/diag_CLOUDAP_20220704-135003.tar.gz]:
Diagnostic information is outputting to flash:/diag_CLOUDAP_20220704-135003.tar.gz.
Please wait...
Save successfully.
<CLOUDAP>
```

6. 取得した診断情報をダウンロードするには、上部のナビゲーションバーメンテナンス > ファイルシステムを選択します。

Flash記憶空間： 26% 使えます 190.45 MB, 共 256.00 MB。



ロファイル

cfg、mdb、txtファイルを含み、慎重に


[管理](#)



データベースファイル

dat、dbファイルを含み、慎重に


[管理](#)



ログファイル

log、log.gzファイルを含む

[管理](#)



診断ファイル

coreファイルを含む

[管理](#)

● ● ●

その他

未分類のすべてのファイルを含む

[管理](#)

7. 表示された画面で**その他**のカテゴリの**管理**をクリックします。
そして、先ほどのコマンドで保存されたファイルを選択し、**ダウンロード**をクリックします。

[↓ ダウンロード](#)[📄 名前変更](#)[🗑️ 削除](#)[🔄 リフレッシュ](#)

[前のステージに戻ります](#) | [その他](#)

	ファイル名	サイズ
<input checked="" type="radio"/>	⋮ diag_CLOUDAP_20220704-135003.tar.gz	95.77 KB
<input type="radio"/>	⋮ dsakey	567.00 B
<input type="radio"/>	⋮ hostkey	735.00 B
<input type="radio"/>	⋮ https-server.p12	2.34 KB
<input type="radio"/>	⋮ serverkey	591.00 B

Total entries: 5 , current entries: 1 - 5. Page 1 of 1

8. ダウンロードされたファイルを以下のように障害の内容を記載して以下のテクニカルサポート宛に送付ください。

【送付先】

TO: h3cts@h3c.com

CC: &TS-INTL-JPN@h3c.com

【H3C カスタマーサービスE-mail テンプレート】

会社名 & 担当者名 :

プロジェクト名 (オプション) : *office Network Reconstruction Project**

問題説明: S5130S Switch interface fails to go up

※オペレーションログ : Record the process of the operation, or the process log of the failure.

※Diag診断ログ: diagnostic information in failure time

※ログファイル : log information in failure time

※ネットワークポロジ : ***

※製品モデル: S5130S-28P-EI

※シリアル番号: 219801A1N59186Q0XXXX

※ソフトウェアバージョン : Version 7.1.064, Release 5223

※緊急性:

付録6 GUIへのアクセス方法

ローカルでの場合

CloudnetからへのAPの設定、監視が前提であるCloud APですが、ローカルセグメント上でGUIにアクセスする方法をご紹介します。ここでは、VLANの作成や、クラウドでサポートしていない機能を設定することはお勧めできません。Cloudで設定を保証しているのは、あくまでもCloudnetで行った設定だからです。

1. APは管理用の隠しSSIDであるH3C_xxxxxx、ここではMACアドレスの下6桁(下の例ではF361A0)を加えたH3C_F361A0を送信しています。

※装置のシリアル番号は装置のCLIコマンドで確認できます。

<CLOUDAP>**dis device manuinfo**

DEVICE_NAME:WA6638

DEVICE_SERIAL_NUMBER:219801A24F8201E0009X

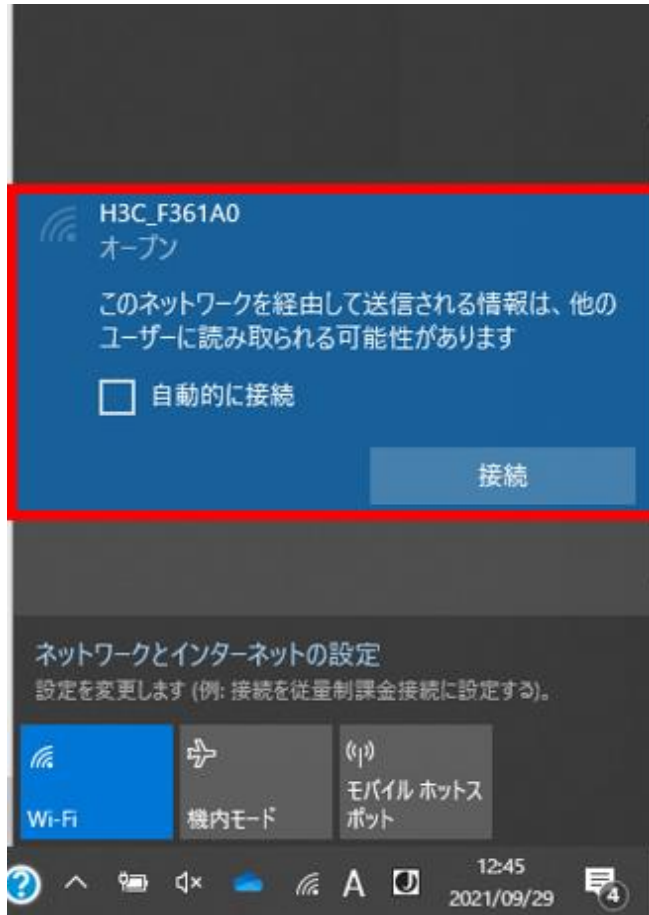
MAC_ADDRESS:F010-90**F3-61A0**

MANUFACTURING_DATE:2020-02-29

VENDOR_NAME:H3C



2. このSSIDに接続します。



3. APから10.40.94.xのアドレスが割り当てられます。

```
cmd コマンドプロンプト
C:\Users>ipconfig
Windows IP 構成

Wireless LAN adapter ローカル エリア接続* 1:
   メディアの状態. . . . . : メディアは接続されていません
   接続固有の DNS サフィックス . . . . . :

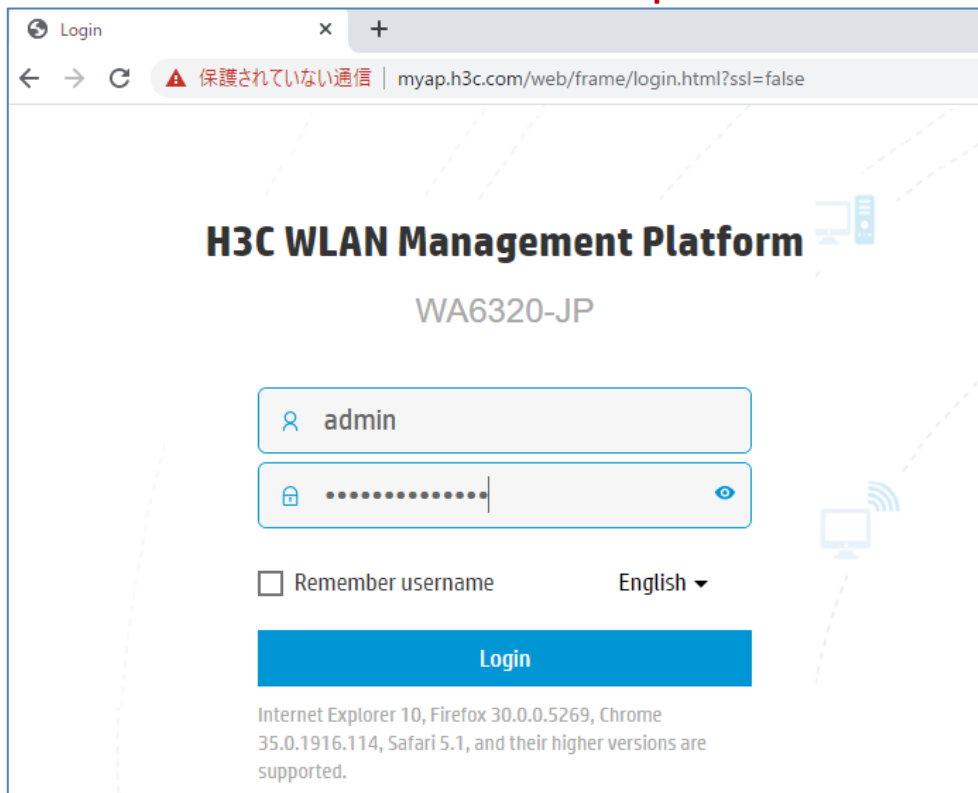
Wireless LAN adapter ローカル エリア接続* 2:
   メディアの状態. . . . . : メディアは接続されていません
   接続固有の DNS サフィックス . . . . . :

Wireless LAN adapter Wi-Fi:
   接続固有の DNS サフィックス . . . . . :
   リンクローカル IPv6 アドレス. . . . . : fe80::35e8:d633:3383:d67%7
   IPv4 アドレス. . . . . : 10.40.94.2
   サブネット マスク . . . . . : 255.255.255.0
   デフォルト ゲートウェイ . . . . . : 10.40.94.1

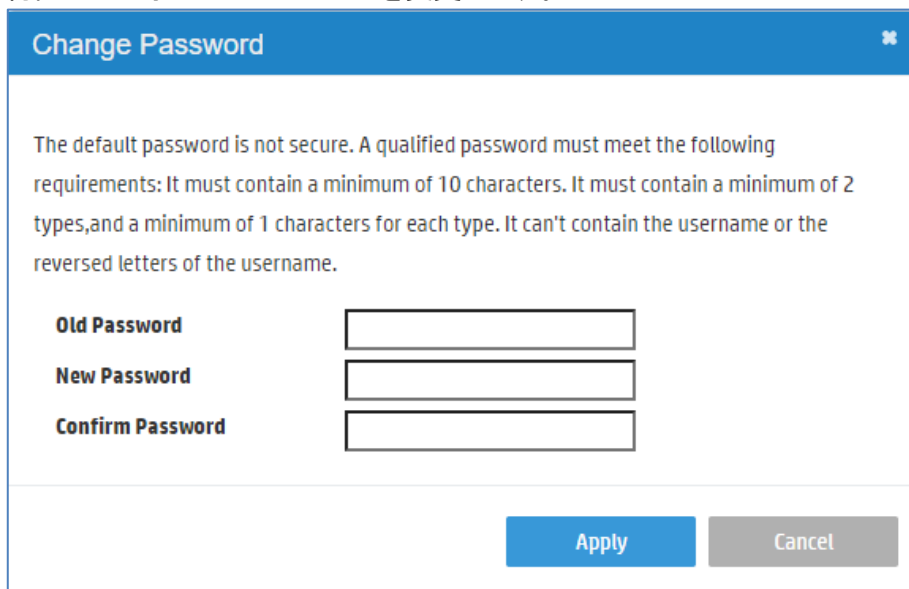
イーサネット アダプター Bluetooth ネットワーク接続:
   メディアの状態. . . . . : メディアは接続されていません
   接続固有の DNS サフィックス . . . . . :

C:\Users>
```

4. PCのブラウザを起動し以下のURLを入力します。
<http://myap.h3c.com/>
5. Cloud APのGUIでのログイン画面が現れます。
デフォルトのユーザー名: **admin**、パスワード: **h3capadmin**

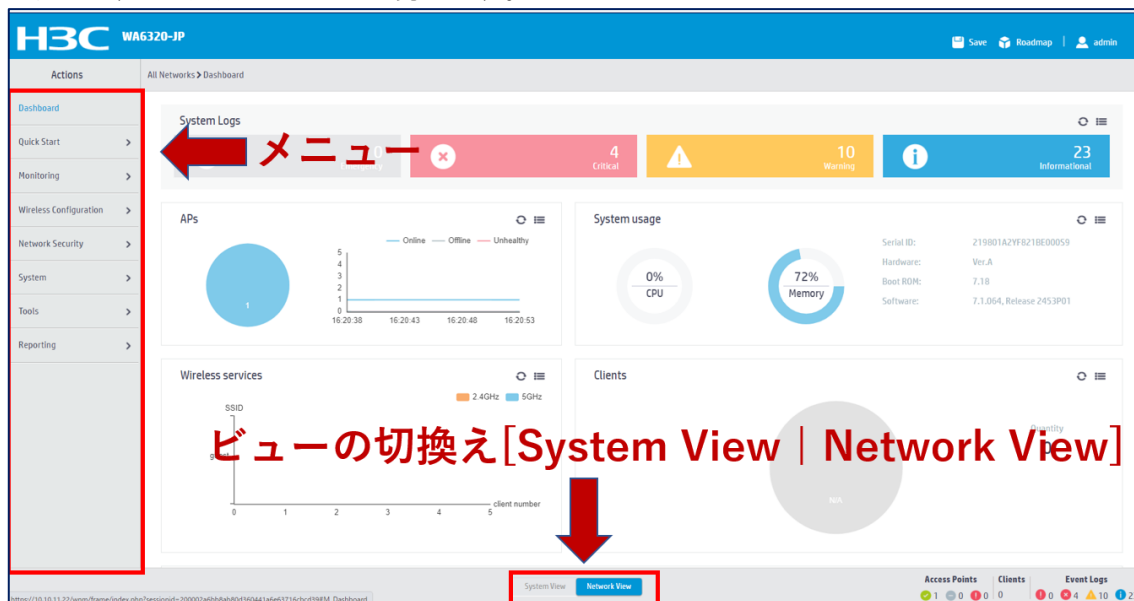


6. 初回はデフォルトのパスワードを変更します。



パスワードは10文字以上で、英数字記号などの2種類を含み、登録されているユーザー、adminなどの文字を含まないこと。

7. ログインするとダッシュボードが現れます。

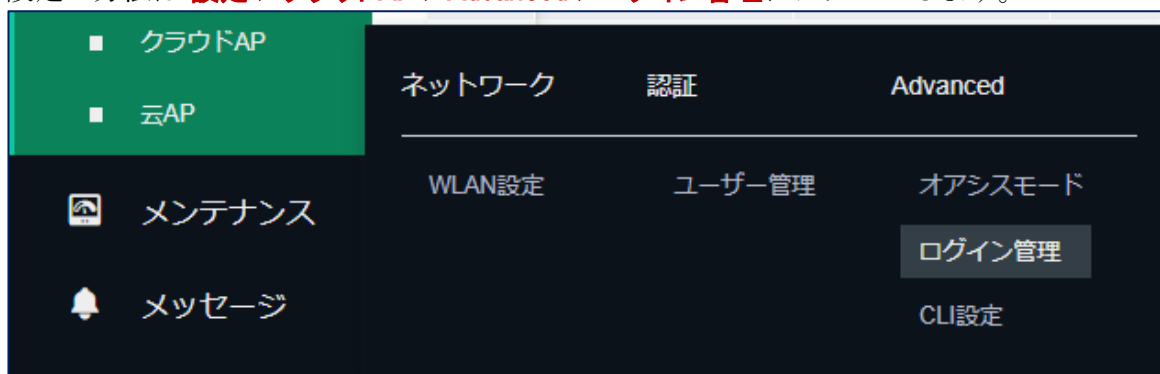


管理用SSIDのセキュリティ強化

管理用のSSIDをクライアントから見られる状態で、認証なしでアクセスできるのはセキュリティ上問題です。

従って、非表示にしてパスワードを要求するようにすることを推奨します。

設定の方法は **設定 > クラウドAP > Advanced > ログイン管理** にアクセスします。



非表示にしてパスワードを要求するには以下のようにします。

管理Wi-Fi

① 管理Wi-Fiを介してクラウドAPデバイスにアクセスし管理できます,管理Wi-FiのデフォルトのSSIDは「H3C_XXXXXX」

非表示SSID ② オンにする シャットダウン

暗号化ステータス ② オンにする シャットダウン

..... (注: パスワードは、8-63の数字、文字、或

CloudnetからローカルのGUIへアクセスの場合

CloudnetからへのAPのGUIへアクセスする方法があります。こちらもGUIにアクセスするとCloudnetでサポートしていない機能にアクセスすることができますが、Cloudnetには表示されませんので気を付けてください。

1. 部のナビゲーションバーネットワーク > デバイスを選択します。
2. CloudAPの列のチェックボックスをチェックします。



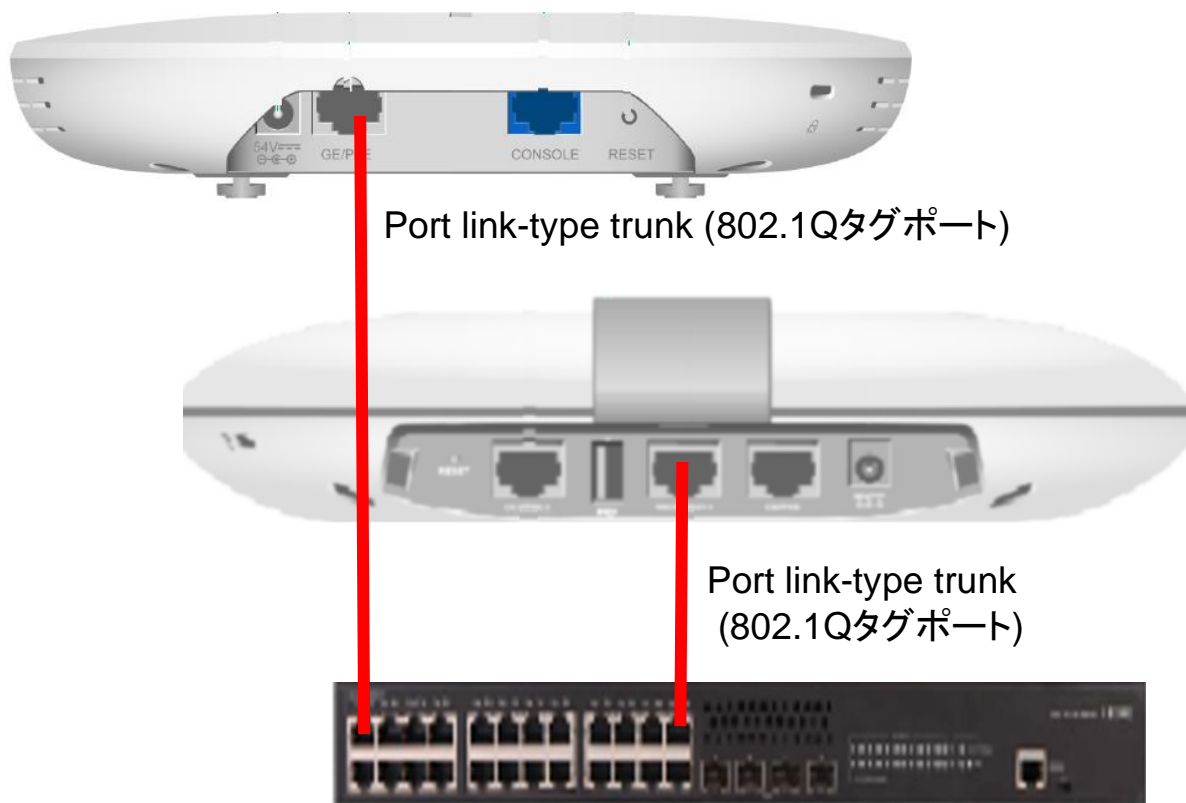
The screenshot shows the Cloudnet web interface. The top navigation bar includes 'ネットワーク' (Network), 'スマートO&M', and 'サービス'. The left sidebar has 'デバイス' (Devices) selected. The main content area shows 'デバイス' (Devices) with a 'クラウドAP' (Cloud AP) button. Below this are several action buttons: 'リフレッシュ', '削除', '再接続', 'クラウド接続をreset', 'アップグレードバージョン', 'CLIヘルパー', 'ファイルシステム', and 'ローカル管理' (Local Management). A table below lists devices with columns for '状態' (Status), '修正' (Action), 'デバイス名' (Device Name), 'シリアル番号' (Serial Number), 'タイプ' (Type), '型番' (Model Number), and 'サイト名' (Site Name). The first row shows a device named 'CLOUDAP' with a checked checkbox in the '状態' column and a 'ローカル管理' button highlighted in red.

	状態	修正	デバイス名	シリアル番号	タイプ	型番	サイト名
<input checked="" type="checkbox"/>	●	✉	CLOUDAP	219801A24F8201E0000J	Cloud AP	WA6638	tokyo

3. 水色で示された利用できる機能の中で、ローカル管理をクリックします。
4. ローカルでの場合同様、ログイン画面が現れますので、ログインします。
この場合、CloudnetからCloud APのGUIにアクセスするため、ローカルに比べて、遅い、一部の画面の表示が乱れるなどの症状が現れます。

付録7 PoEとの接続

CloudAPのインタフェースポートはTRUNK(タグ)ポートになっておりますので、デフォルトVLAN 1以外のVLANを作成した場合、PoEスイッチのポートもTRUNKに設定する必要があります。



PoEスイッチの設定例

```
<H3C>system-view
```

```
System View: return to User View with Ctrl+Z.
```

```
[H3C]interface GigabitEthernet 1/0/1
```

```
[H3C-GigabitEthernet1/0/1]port link-type trunk
```

```
[H3C-GigabitEthernet1/0/1]port trunk permit vlan all
```

```
[H3C-GigabitEthernet1/0/1]quit
```