Technical Note

aruba
a Hewlett Packard Enterprise company

Aruba Central 基本操作ガイド

～AP 編 (AOS10)～

日本ヒューレット・パッカード合同会社
Aruba 事業統括本部

目次

以下の表に、本文書の修正点を示します。

表 1: 改訂履歴

版数	主な変更内容
第1版	初版発行

1. はじめに

1.1. 本資料について

本資料は Aruba Central におけるインスタントアクセスポイント(AOS10)の基本操作、設定についてサンプル構成を用いた設定例を紹介しています。

1.2. 注意事項

本資料は弊社内において基本動作等を確認したものであり、お客様の環境における動作の保証をしているものではございません。また、Windows, Windows Server など Aruba で取り扱っていない製品を使用して説明しているため、設定内容における保証は致しかねます。構成を構築する上での参考にしていただくドキュメントであることを予めご了承ください。本資料の内容は予告なく変更される場合があります。

Central を初めて使われる方は以下の Central 基本操作ガイド(入門編)をはじめに参照いただくことを推奨いたします。

https://www.arubanetworks.com/ja/resource/aruba-central-basic-operation-technical-guide/

1.3. Software Version

本資料は Aruba Central 2.5.6 を元に作成しております。

※一部キャプチャ画像が最新の Central 画面と異なることがございます。ご了承ください。

2. Central へ AP のオンボーディング

2.1 サブスクリプション、デバイスの追加方法とサブスクリプションの割り当て

Central へ AOS10 AP をオンボーディングするには以下のことが GLCP で完了している必要があります。

- Central で管理する AP 数分のサブスクリプションが GLCP に登録されていること
- AP が GLCP へ登録されていること
- サブスクリプションが AP に割り当てられていること

サブスクリプション、デバイスの追加方法とサブスクリプションの割り当てに関しては、以下 Central 設定入門ガイドを参照してください。
https://www.arubanetworks.com/ja/resource/aruba-central-basic-operation-technical-guide/

2.2 グループ・サイト・ラベルの作成方法

Central 内で事前に AP を割り当てるためのグループ（作成必須）・サイト（作成推奨）・ラベル（オプション）を作成する必要があります。
グループ・サイト・ラベルそれぞれの昨日説明・作成方法に関しては、以下 Central 設定入門ガイドを参照してください。
https://www.arubanetworks.com/ja/resource/aruba-central-basic-operation-technical-guide/

2.3 AP のプロビジョニング

上記で作成したグループ・サイト・ラベルに AP を割り当てます。グループへ AP を割り当てる際には“Central でオンラインになったことがあるデバイス”と“Central で一度もオンラインになったことがないデバイス”で操作方法が異なります。
それぞれの操作方法に関しては、以下 Central 設定入門ガイドを参照してください。
https://www.arubanetworks.com/ja/resource/aruba-central-basic-operation-technical-guide/

3. AP の起動

3.1 AP を起動する前に

AP が AOS10 のデフォルトイメージで起動してくることを確認ください。AOS6 or AOS8 のデフォルトイメージで起動する場合、AOS10 のイメージへバージョンアップしてください。AOS6 or AOS8 で既存の設定がある場合、**AOS10 のイメージへバージョンアップすると設定は初期化されるためご注意ください。**
AP は初期値として IP アドレスが設定されておりません。**DHCP サーバが動作をしている環境**、もしくは**コンソールケーブル**をご用意ください。DHCP サーバを利用する場合は、配布をする Default Gateway に通信が可能な環境で行ってください。

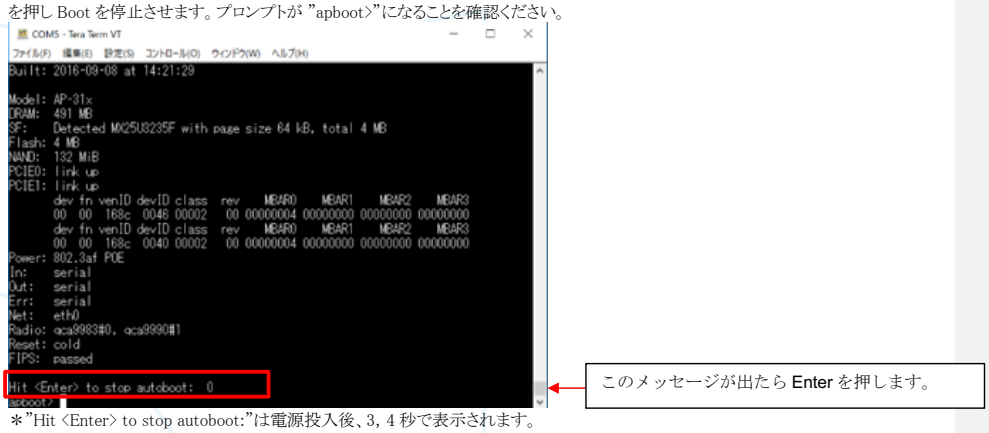
3.2 電源の投入

AP には電源アダプタ、もしくは PoE にて給電を行うことができます。
＊モデルによって起動に必要な電力が違います。詳しくはアクセスポイントのデータシート等を確認ください。

3.3 コンソールケーブルを用いての IP アドレス設定

コンソールケーブルは AP の製品により異なります。コンソールケーブルは同梱されておらず別売りとなっておりますので、ご注意ください。
① ターミナルソフト設定
Baud rate:9600，Data:8bit，Parity: none，Stop:1bit，Flow control: none に設定をし、電源が入っていない AP にコンソールケーブルを接続します。

② 電源の投入
アダプタもしくは、PoE から AP に給電を行います。
③ Boot の停止
AP に IP アドレスを振るためには、Boot 途中で ”Hit <Enter> to stop autoboot:” が表示されますので、このメッセージが出たら Enter を押し Boot を停止させます。プロンプトが ”apboot>”になることを確認ください。



このメッセージが出たら Enter を押します。

＊”Hit <Enter> to stop autoboot:”は電源投入後、3，4 秒で表示されます。

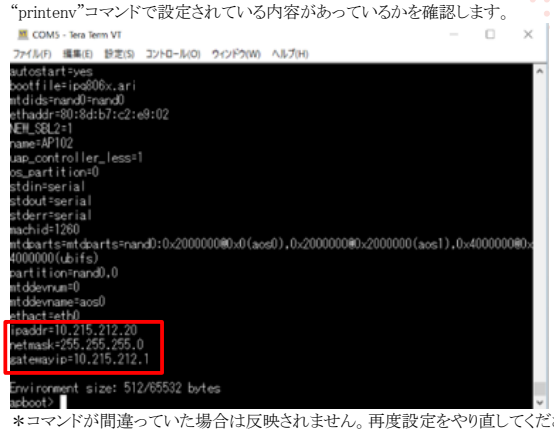
④ IP Address/Subnet Mask/Default Gateway/DNS の設定

下記のコマンドで IP Address/Subnet Mask/Default Gateway を指定します。

- setenv ipaddr <ip アドレス>
- setenv netmask <netmask>
- setenv gatewayip <default gateway アドレス>
- setenv dnsip <DNS Server アドレス>

⑤ 設定内容の確認

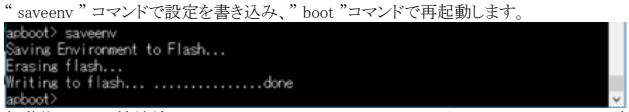
“printenv”コマンドで設定されている内容があっているかを確認します。



＊コマンドが間違っていた場合は反映されません。再度設定をやり直してください。

⑥ 設定内容の保存・起動

“ saveenv ” コマンドで設定を書き込み、” boot ”コマンドで再起動します。



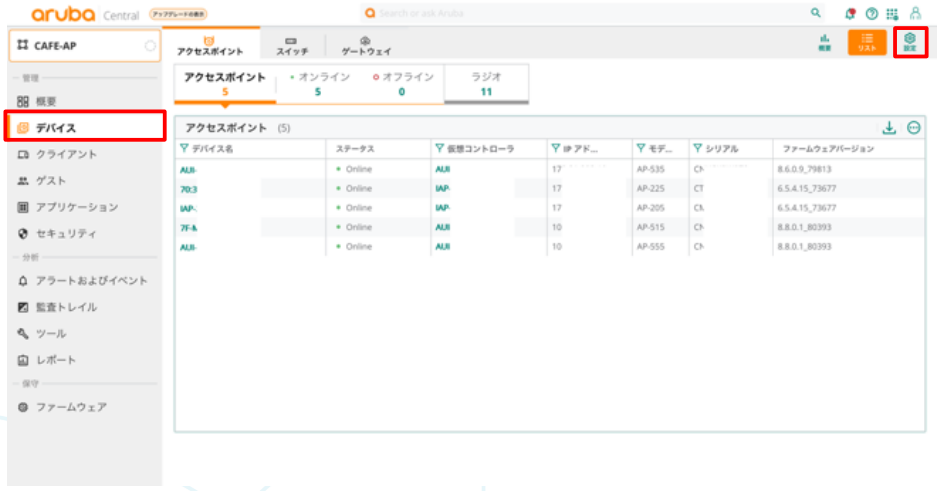
起動後 Central 接続前は User:admin Password:AP のシリアルナンバーで入り、Central 接続後は User:admin Password:Central のグループで設定したパスワード”でログイン後、“show ip interface brief ”で設定した内容が反映されていることが確認できます。

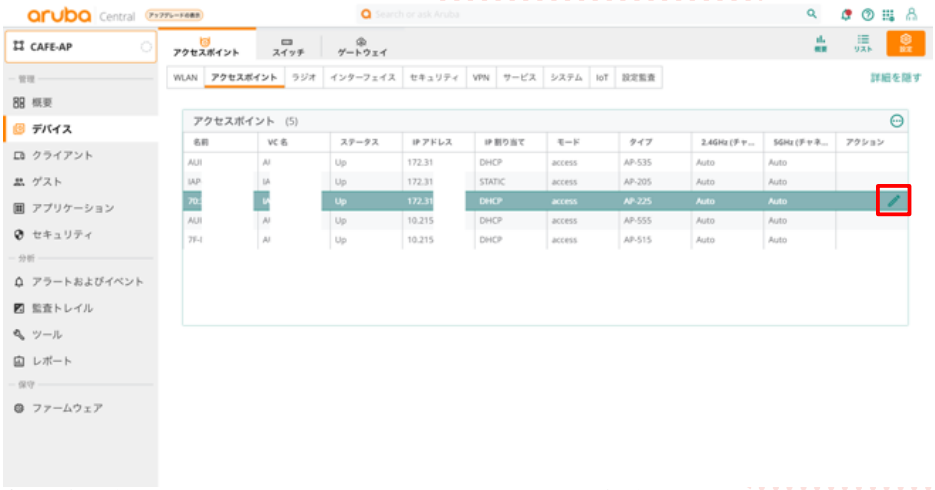
4 AP 基本設定

4.1 各 AP の AP 名・IP アドレス設定

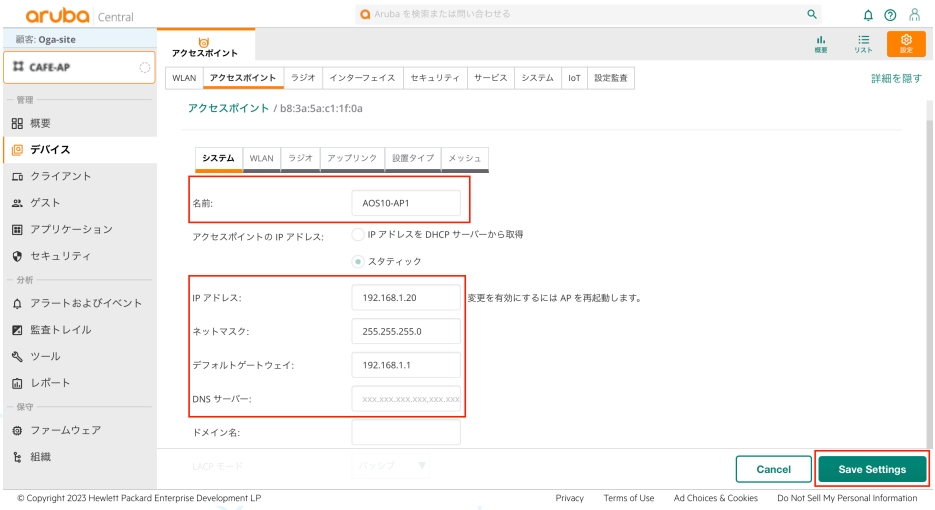
① フィルターからグループを選択

② デバイスメニューを選択し、右上に表示されるギアマークをクリックして、設定変更画面へ移動し、該当の AP を選択して右に表示される鉛筆マークをクリック

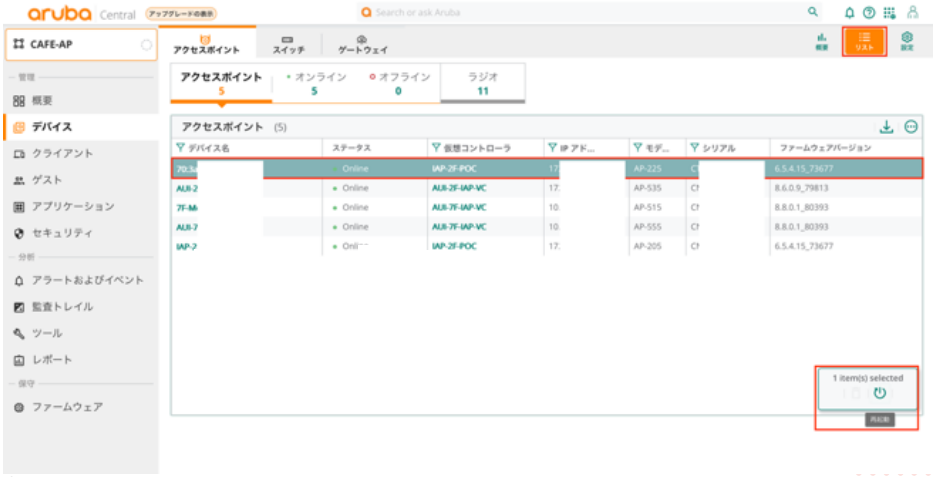




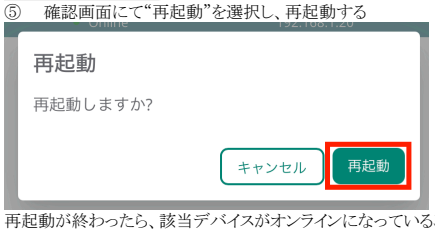
③　名前を編集し、アクセスポイントの IP アドレスをスタティックで設定し、”設定の保存”ボタンをクリック
＊アドレスを変更した場合は再起動が促されます。自動で再起動は行われません。



④ 再起動するため右上のリスト表示アイコンをクリックして、デバイス一覧に戻る。
AP 名、IP アドレスの変更をしたデバイスを選択すると“再起動”タブが表示されるため、それをクリックして再起動する



⑤ 確認画面にて“再起動”を選択し、再起動する



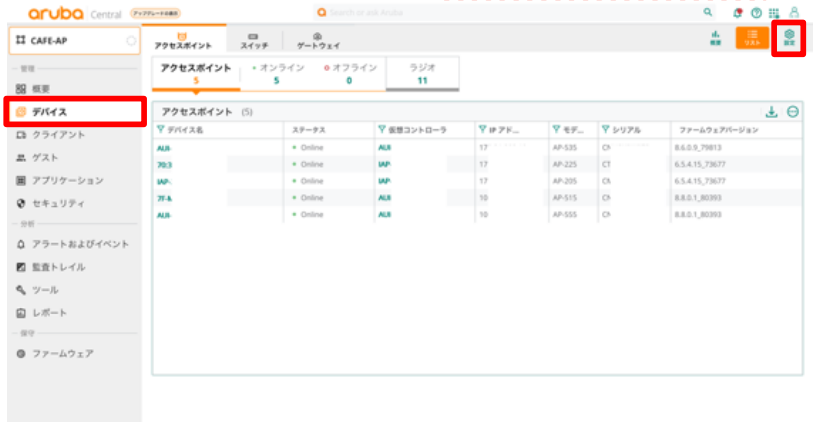
再起動が終わったら、該当デバイスがオンラインになっていることを確認し、AP 名と IP アドレスが変更されていることをご確認ください。

4.2 NTP 設定

AP はデフォルトで pool.ntp.org と時刻同期をします。他の任意の NTP サーバと時刻同期を行う場合に設定を行います。不具合発生をした場合には他機器とのログ比較を行う必要が出てきますので、設定していただくことを推奨いたします。

① フィルターよりグループを選択

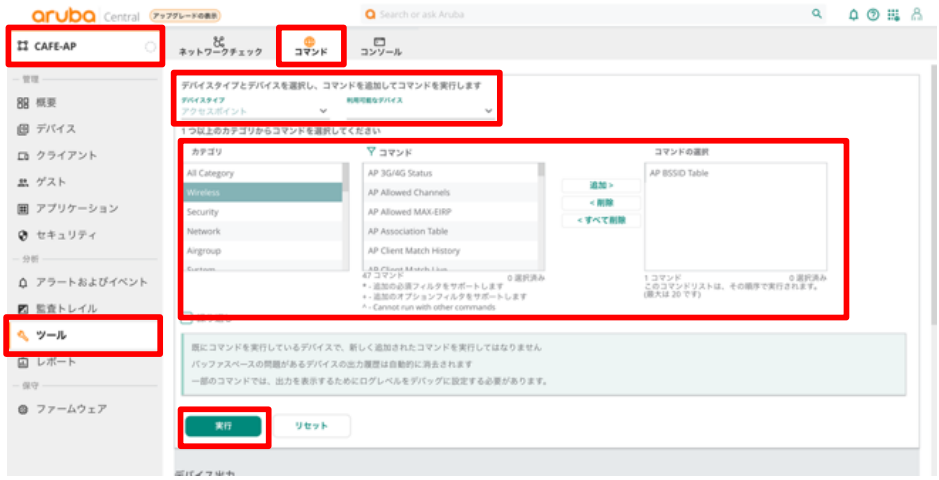
② 左メニューよりデバイスを選択し、右上の ⚙ をクリック



③ 右側にある“詳細を表示”をクリックし、“システム”タブを選択
NTP サーバーのアドレスを入力し、タイムゾーンは“Tokyo UTC +09”に変更し、“設定の保存”ボタンをクリック

4.2.1 時刻同期の確認1（GUI）

① グループを選択後、メニューから“ツール”を選択し、“コマンド”タブをクリック
デバイスタイプとデバイスを選択してから、適当なコマンドを選んで“実行”をクリック
実行結果の時間から時刻が同期されていることを確認



4.2.2 時刻同期の確認2（GUI コンソール）

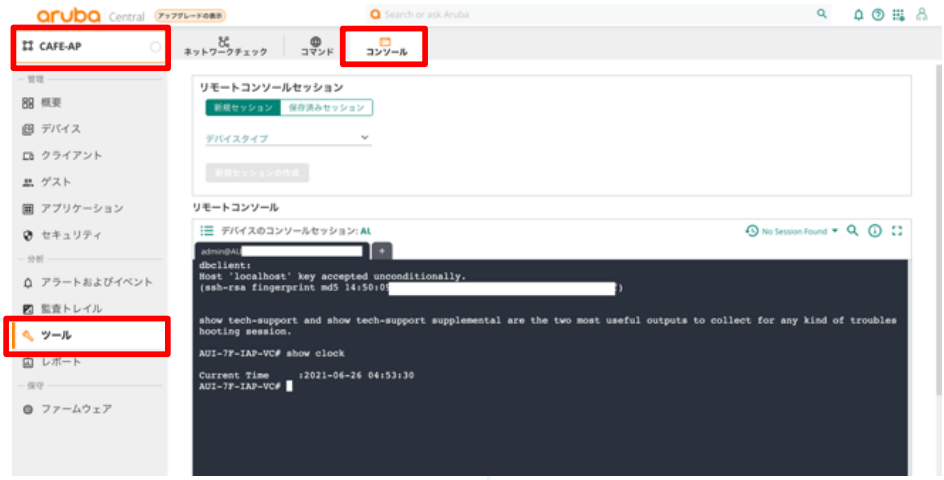
Central では GUI から AP のコンソールが開けます。

① グループを選択後、メニューから“ツール”を選択し、“コンソール”タブをクリック

② コンソールを開きたいデバイスタイプ・デバイス名・ユーザー名・パスワードを入力して“新規セッションの作成”をクリック

※Central 管理のデバイスのユーザー名・パスワードは基本的に、admin/グループのパスワード になります。

コンソールで“show clock”で時刻を確認

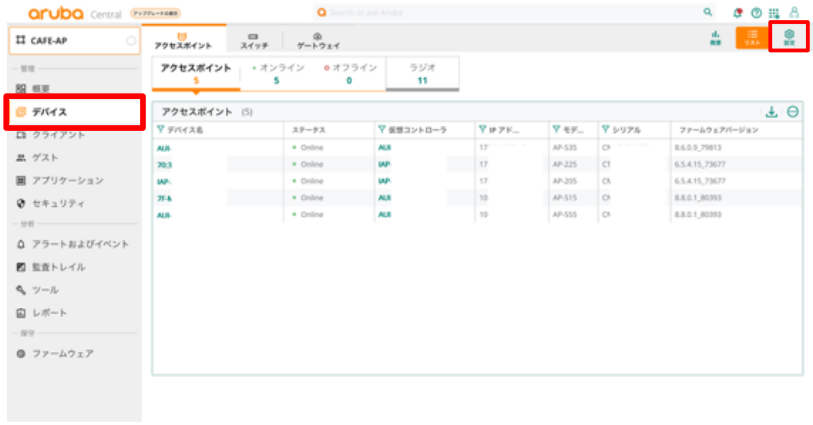


4.3 AppRF

AppRF を有効にすることで、Instant AP を通過するパケットから利用しているアプリケーションを特定することが可能になります。SSID のアクセスルールと組み合わせることにより、特定のアプリケーションに対して QoS を付与や、拒否することが可能となります。必要によって設定を行ってください。

① フィルターよりグループを選択

② 左メニューより“デバイス”を選択し、右上の ⚙ をクリック



③　“詳細を表示”をクリックし、サービスタブをクリック
　　“AppRF”から“詳細なパケット検査”ですべてを選択し、“アプリケーションのモニタリング”を有効にして“設定の保存”をクリック

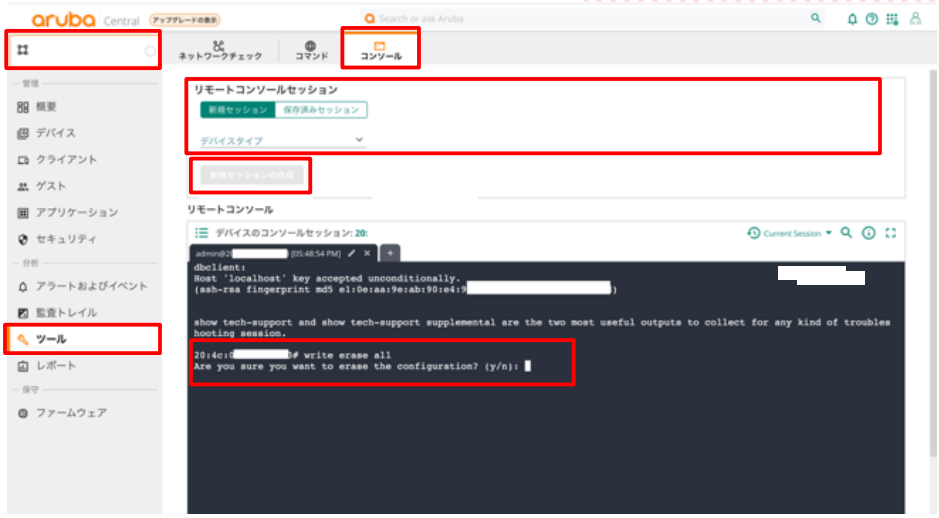
4.4 工場出荷状態への戻し方

4.4.1 グループを使った AP の初期化

設定の入っていない新規グループを作成し、AP を作ったグループに移すことで設定の初期化をします。
グループの作り方と AP の割り当てについて詳しくは Central 設定入門ガイドを参照してください。
https://www.arubanetworks.com/ja/resource/aruba-central-basic-operation-technical-guide/

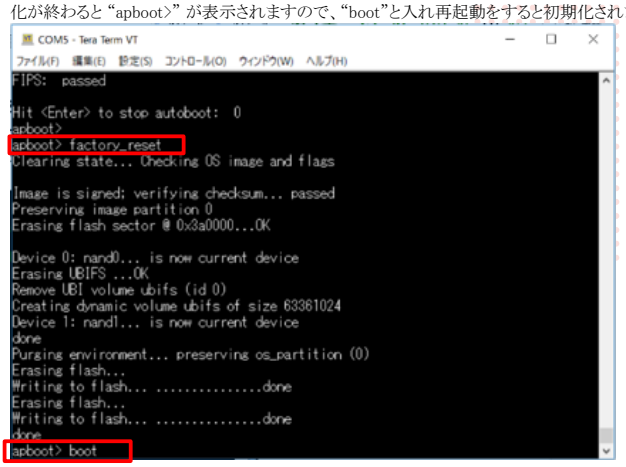
4.4.2 リモートコンソールからの初期化

GUI から AP の CLI にリモート接続ができます。
① グループを選択し、ツールメニューをクリックし、コンソールタブをクリック
② CLI を開く AP を選択し、ユーザ名・パスワードを入力して“新規セッションの作成”をクリック
③ CLI が起動したらログイン後 “write erase all” を実行し初期化する



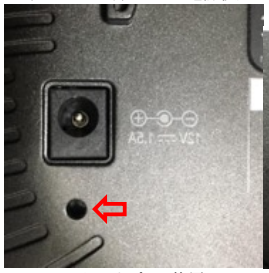
4.4.3 CLI からの初期化

Instant AP の電源の OFF/ON を行います。Boot 途中で “Hit <Enter> to stop autoboot:” が表示されますので、このメッセージが出たら Enter を押し Boot を停止させます。プロンプトが ”apboot>”になった後、“factory_reset” コマンドを入れます。コンフィグの初期化が終わると “apboot>” が表示されますので、“boot”と入れ再起動をすると初期化されます。



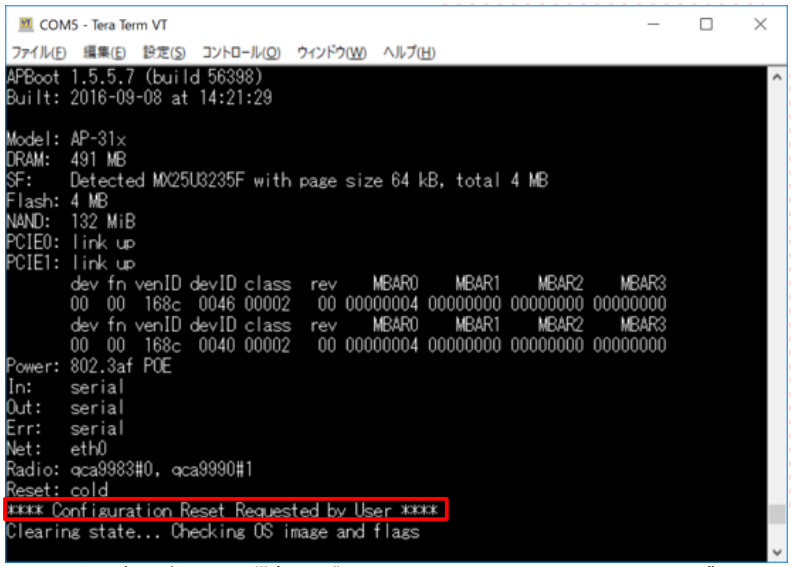
4.4.4 リセットボタンからの初期化

全ての Instant AP にはリセットボタンがついています。
リセットボタンを押しながら電源投入し、約 5 秒後リセットボタンをはなすことで初期化を行うことができます。



IAP-315 リセットボタン位置

AP-345 リセットボタン位置



コンソールケーブルで確認している場合には、“**** Configuration Reset Requested by User **** ”のメッセージが出るまで、リセットボタンを押し続けてください。

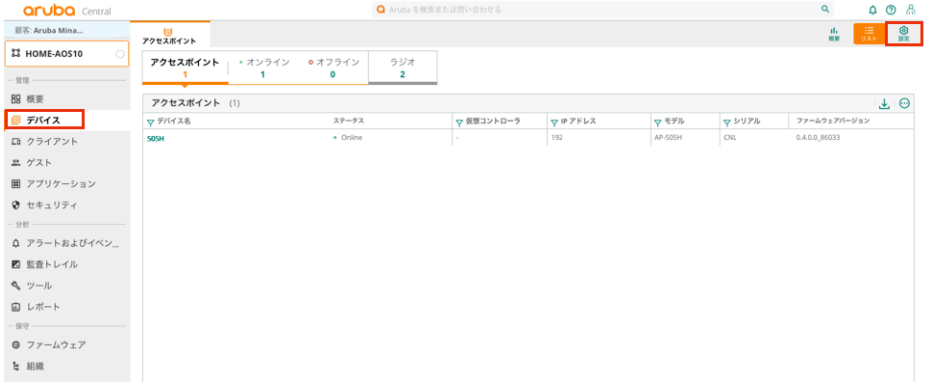
5　有線ポート設定

コメントの追加 [OY1]: 南くん担当スタート

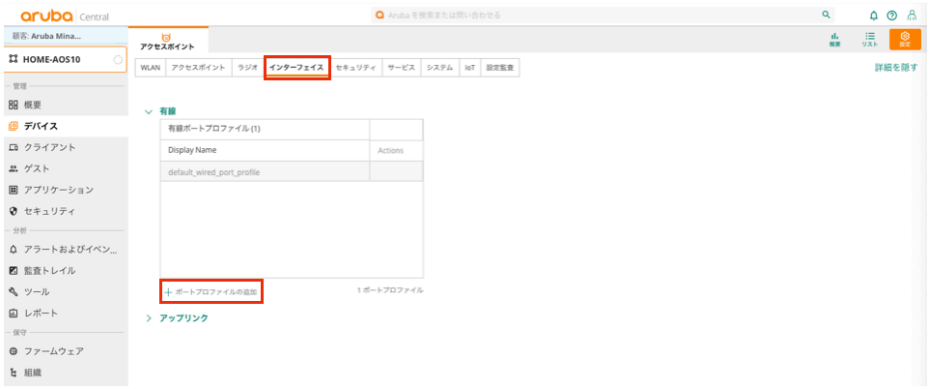
有線 Port は設定をしなければ利用することができません。本設定では有線ポートを L2SW として利用する方法を紹介します。

①　フィルターよりグループを選択

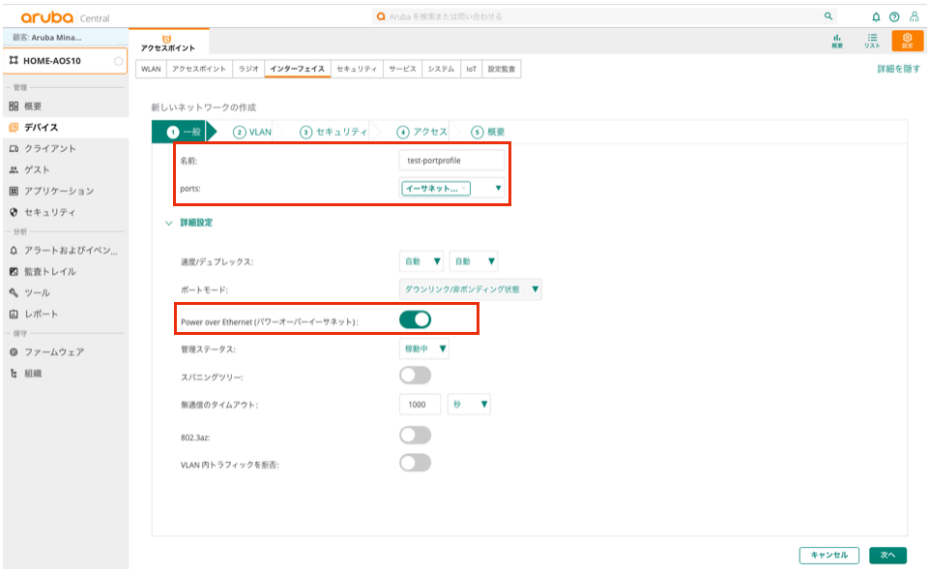
②　左メニューよりデバイスを選択し、右上の ⚙ をクリック



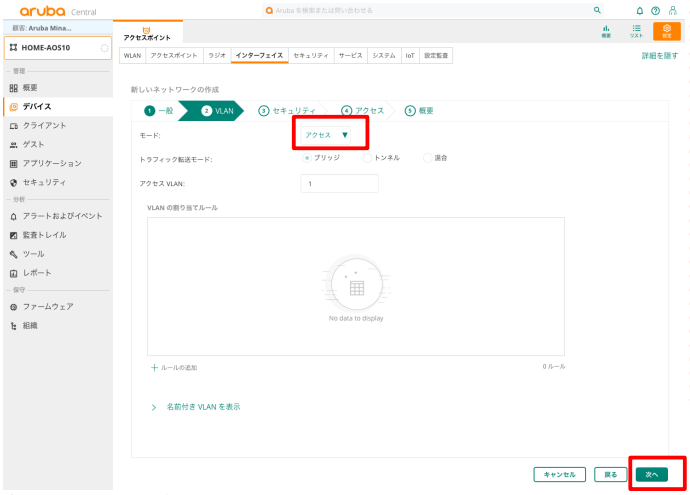
③ “詳細を表示”をクリックし、インターフェイスタブをクリック
“＋ポートプロファイルの追加”から新規ポートプロファイルを作成



④ 名前は任意のものを設定し、当インターフェイスプロファイルを割り当てるポートを選択
＊PoE 給電を行うことが可能な有線ポートを持つ AP もあるので、必要によって詳細設定を開き、PoE を”有効”と設定します。IP Phone や IP Camera に給電を行うことができます。
“次へ”をクリック



⑤　モードをアクセスにし、“次へ”をクリック



⑥　Trusted ポートを有効にします。Trusted ポートを無効にすると、MAC 認証、802.1x 認証を有効にすることができる
“次へ”をクリック

⑦ Trusted ポートを有効としたため、アクセスルールは制限なしになる
“次へ”をクリック

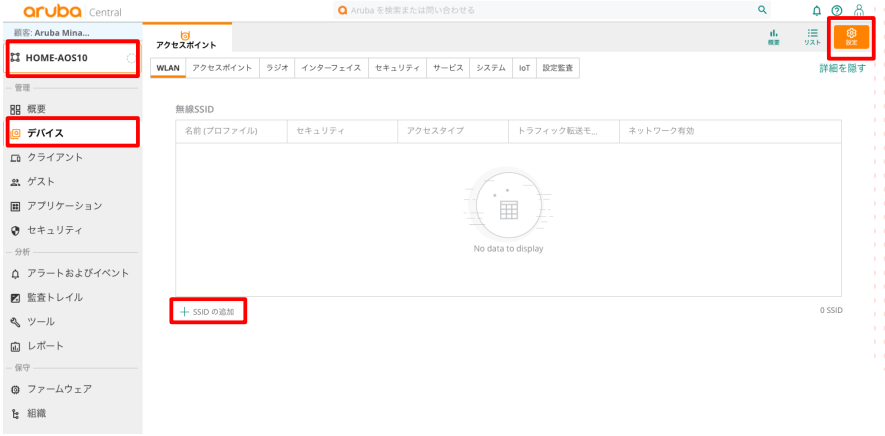
⑧ 概要を確認し、間違いがなければ“終了”をクリック

6 SSID の設定

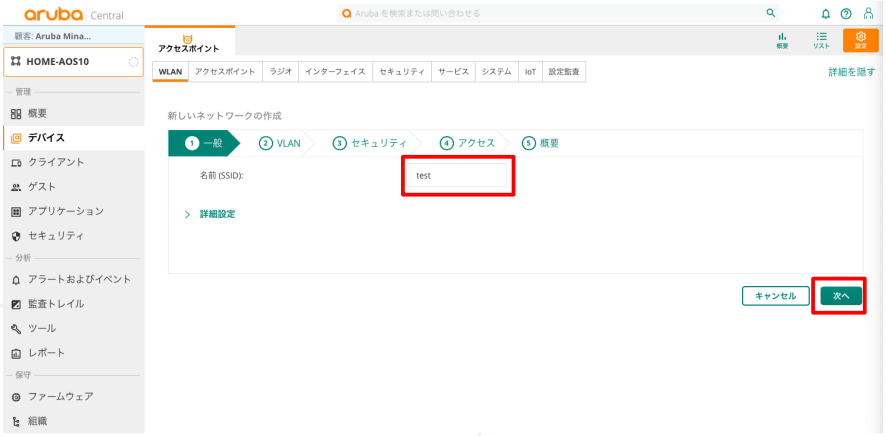
6.1 SSID の作成手順

基本的な SSID の作成フロー
① フィルターアイコンより SSID を作成するグループを選択

② 左メニューより“デバイス”を選択し、右上の ボタンをクリック
③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成



④ 名前(SSID)を指定し、“次へ”をクリック



⑤　トラフィック転送モードとクライアント VLAN の割り当て設定をする

トラフィック転送モード

”ブリッジ”→AP はブリッジとして動作を行い、トラフィックは接続先スイッチに転送されます。ネイティブ VLAN もしくは、接続先スイッチに設定された VLAN を指定します。

”トンネル”→トラフィックはトンネル経由でゲートウェイに転送されます。ゲートウェイに設定された VLAN を指定します。(GRE トンネルによる L2 延伸)

”混合”→ルールに基づいてフォワーディング・モード(Bridge もしくは Tunnel)と VLAN をクライアントに割り当てます。ルールには MAC アドレスやユーザー名等を指定可能です。

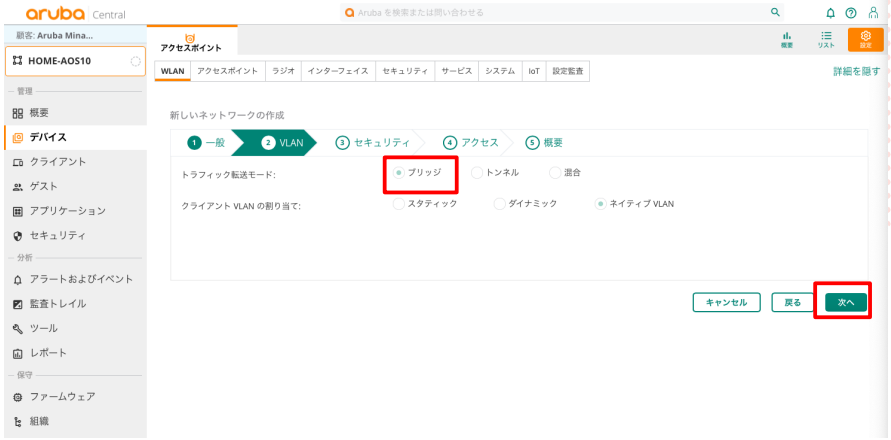
コメントの追加 [YM2]: トラフィック転送モードを追記

クライアント VLAN の割り当て

“ネイティブ VLAN” → VLAN との紐付けをせず、AP が属するネットワークに出力されます。

“スタティック” → 指定をした VLAN と紐付けます。有線側には指定した VLAN Tag がついて出力されますので、AP と接続している Switch 側で Tag VLAN 設定をしてください。

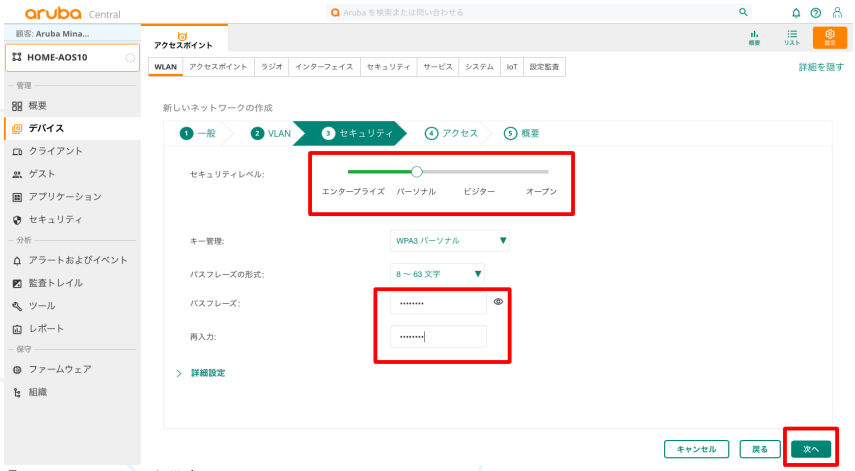
“ダイナミック” → Radius Attribute の利用や、特定文字列等をトリガーにして Dynamic VLAN を行うことができます。有線側には指定した VLAN Tag がついて出力されますので、AP と接続している Switch 側で Tag VLAN 設定をしてください。



⑥　セキュリティレベルを設定

エンタープライズ WPA(2,3) Radius 利用/パーソナル WPA(2,3)-PSK/キャプティブポータル(web 認証)/オープン(暗号化なし)の設定を行う

エンタープライズ-内蔵 Radius 利用については、この画面からでもユーザ追加を行うことができる



⑦　アクセスルールを設定

ロールベース/ネットワークベース/制限なし　のアクセス制御を設定する

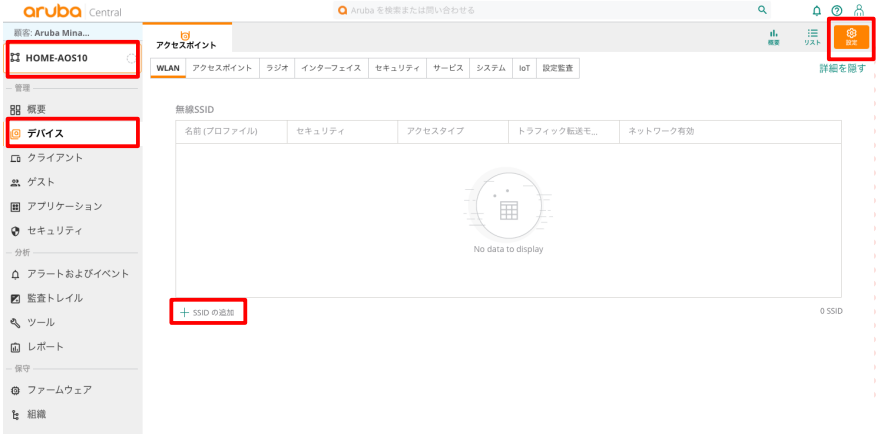
⑧　概要で設定内容に間違いなければ“終了”ボタンをクリックすると、SSID が作成され、しばらくしてから Instant AP から SSID が出力し始める

6.2 設定例)オープン認証(暗号/認証なし)

① フィルターアイコンより SSID を作成するグループを選択

② 左メニューより“デバイス”を選択し、右上の ボタンをクリック

③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成



④ 任意の SSID を設定します。本設定では“OPEN”という SSID とし、“次へ”をクリック

⑤　SSID と VLAN との紐付けを行う
本設定ではトラフィック転送モードは“ブリッジ”、SSID=OPEN と VLAN10 を紐付けるため”スタティック” を選択し、VLAN ID に ”10 ” を入力します。
VLAN は“名前つき VLAN を表示”から新規作成可能

⑥　暗号なし・暗号なし設定となるため セキュリティーレベルにて”オープン”を選択

⑦ 本設定では、アクセスルール制限をしないため、”制限なし”を選択

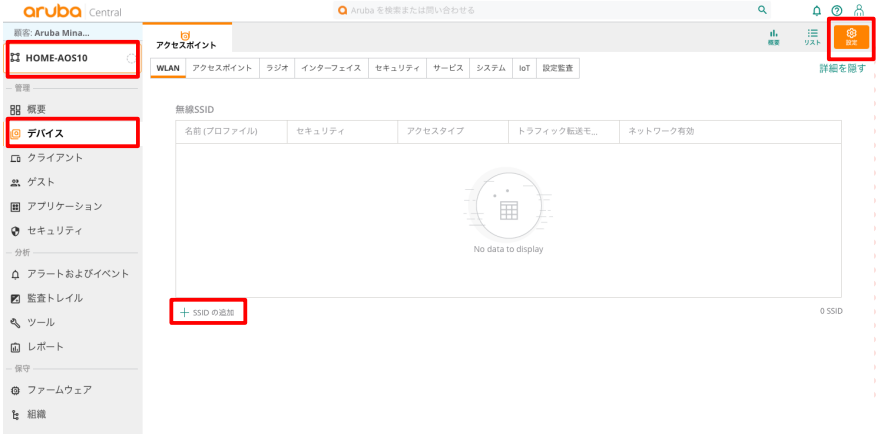
⑧ 概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=OPEN が作成され、全ての Instant AP から出力される

6.3 設定例）WPA3-PSK

① フィルターアイコンより SSID を作成するグループを選択

② 左メニューより“デバイス”を選択し、右上の ボタンをクリック

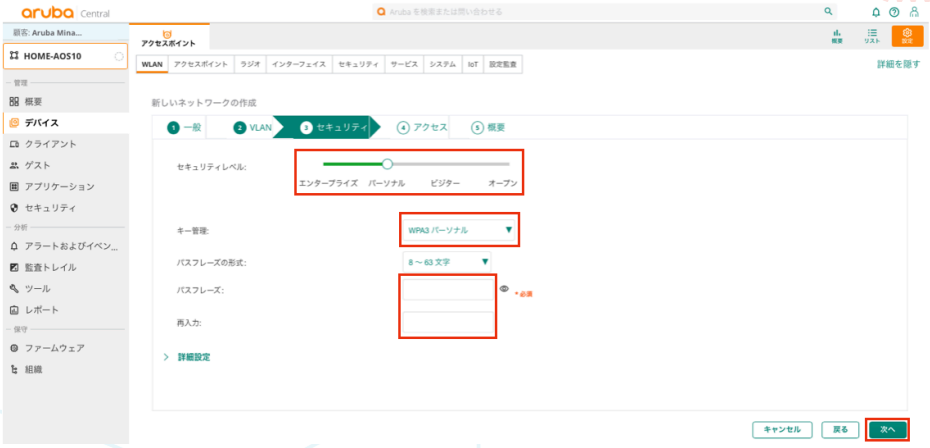
③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成



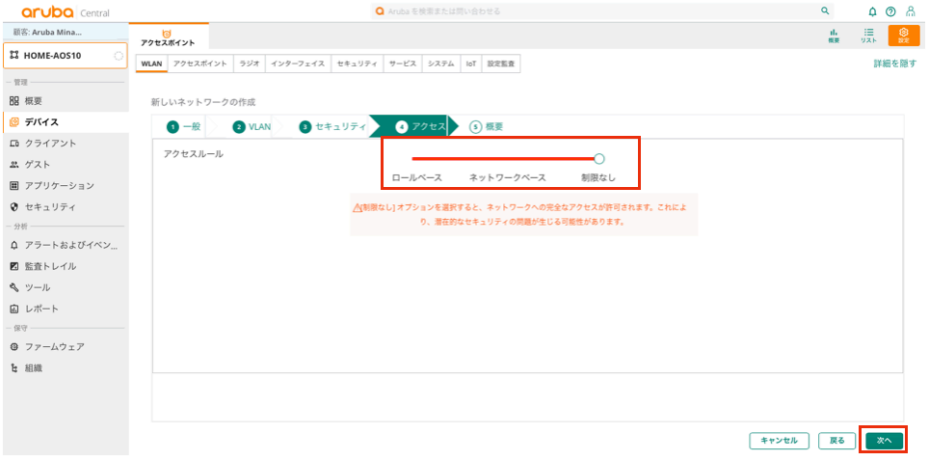
④ 任意の SSID を設定します。本設定では“WPA3-PKS”という SSID とし、“次へ”をクリック

⑤ SSID と VLAN との紐付けを行う
本設定では、トラフィック転送モードを“ブリッジ”、SSID=WPA3-PSK と VLAN20 を紐付けるため”スタティック” を選択し、VLAN ID に ”20 ” を入力
VLAN は“名前つき VLAN を表示”から新規作成可能

⑥ セキュリティーレベルにおいて、”パーソナル”を選択
パスフレーズ(8 文字以上)を入力



⑦ 本設定では、アクセスルール制限をしないため、”制限なし”を選択



⑧ 概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=WPA3-PSK が作成され、全ての Instant AP から出力される

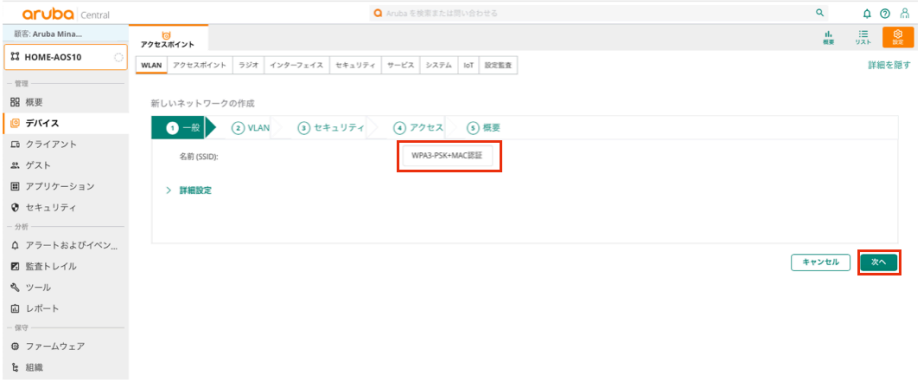
6.4 設定例）WPA3-PSK＋MAC 認証(Cloud Auth)

① フィルターアイコンより SSID を作成するグループを選択

② 左メニューより“デバイス”を選択し、右上の ボタンをクリック

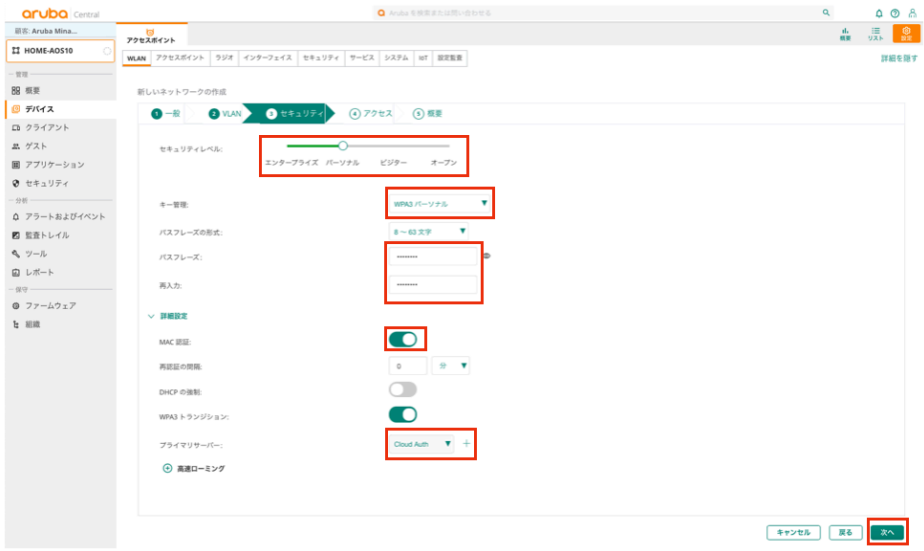
③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成

④ 任意の SSID を設定します。本設定では“WPA3-PKS＋MAC 認証”という SSID とし、“次へ”をクリック

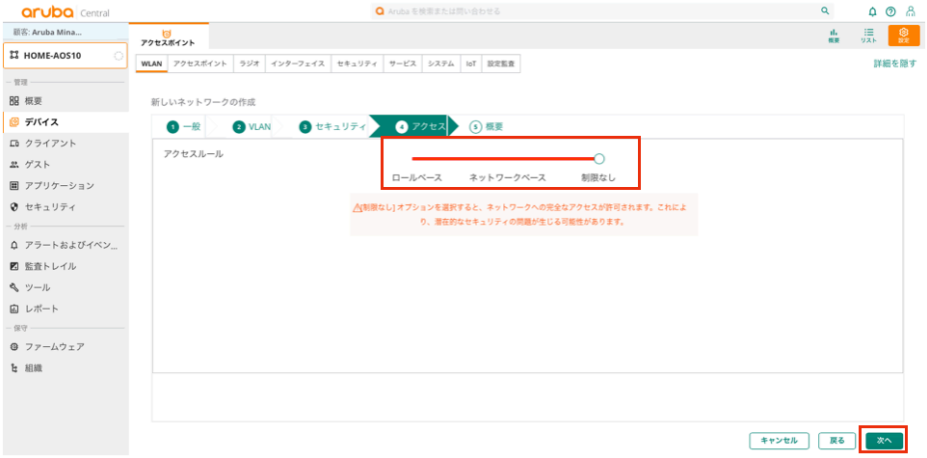


⑤ SSID と VLAN との紐付けを行う
本設定ではトラフィック転送モードを“ブリッジ”、SSID=WPA3-PSK＋MAC 認証と VLAN30 を紐付けるため”スタティック” を選択し、VLAN ID に ”30 ” を入力
VLAN は“名前つき VLAN を表示”から新規作成可能

⑥ セキュリティーレベルにおいて、”パーソナル”を選択
パスフレーズ(8 文字以上)を入力
PSK を入力した後、詳細設定を開き MAC 認証を”有効”
MAC 認証を有効にすると、認証サーバ項目が表示されるようになる
今回は“Cloud Auth”を選択　Cloud Auth の概要についてはこちらをご参照ください。
右の+ボタンから新規認証サーバを登録可能



⑦ 本設定では、アクセスルール制限をしないため、”制限なし”を選択



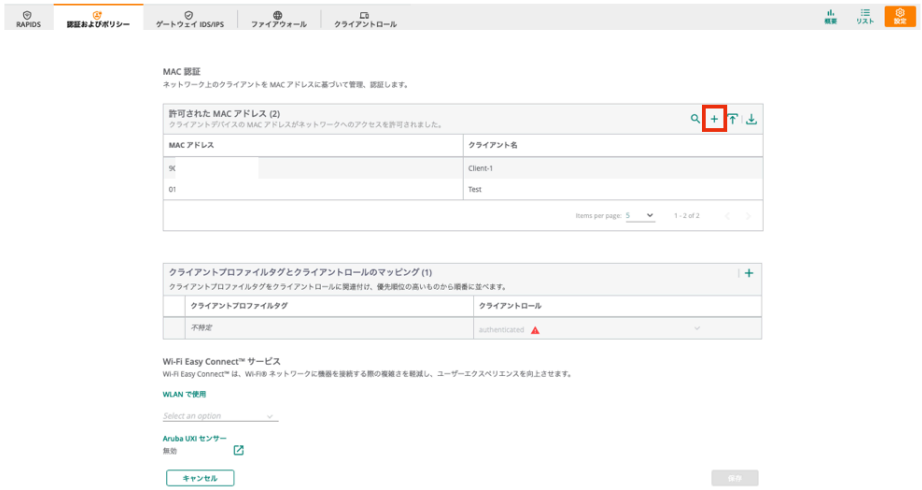
⑧ MAC アドレスの登録

Aruba Central 側に MAC アドレスを登録します。

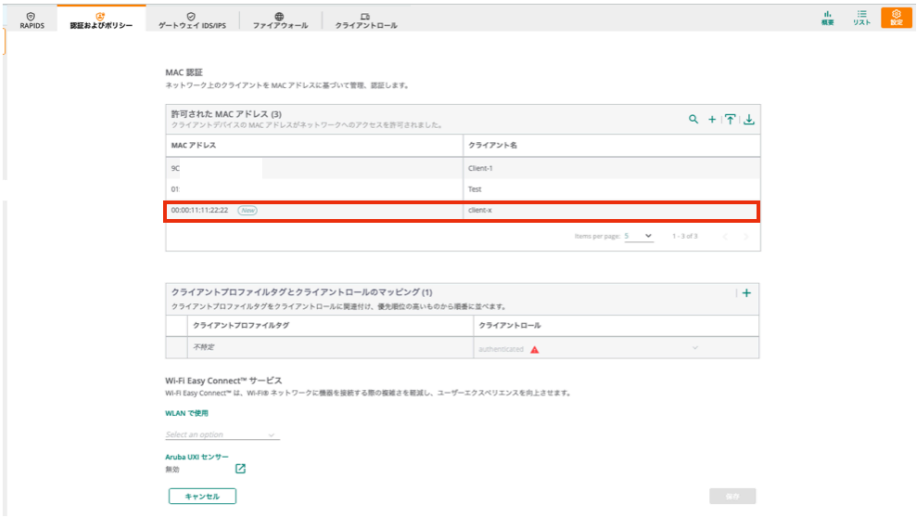
“グローバル”レベルの階層から“セキュリティ”→“認証およびポリシー”を選択

“設定”をクリックして“クライアントアクセスポリシー”の編集ボタンをクリック

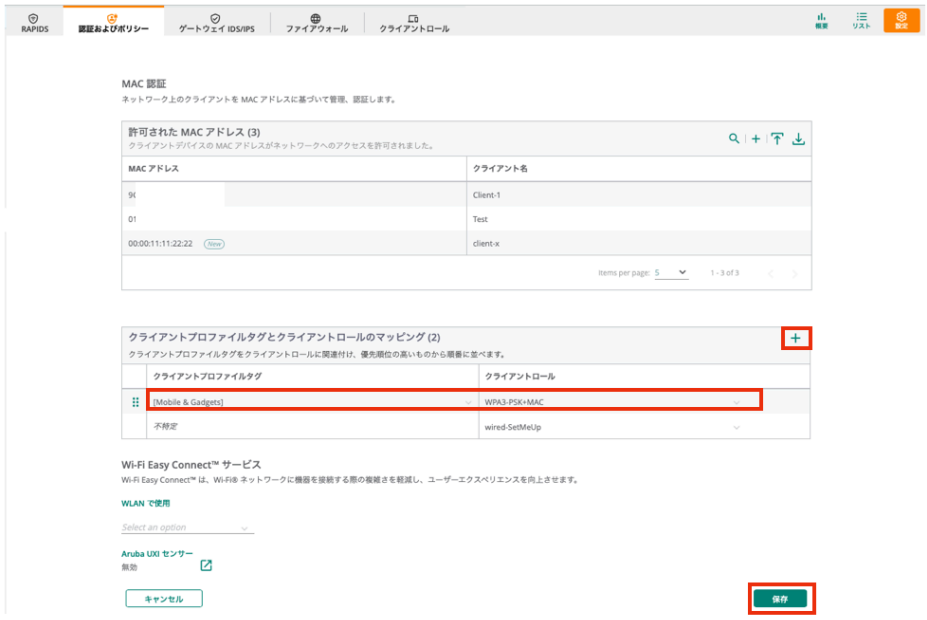
⑨ ＋ボタンから MAC アドレスを登録する



MAC アドレス一覧に追加されていることを確認する



⑩ クライアントプロファイルタグのマッピング＆クライアントロールのマッピング
クライアントプロファイルタグを“Mobile & Gadgets”（スマホ・タブレット等の場合）
クライアントロールを作成した SSID と同じ名前のロールに割り当てる



概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=WPA3-PSK+MAC が作成され、全ての AP から出力される

6.5 設定例）802.1x Cloud Auth 利用

① フィルターアイコンより SSID を作成するグループを選択

② 左メニューより“デバイス”を選択し、右上の ボタンをクリック

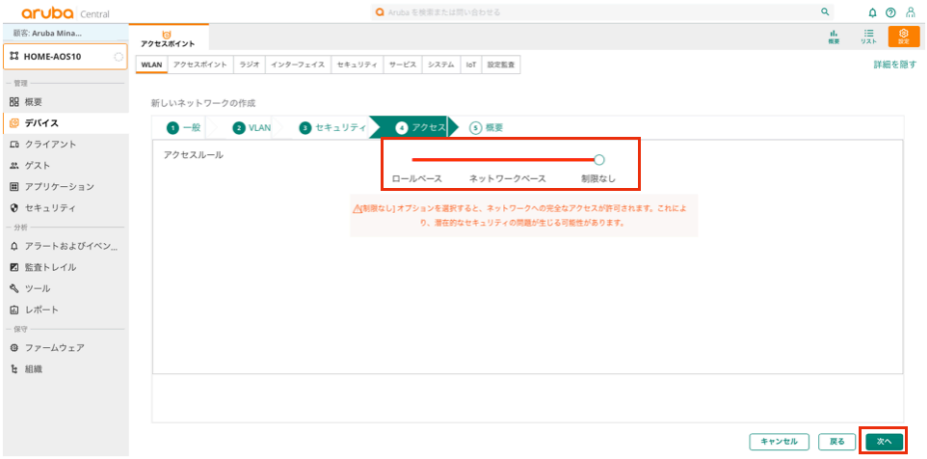
③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成

④ 任意の SSID を設定します。本設定では“Dot1x-CloudAuth”という SSID とし、“次へ”をクリック

⑤ SSID と VLAN との紐付けを行う
本設定では、トラフィック転送モードを“ブリッジ”、SSID=Dot1x-CloudAuth と VLAN40 を紐付けるため”スタティック” を選択し、VLAN ID に ”40 ” を入力
VLAN は“名前つき VLAN を表示”から新規作成可能

⑥ セキュリティーレベルにおいて、“エンタープライズ”を選択
プライマリーサーバー項目で“Cloud Auth”を選択

⑦ 本設定では、アクセスルール制限をしないため、“制限なし”を選択



概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID= Dot1x-CloudAuth が作成され、全ての Instant AP から出力される

⑧ Cloud Auth 認証ソース指定
“グローバル”レベルの階層から“セキュリティ”→“認証およびポリシー”を選択
“ユーザーアクセスポリシー”を選択して編集ボタンをクリックする

⑨ ID ストアの設定
ID ストアを Microsoft Azure AD に指定
（Microsoft Azure AD 側の設定は本稿では割愛させて頂きます）
テナント ID・クライアント ID・クライアント秘密キーを入力
“接続”をクリックする
正常に接続されている場合“接続済み”と表示されます

必要に応じてユーザーグループとロールのマッピングを設定します

6.6 設定例）802.1x External Radius 利用

コメントの追加 [OY3]: 南くん担当ゴール

① フィルターアイコンより SSID を作成するグループを選択

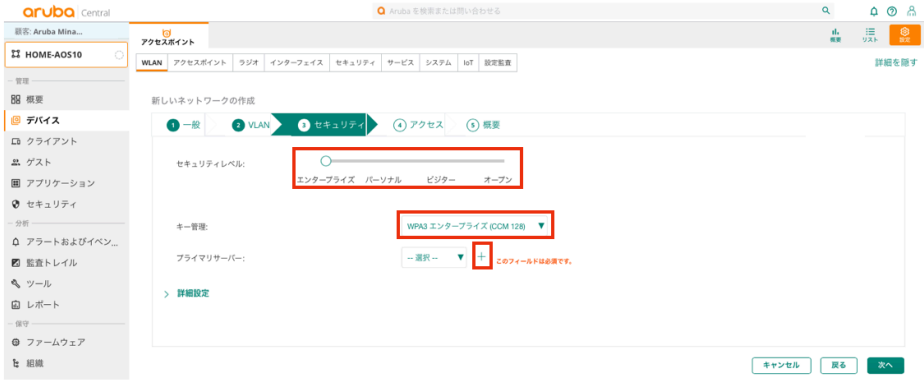
② 左メニューより“デバイス”を選択し、右上の ボタンをクリック

③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成

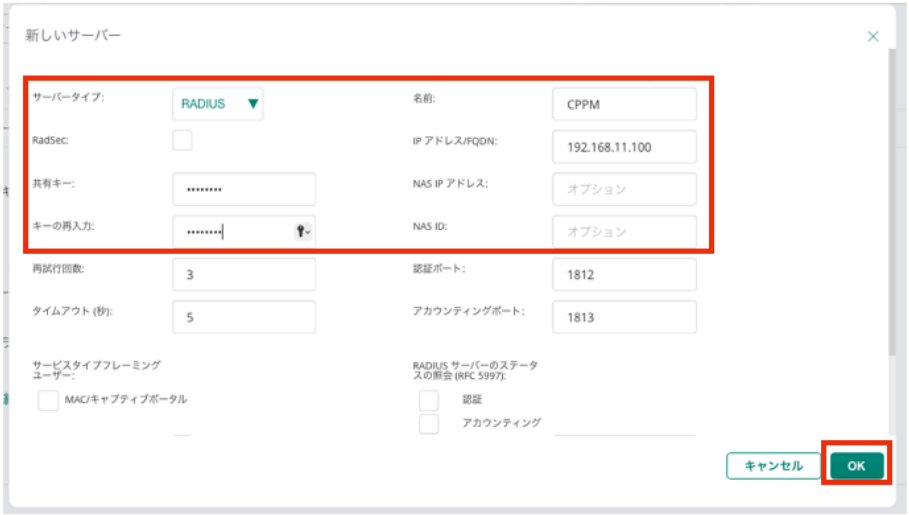
④ 任意の SSID を設定します。本設定では“Dot1x-external”という SSID とし、“次へ”をクリック

⑤ SSID と VLAN との紐付けを行う
本設定ではトラフィック転送モードを“ブリッジ”、SSID=Dot1x-external と VLAN50 を紐付けるため”スタティック” を選択し、
VLAN ID に ”50 ” を入力
VLAN は“名前つき VLAN を表示”から新規作成可能

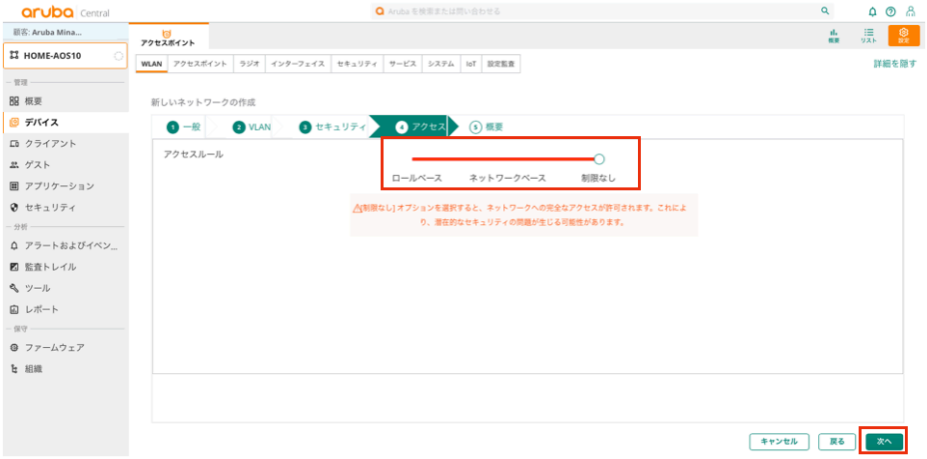
⑥ セキュリティーレベルにおいて、”エンタープライズ”を選択
プライマリーサーバー項目で“＋”から RADIUS サーバーを登録する



⑦ Radius サーバ名、IP アドレス、共有キー(シークレットキー)を入力し”OK”をクリック



⑧ 本設定では、アクセスルール制限をしないため、”制限なし”を選択



概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=Dot1x-external が作成され、全ての Instant AP から出力される

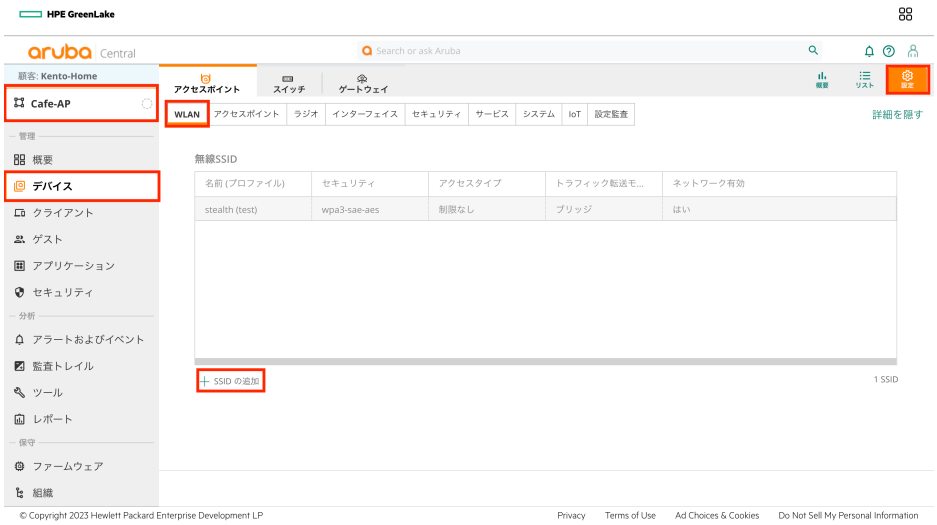
6.7 Dynamic VLAN（External Radius 利用）

コメントの追加 [OY4]: 横山くんスタート

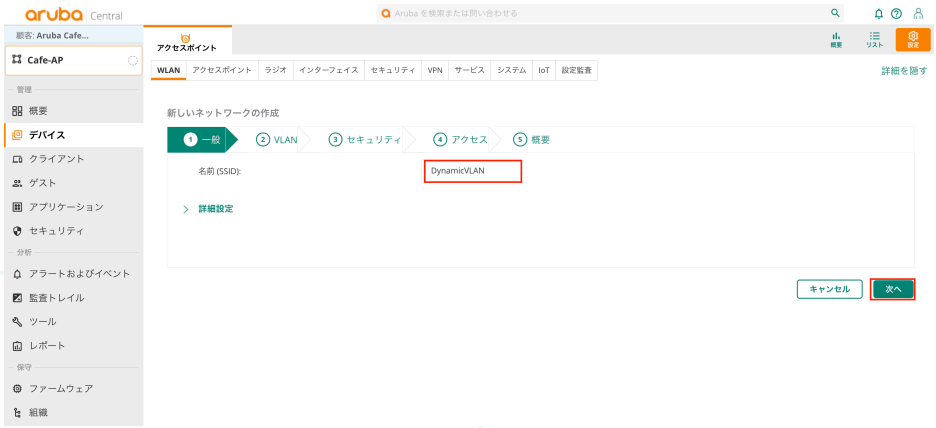
① フィルターアイコンより SSID を作成するグループを選択

② 左メニューより“デバイス”を選択し、右上の ボタンをクリック

③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成

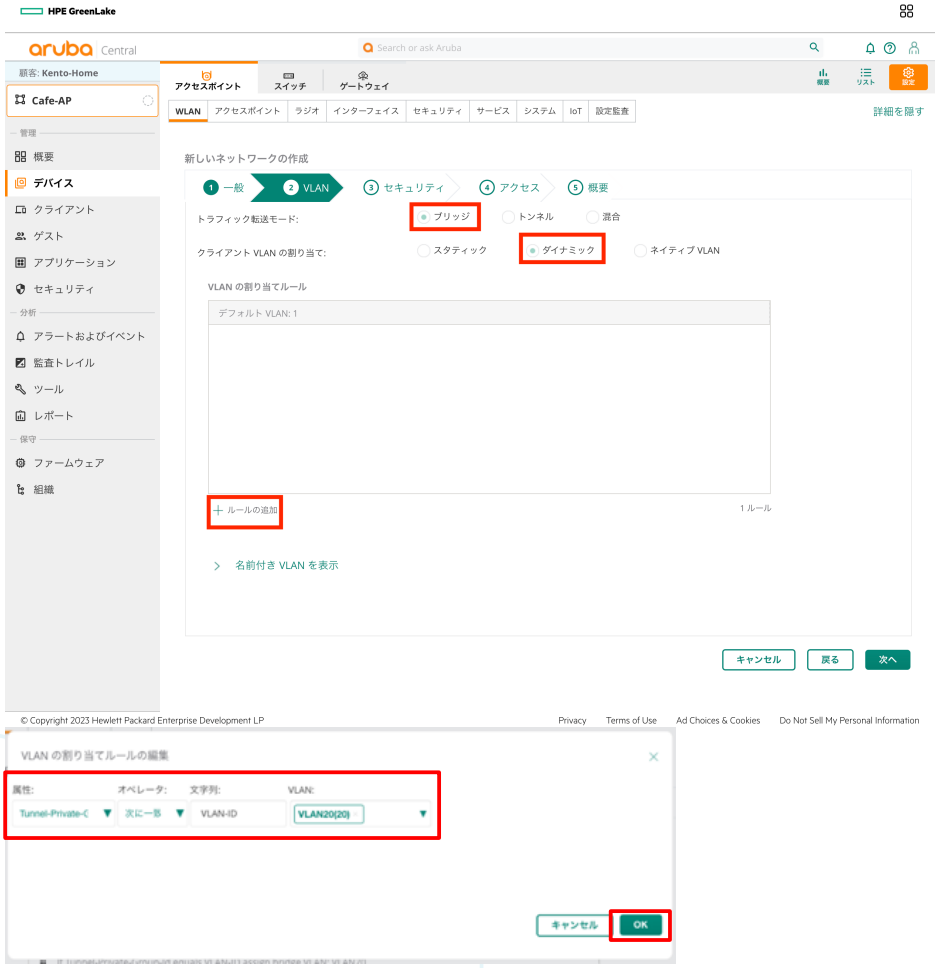


④ 任意の SSID を設定します。本設定では“DynamicVLAN”という SSID とし、“次へ”をクリック

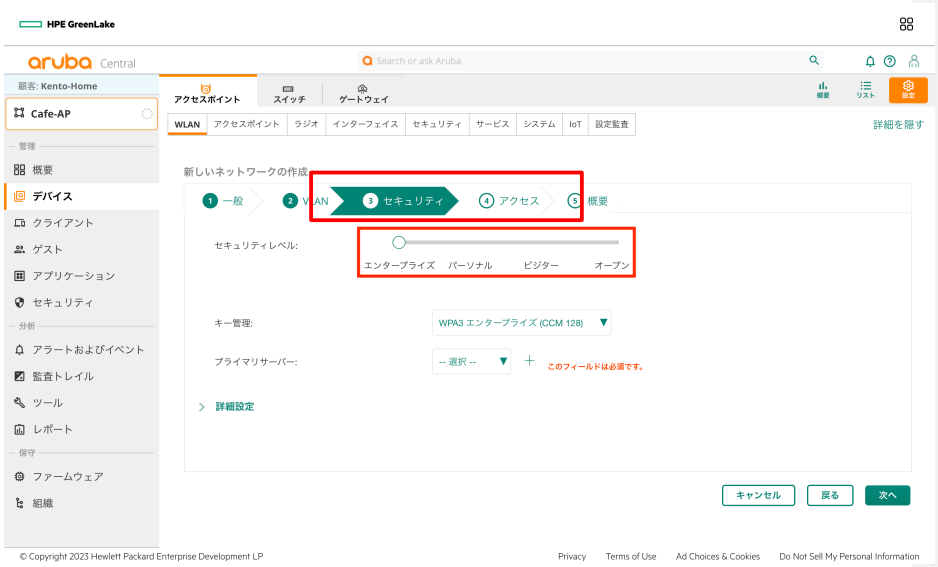


⑤　SSID と VLAN との紐付けを行う
Dynamic VLAN となるため、SSID との紐付けは行わず、Radius サーバからの情報で VLAN をアサインできるようにする
本設定では、一般的に利用される”Tunnel Private Group Id”を利用して VLAN を振り分けられるようにする

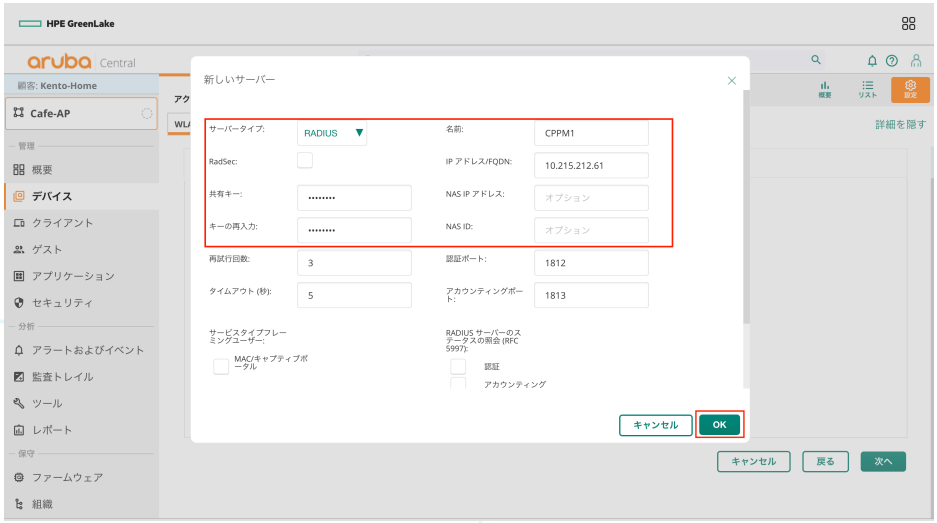
本設定ではトラフィック転送モードを“ブリッジ”、クライアント VLAN の割り当てにおいて、”ダイナミック”を選択
VLAN の割り当てルール欄の”+ルールの追加”ボタンをクリック
割り当てルールにおいて “属性” ＝ ”Tunnel-Private-Group-Id”，”オペレータ” = ”次に一致”，”文字列”=”VLAN-ID”，“VLAN” = ”VLAN-ID”で割り振られる VLAN を追加
デフォルトは作成したルールに合わなかった場合に付与される VLAN となる



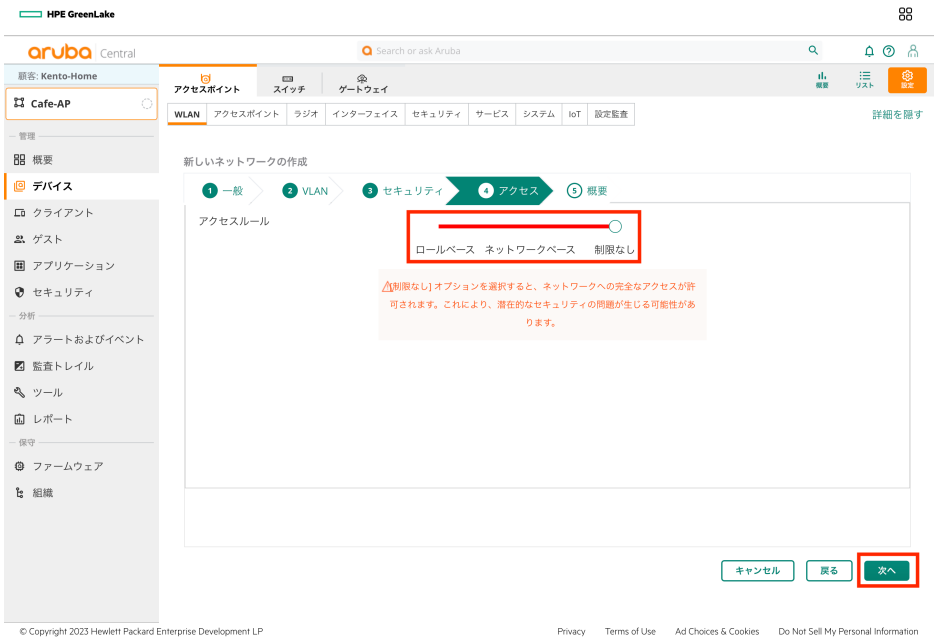
⑥ セキュリティーレベルにおいて、”エンタープライズ”を選択 10.215



⑦ プライマリーサーバー項目で”+ボタン”をクリック
“+”をクリックすると、Radius サーバを登録可能
Radius サーバ名、IP アドレス、共有キー（シークレットキー）を入力し”OK”をクリック



⑧　本設定では、アクセスルール制限をしないため、”制限なし”を選択



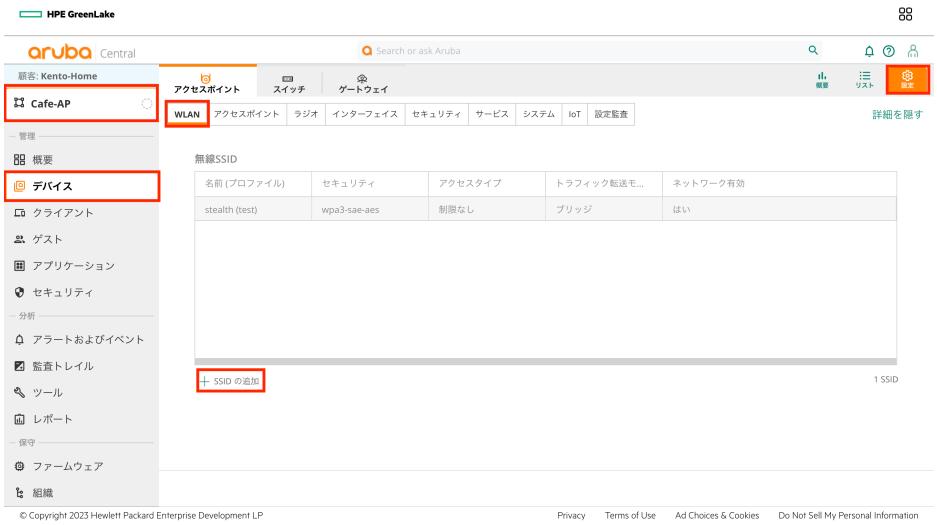
概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=DynamicVLAN が作成され、全ての Instant AP から出力される

6.8 設定例）クラウドゲスト

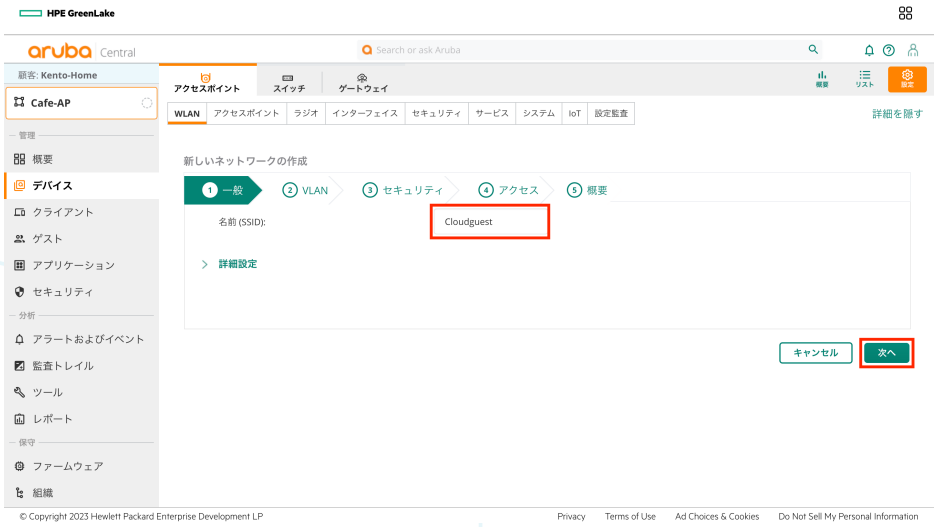
① フィルターアイコンより SSID を作成するグループを選択

② 左メニューより“デバイス”を選択し、右上の ボタンをクリック

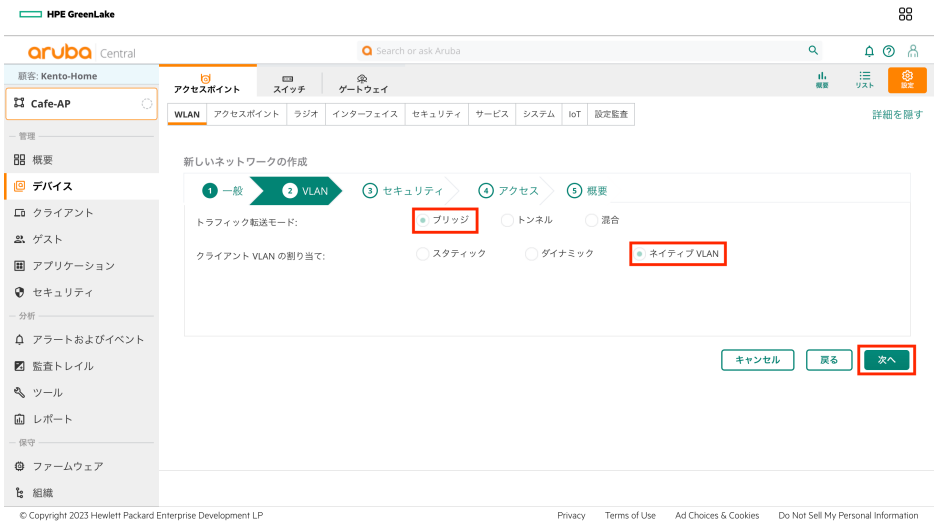
③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成



④ 任意の SSID を設定します。本設定では“Cloudguest”という SSID とし、“次へ”をクリック

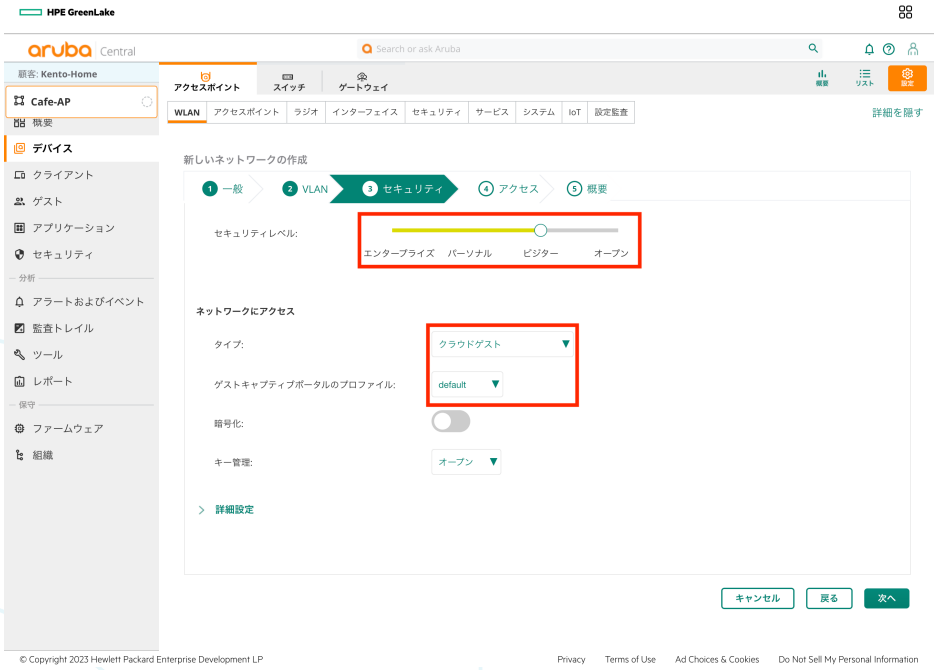


⑤ 本設定ではトラフィック転送モードを“ブリッジ”、クライアントVLANの割り当てにおいて、”ネイティブVLAN”を選択

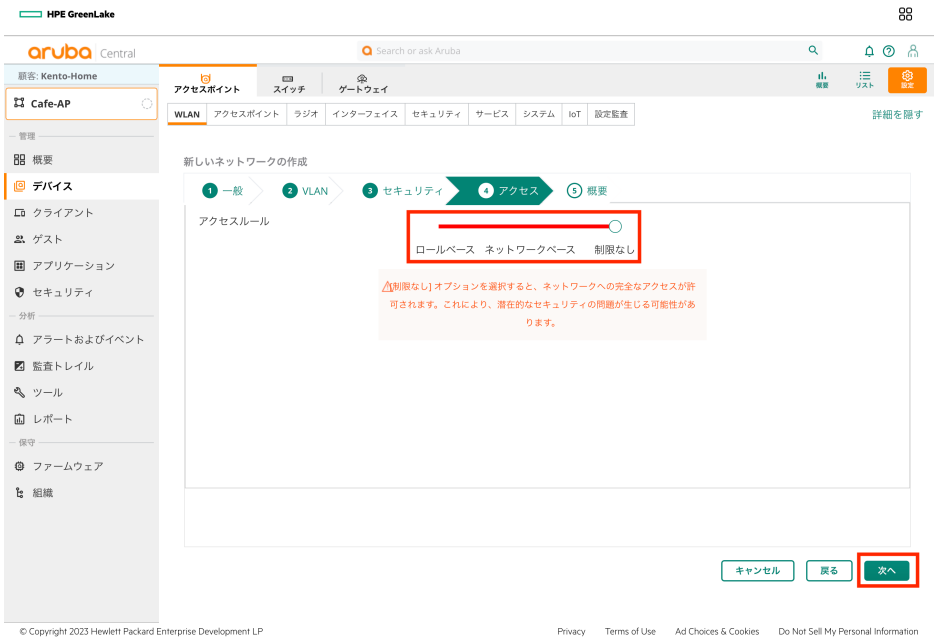


⑥ セキュリティーレベルにおいて、”ビジター”を選択

⑦ タイプにおいて”クラウドゲスト”、ゲストキャプティブポータルのプロファイルにおいて“default”を選択



⑧　本設定では、アクセスルール制限をしないため、”制限なし”を選択



概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=Cloudguest が作成され、全ての AP から出力される

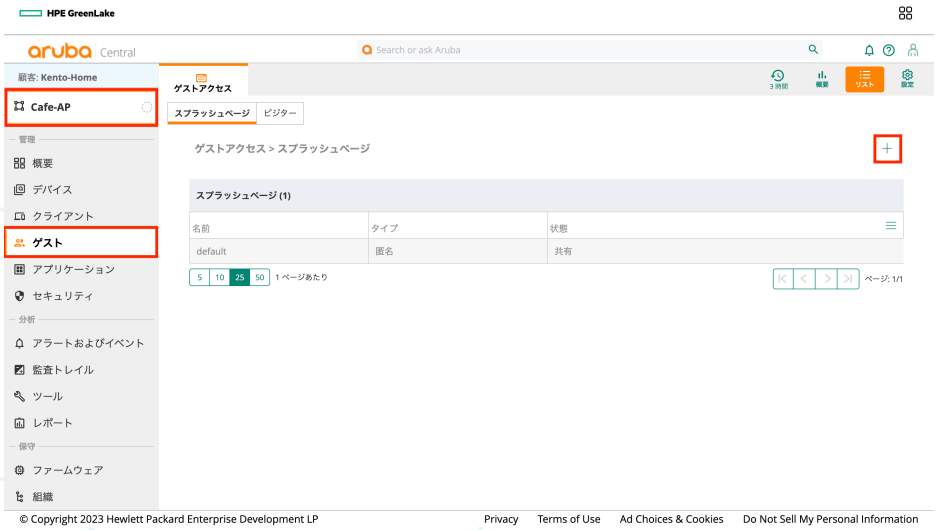
6.9 Central ゲスト(メール認証)

Central のゲスト機能を追加すると、ゲスト wi-fi 作成時に以下のような認証方式が利用できます。

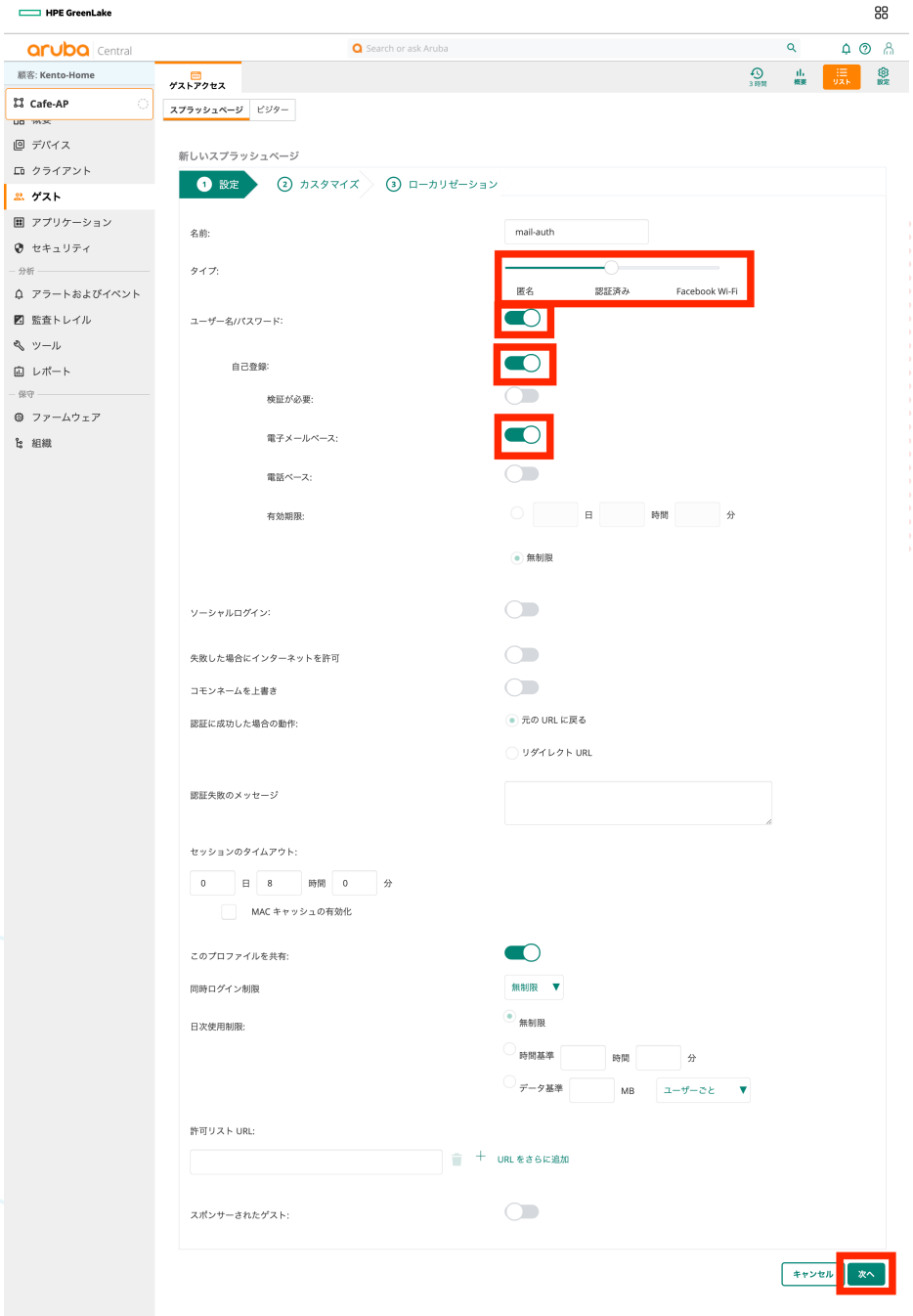
- 同意認証:利用規約に同意(利用規約は任意に設定が可能)
- メール認証:メールアドレスを登録して認証する
- SNS 認証:SNS アカウントでログイン可能
- Facebook Wi-Fi:Facebook ページでチェックイン
- SMS 認証:電話番号に ID を通知し、ID を使って認証
- ID 認証:Aruba Central に登録した ID/Pass を入力して認証

また、キャプティブポータルのカスタマイズも柔軟に行えるため、以下のようなページも作成することができます

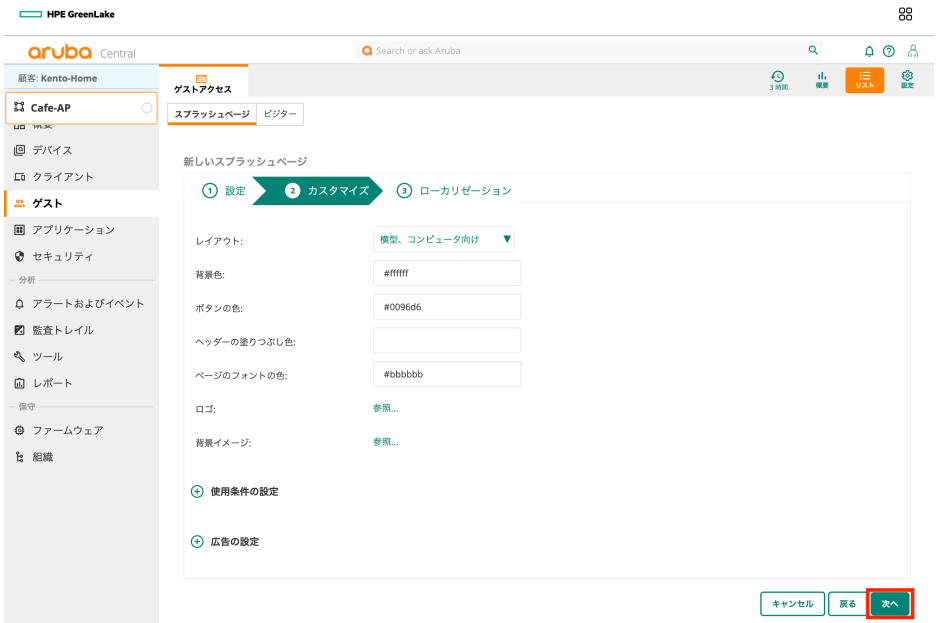
① フィルターアイコンよりスプラッシュページを作成するグループを選択
② 右上の“＋”ボタンから新規スプラッシュページを作成



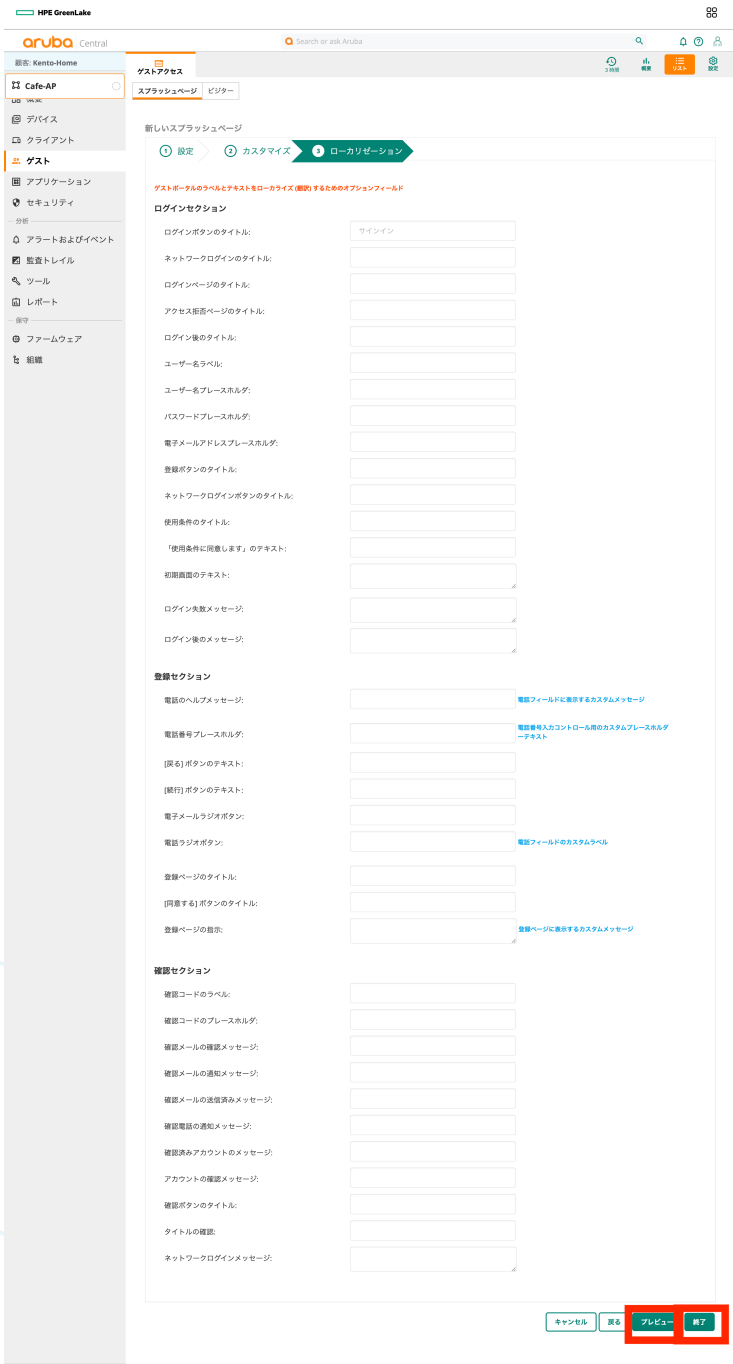
③ 任意のスプラッシュページ名を指定
本設定では“mail-auth”とし、タイプを“認証済み”に設定
ユーザー名/パスワードを有効にし、自己登録を有効にすると、自己登録のタイプが表示されるため、今回は“電子メールベース”を有効にする



④　必要に応じてページのデザインや使用条件等をカスタマイズする

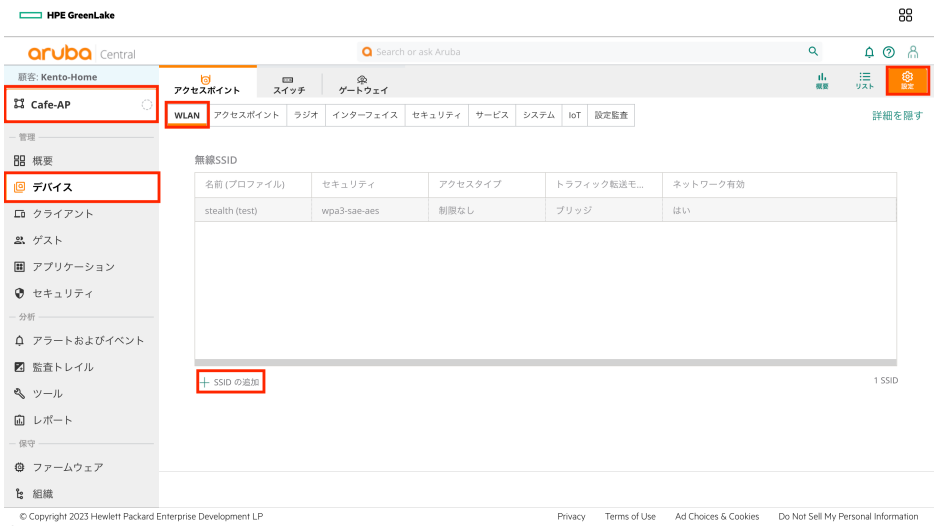


⑤ 必要に応じて各セクションをカスタマイズし、プレビューボタンから最終確認をし、終了をクリック

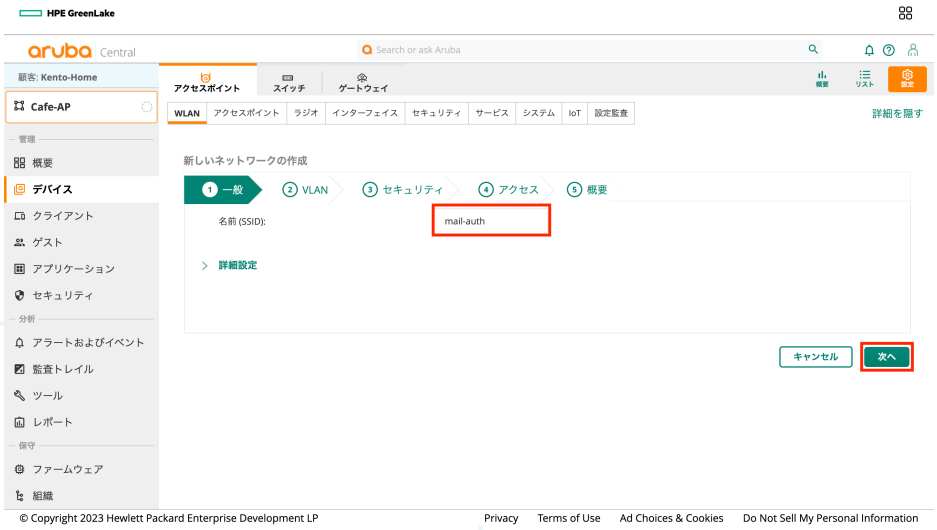

HPE GreenLake
aruba Central
Search or ask Aruba
顧客: Kento-Home
Cafe-AP
デバイス
クライアント
ゲスト
アプリケーション
セキュリティ
分析
アラートおよびイベント
監査トレイル
ツール
レポート
保守
ファームウェア
組織
ゲストアクセス
スプラッシュページ
ビジター
新しいスプラッシュページ
1 設定
2 カスタマイズ
3 ローカリゼーション
ゲストポータルのラベルとテキストをローカライズ (翻訳) するためのオプションフィールド
ログインセクション
ログインボタンのタイトル:
サインイン
ネットワークログインのタイトル:
ログインページのタイトル:
アクセス拒否ページのタイトル:
ログイン後のタイトル:
ユーザー名ラベル:
ユーザー名プレースホルダ:
パスワードプレースホルダ:
電子メールアドレスプレースホルダ:
登録ボタンのタイトル:
ネットワークログインボタンのタイトル:
使用条件のタイトル:
「使用条件に同意します」のテキスト:
初期画面のテキスト:
ログイン失敗メッセージ:
ログイン後のメッセージ:
登録セクション
電話のヘルプメッセージ:
電話フィールドに表示するカスタムメッセージ
電話番号プレースホルダ:
電話番号入力コントロール用のカスタムプレースホルダーテキスト
[戻る] ボタンのテキスト:
[続行] ボタンのテキスト:
電子メールラジオボタン:
電話ラジオボタン:
電話フィールドのカスタムラベル
登録ページのタイトル:
[同意する] ボタンのタイトル:
登録ページの指示:
登録ページに表示するカスタムメッセージ
確認セクション
確認コードのラベル:
確認コードのプレースホルダ:
確認メールの確認メッセージ:
確認メールの通知メッセージ:
確認メールの送信済みメッセージ:
確認電話の通知メッセージ:
確認済みアカウントのメッセージ:
アカウントの確認メッセージ:
確認ボタンのタイトル:
タイトルの確認:
ネットワークログインメッセージ:
キャンセル
戻る
プレビュー
終了
© Copyright 2023 Hewlett Packard Enterprise Development LP
Privacy
Terms of Use
Ad Choices & Cookies
Do Not Sell My Personal Information


JA
サインイン
ユーザー名
パスワード
サインイン
登録

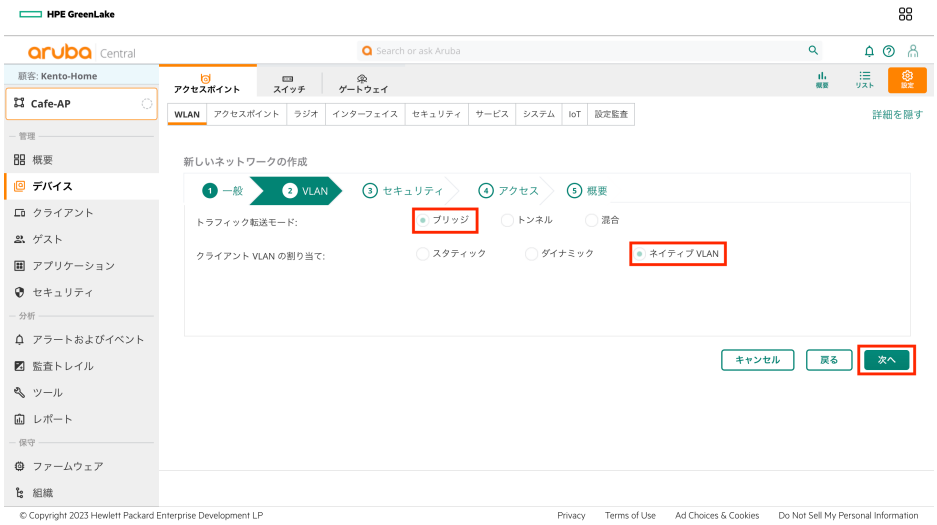
⑥ 正しいグループが選択されていることを確認し、左メニューより“デバイス”を選択し、右上の ボタンをクリック
⑦ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成



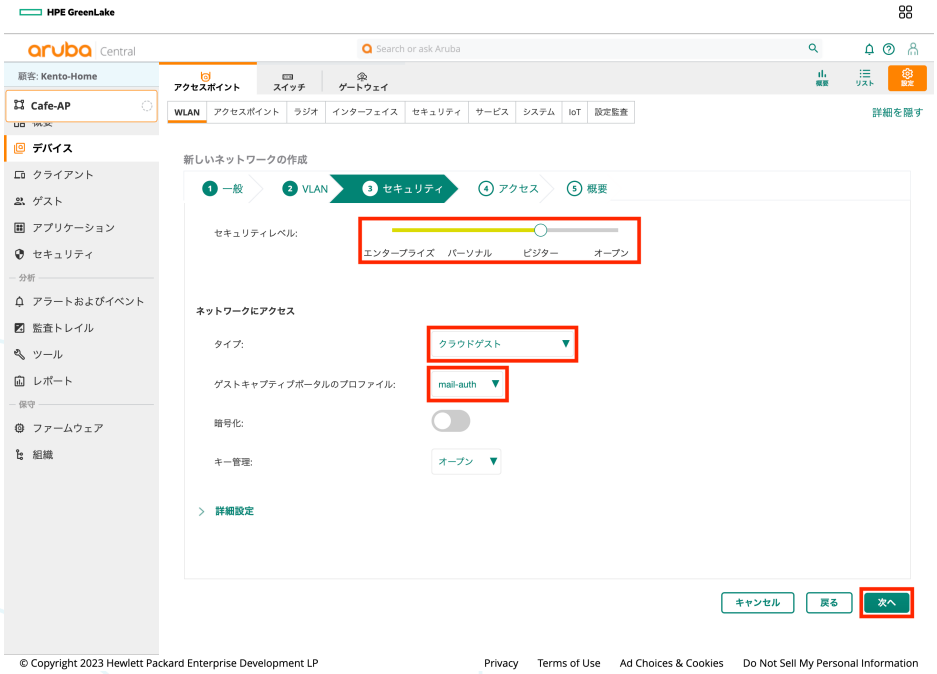
⑧ 任意の SSID を設定します。本設定では“mail-auth”という SSID とし、“次へ”をクリック



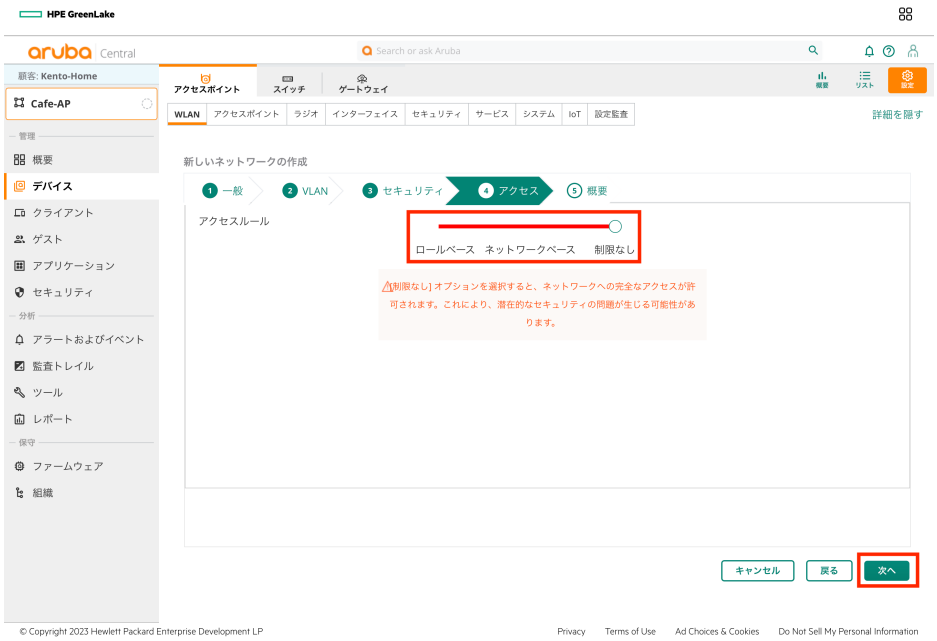
⑨　本設定ではトラフィック転送モードを“ブリッジ”、クライアント VLAN の割り当てにおいて、”ネイティブ VLAN”を選択



⑨　セキュリティーレベルにおいて、”ビジター”を選択
キャプティブポータルのタイプにおいて”クラウドゲスト”を選択し、プロファイルに先ほど作成した“mail-auth”を選択



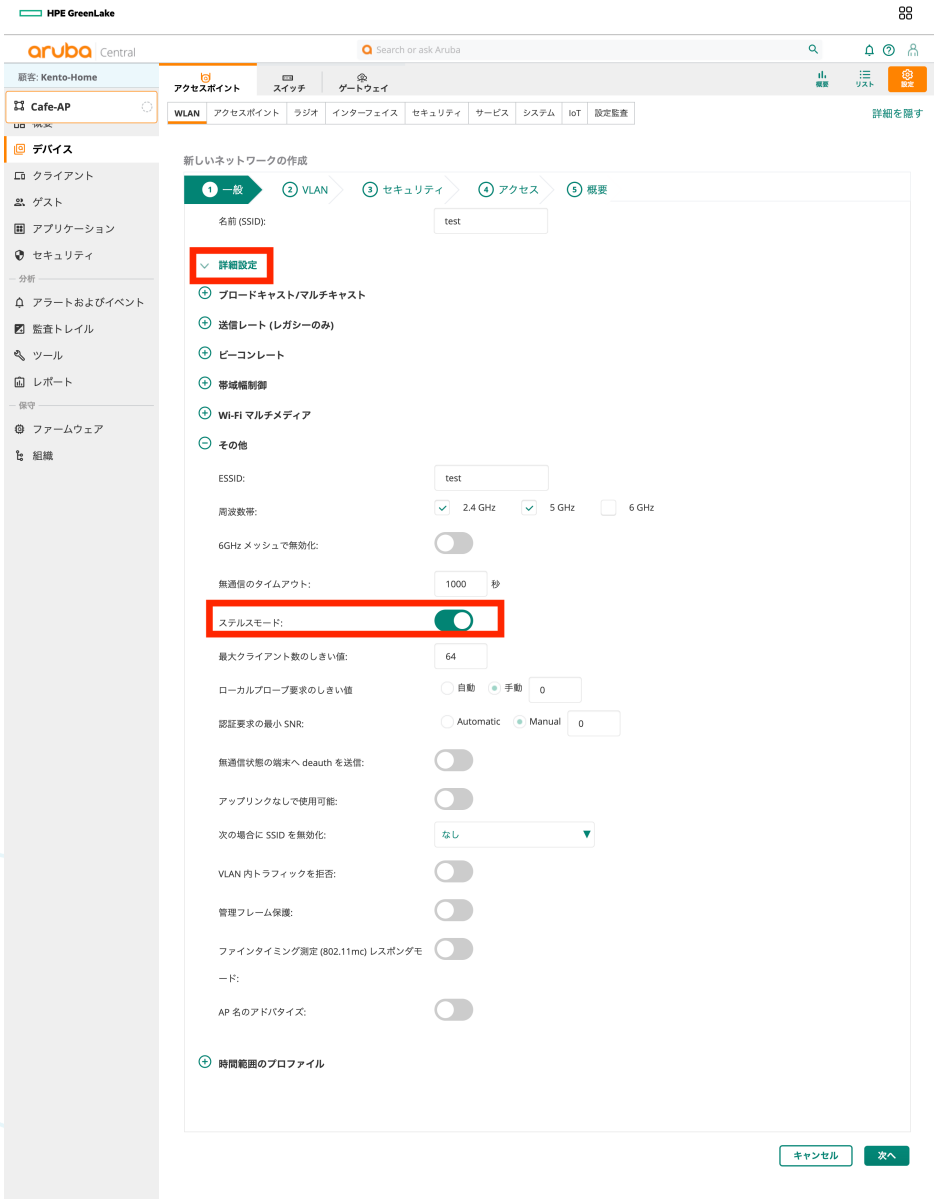
⑩　本設定では、アクセスルール制限をしないため、”制限なし”を選択



概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=mail-auth が作成され、全ての AP から出力される

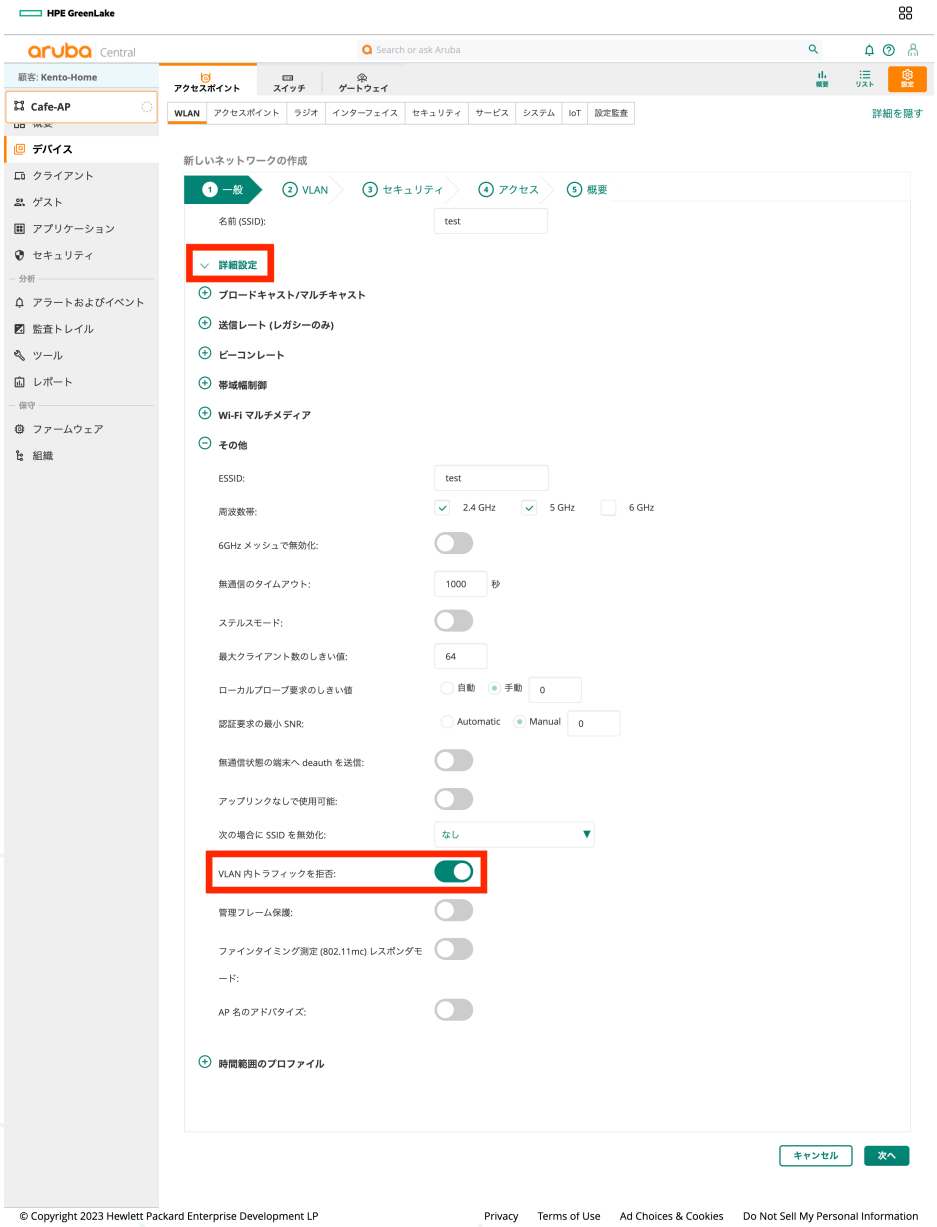
6.10 SSID の隠蔽

SSID を隠蔽して運用したい場合は、WLAN 設定にて”詳細設定”をクリック
ステイルスモードを有効にする



6.11 ユーザ同士の通信制御(User Isolation)について

ゲスト用 SSID 等において、ユーザ同士の通信を禁止したい場合は WLAN 設定にて”詳細設定”をクリックし、”VLAN 内トラフィックを拒否” 項目を有効にする

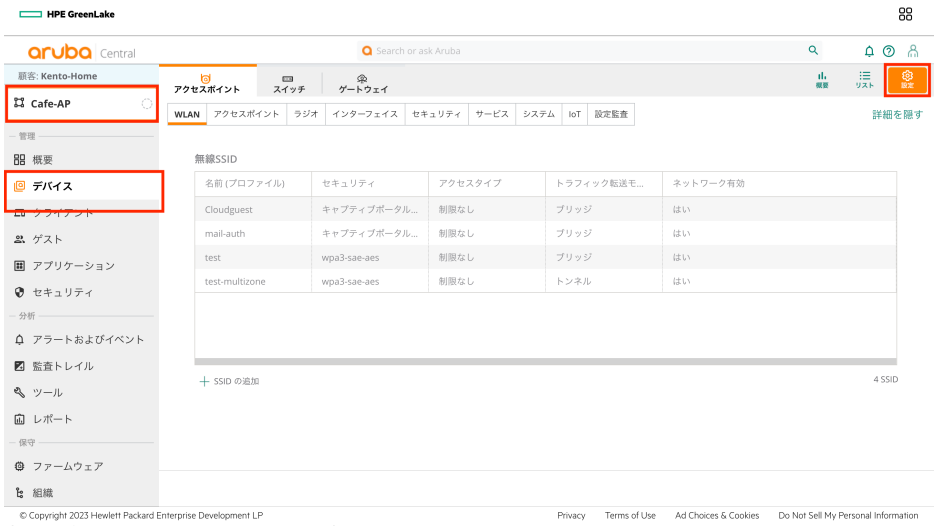


6.12 時間ベースの SSID 制御

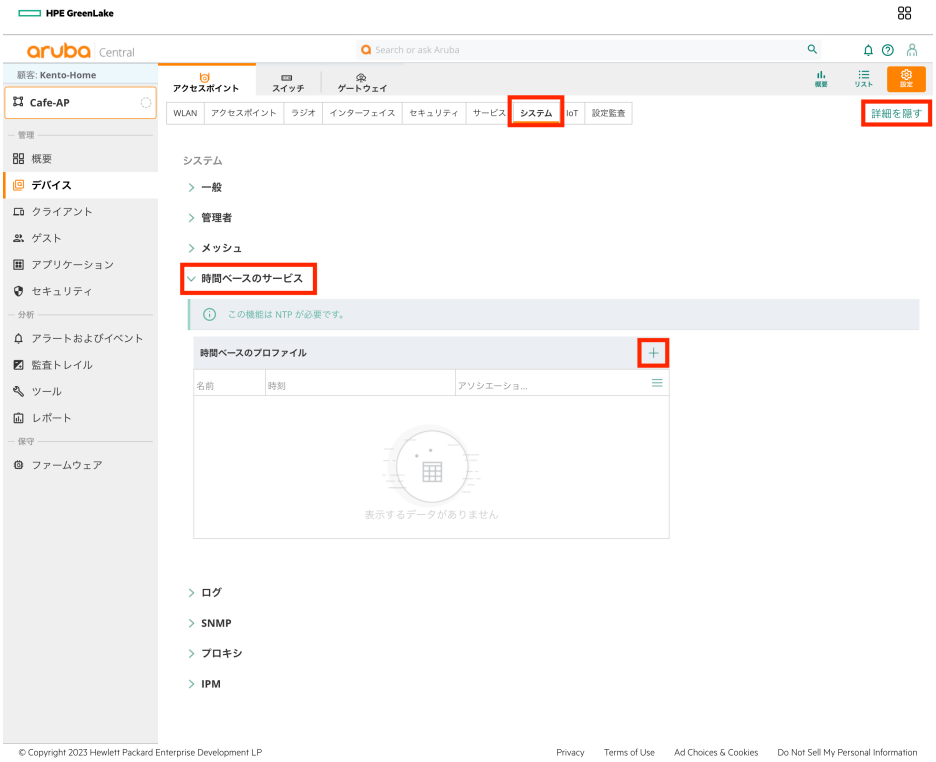
コメントの追加 [OY5]: 横山くんゴール

Instant AP では SSID 毎に時間制限を行うことができる
ゲストに対しての利用時間を制限したい等で利用を行う
① フィルターアイコンよりグループを選択

② 左メニューより“デバイス”を選択し、右上の ⚙ ボタンをクリック

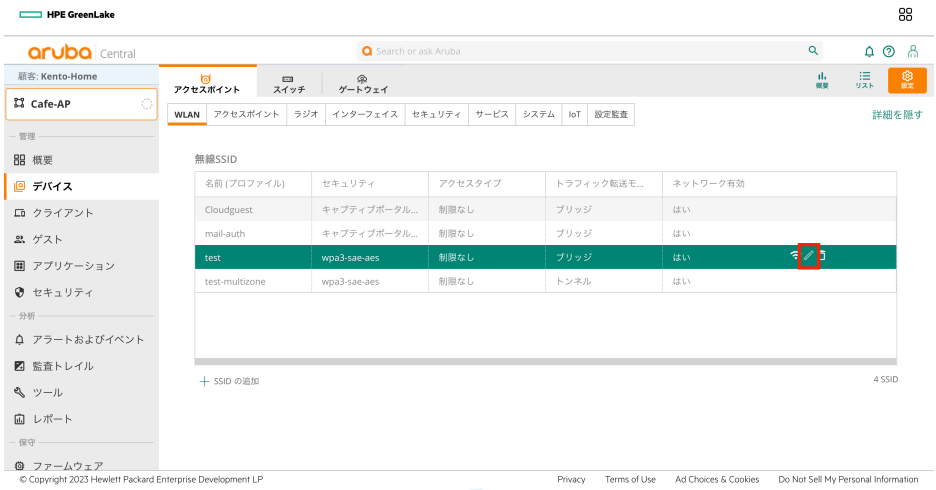


③ “詳細の表示”をクリックして、システムタブを開きます
④ “時間ベースのサービス”から＋ボタンで利用時間のプロファイルを作成

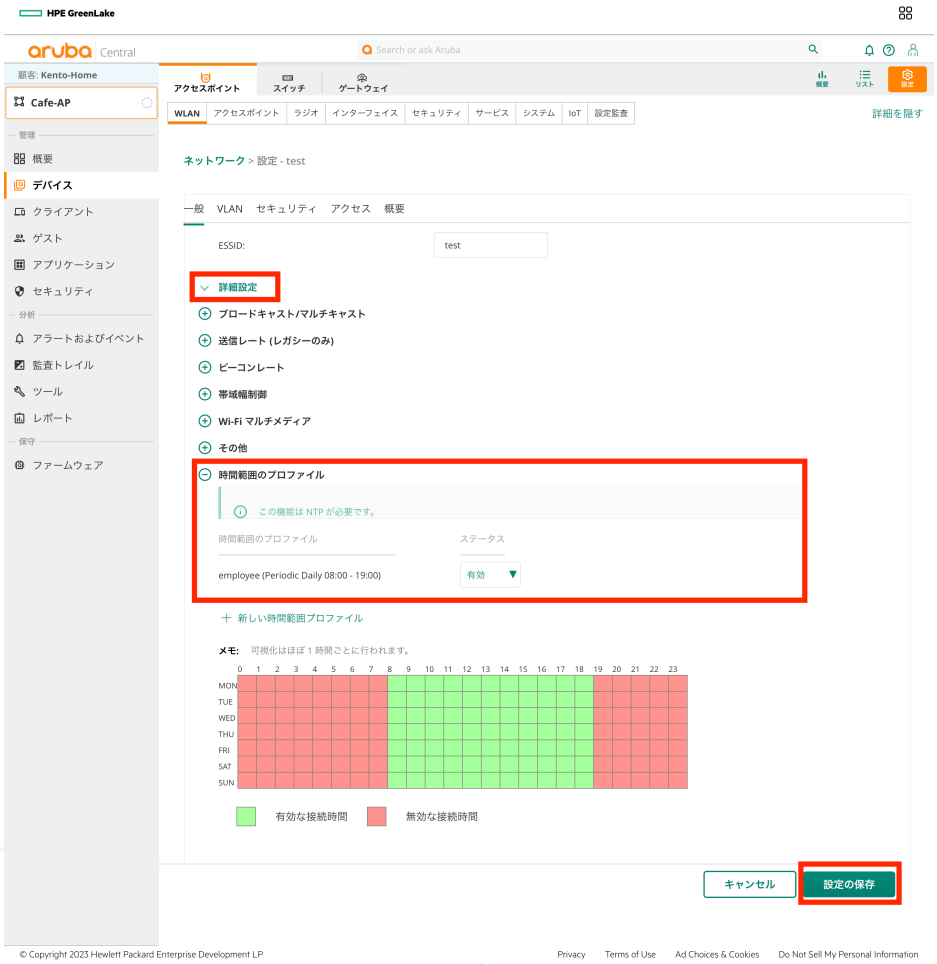

HPE GreenLake
aruba Central
Search or ask Aruba
顧客: Kento-Home
Cafe-AP
アクセスポイント
スイッチ
ゲートウェイ
概要
リスト
設定
WLAN
アクセスポイント
ラジオ
インターフェイス
セキュリティ
サービス
システム
IoT
設定監査
詳細を隠す
管理
概要
デバイス
クライアント
ゲスト
アプリケーション
セキュリティ
分析
アラートおよびイベント
監査トレイル
ツール
レポート
保守
ファームウェア
システム
一般
管理者
メッシュ
時間ベースのサービス
この機能は NTP が必要です。
時間ベースのプロファイル
名前
時刻
アソシエーショ...
表示するデータがありません
ログ
SNMP
プロキシ
IPM
© Copyright 2023 Hewlett Packard Enterprise Development LP
Privacy
Terms of Use
Ad Choices & Cookies
Do Not Sell My Personal Information

⑤　任意の名前、利用時間を指定し、OK をクリック

⑥　WLAN 設定に戻り、時間プロファイルを割り当てる SSID の鉛筆マークから編集する



⑦　“詳細設定”をクリックし、“時間範囲のプロファイル”で先ほど作ったプロファイルを有効
設定の保存をクリックし、SSID 設定を終了する
時間サービスの設定を行った場合、該当の時間のみ SSID を出力するようになる
＊この設定を行う場合、合わせて NTP 設定を行う必要があります。

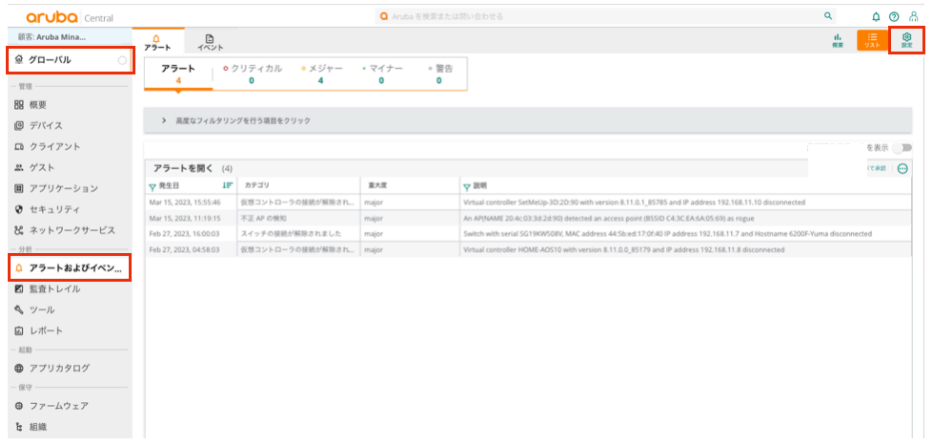


7 アラートとレポート

コメントの追加 [OY6]: 南くんスタート

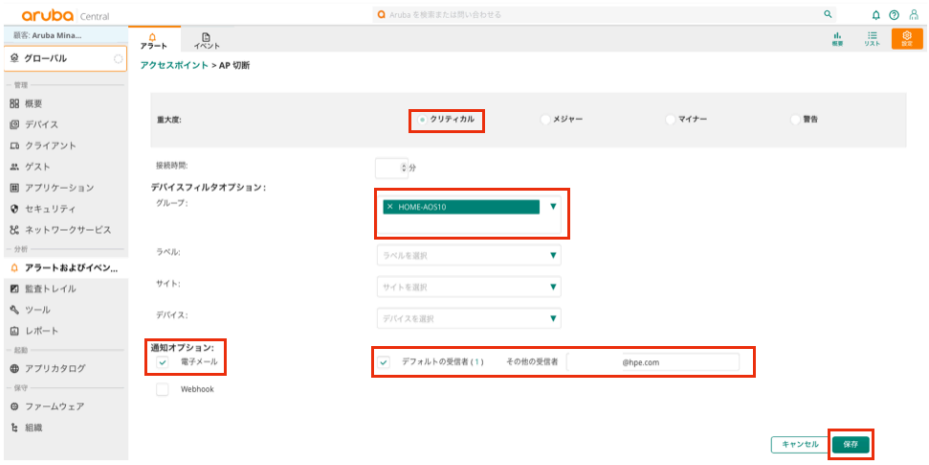
7.1 アラートの設定方法

Central ではデフォルトの通知ポリシーに沿ってアラートを出すことができます。
デフォルトの通知ポリシーを編集することも可能です。
本設定では仮想コントローラの接続が解除された際に、指定のメールアドレスへ通知メールが来るように設定をします。
① フィルターがグローバルになっていることを確認の上、“アラートおよびイベント”を選択し、右の設定ボタンをクリック



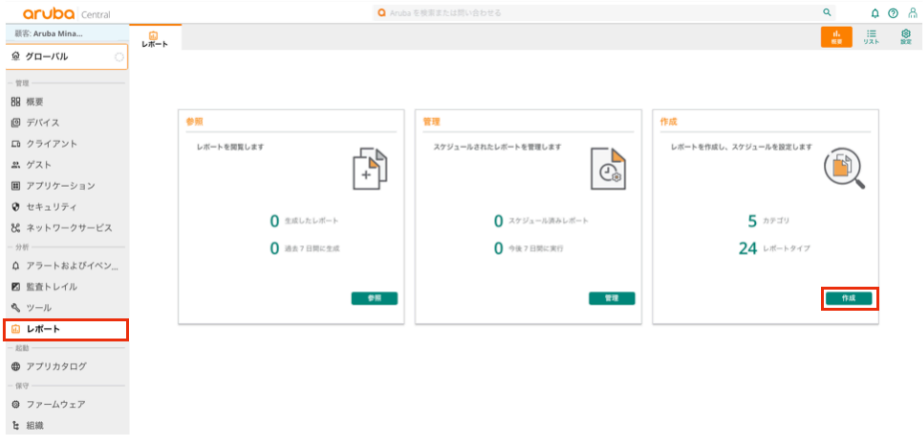
② アクセスポイントの中から“AP 切断”をクリック

③　重要度を“クリティカル”とし、グループを指定
電子メールアドレスのチェックボックスにチェックを入れ、通知を送るメールアドレスを指定する
保存をクリックすると、仮想コントローラの接続が解除された際に、指定メールアドレスにメール通知が来るようになる

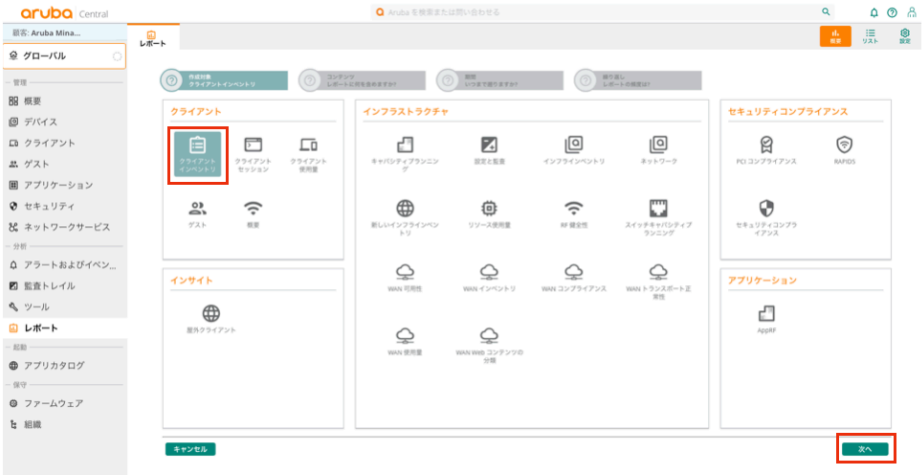


7.2 レポートの出力方法

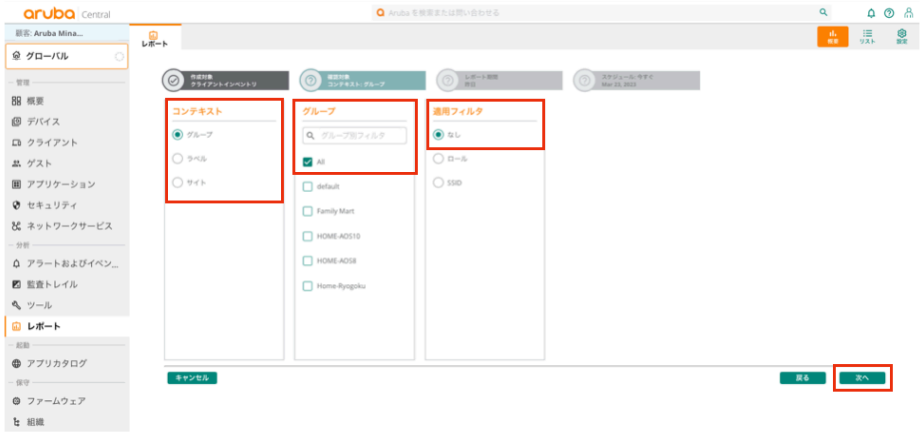
Aruba Central では現在4カテゴリ、24 種類のレポートタイプを出力可能です。
① 左メニューから“レポート”を選択し、“作成”ボタンから新規レポートを作成



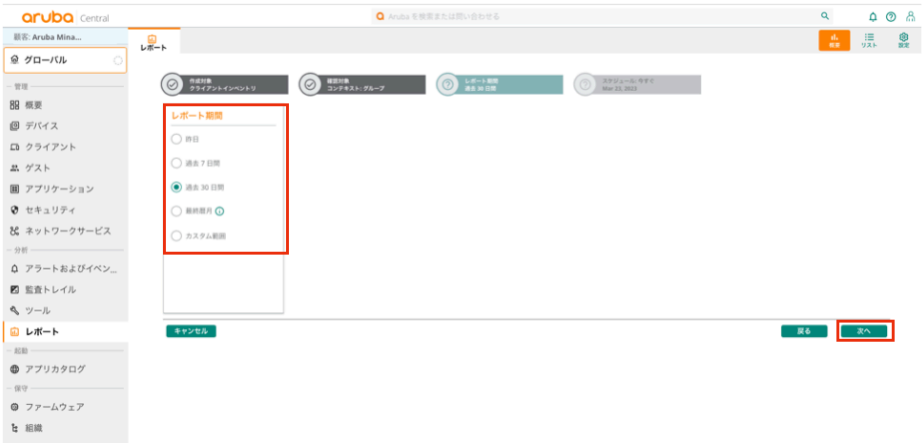
② どのタイプのレポートを作成するのかを選択し、次へ



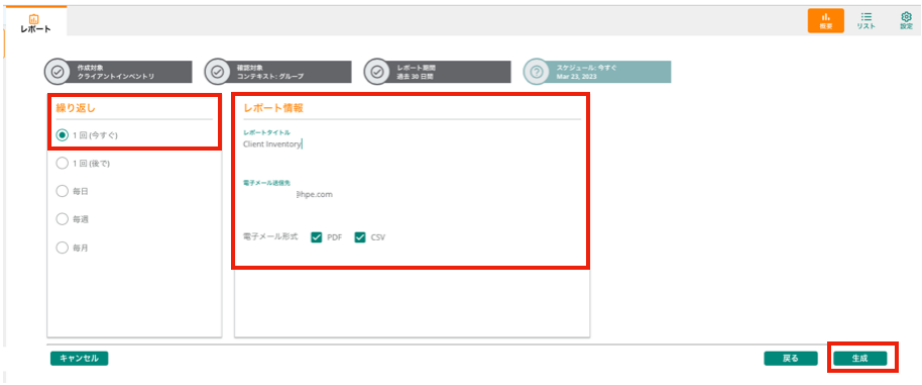
③　レポートを作成する確認対象を確定させ、次へ



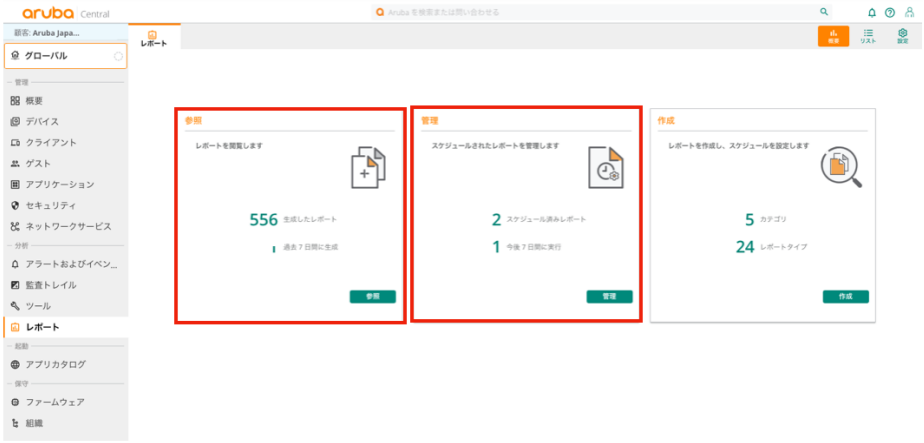
④　レポートに出力する期間を指定する



⑤ レポートを出力する日時を指定し、生成をクリック



⑥ スケジュールしたレポートを管理するには“管理”ボタンから、生成したレポートを確認する場合は“参照”から行えます



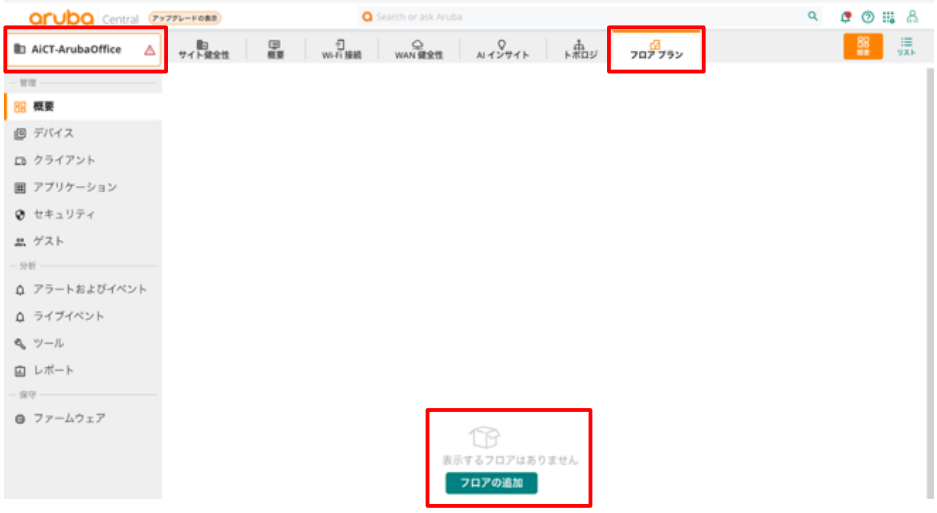
8 FLOORPLANS

コメントの追加 [OY7]: 南くんゴール

FLOORPLANS について

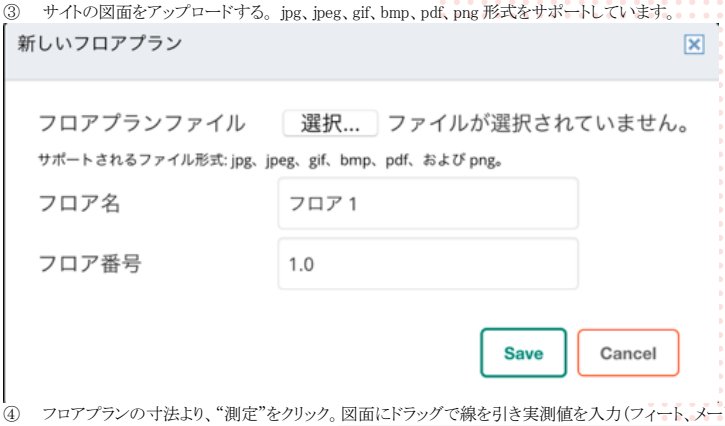
Central ではサイトごとの無線を可視化することができます。また、展開済みの AP だけではなく、仮想的に AP を配置したカバレッジシミュレータとして使用することができます。

① 可視化したいサイトを選択。上部タブの“フロアプラン”を選択後、“フロアの追加”をクリック

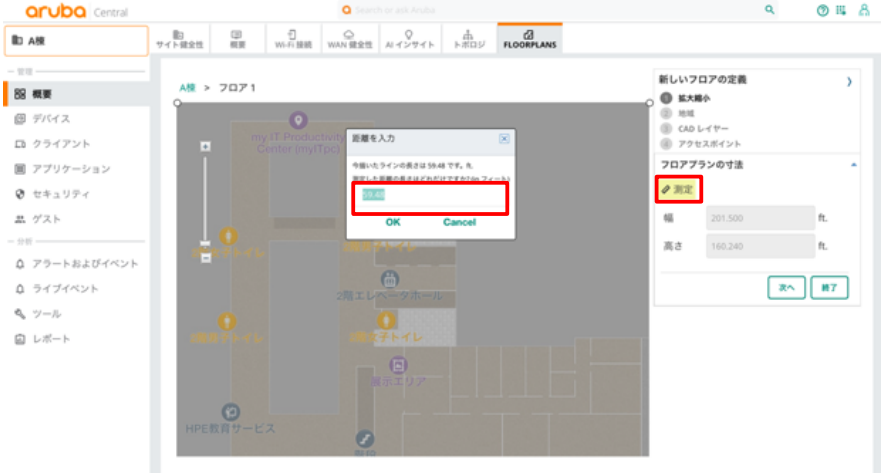


② “新しいフロアプラン”をクリック

③　サイトの図面をアップロードする。jpg、jpeg、gif、bmp、pdf、png 形式をサポートしています。



④　フロアプランの寸法より、“測定”をクリック。図面にドラッグで線を引き実測値を入力(フィート、メートルをサポート)



⑤ アクセスポイントを追加する

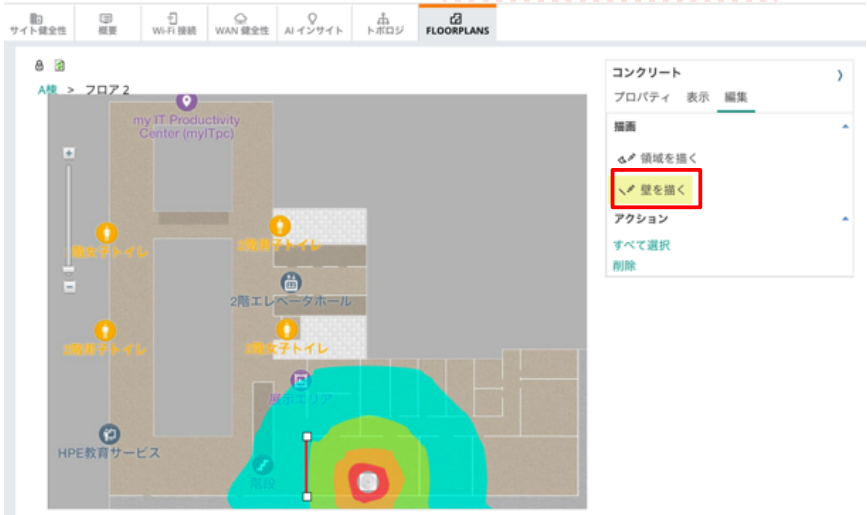
A) 展開済み AP を追加する場合

”展開済み AP の追加”より。サイトに登録している AP を選択。AP をドラッグして実際の位置に配置する。

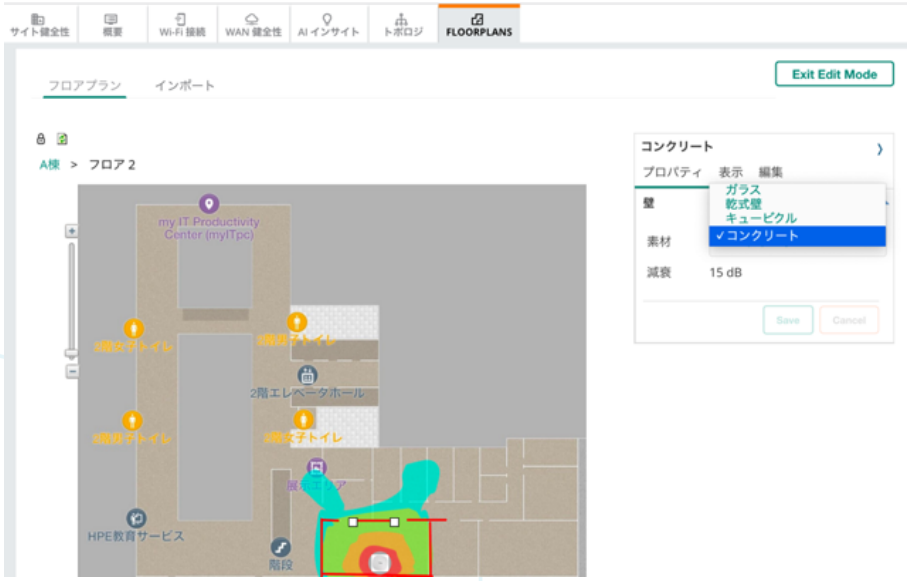
B) 仮想的に AP を配置する場合

“AP の計画”より配置したいモデルを選択し“フロアプランに AP を追加”をクリックし終了

⑥ AP を追加した後、“編集”から“壁を描く”をクリック。フロアプランにドラッグで壁を描画する。



⑦ プロパティから壁の材質を選択可能。壁の材質によって電波の減衰が定められており、リアルタイムにヒートマップが変化する。



10 AIOPs

コメントの追加 [OY8]: 横山くんスタート

AIOPs について

AIOPs は AI Insights・AI Assist・AI Search の 3 つの AI の機能からなり立っています。
今回は AI Insights に焦点を当ててご説明いたします。
Central では AI によってネットワーク内の問題を特定し、ピンポイントの推奨構成を提案します。

AI Insights

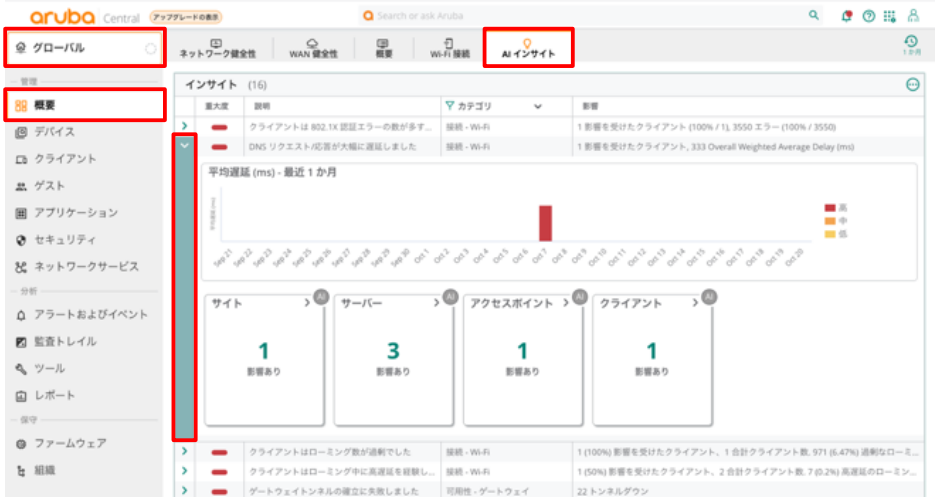
AI Insights のダッシュボードには、ネットワークに影響を与える可能性のあるイベントのレポートが表示されます。これは選択した時間範囲、特定のサイト・デバイスごとやクライアント毎のネットワークイベントのレポートが表示されます。

AI Insights の表示方法

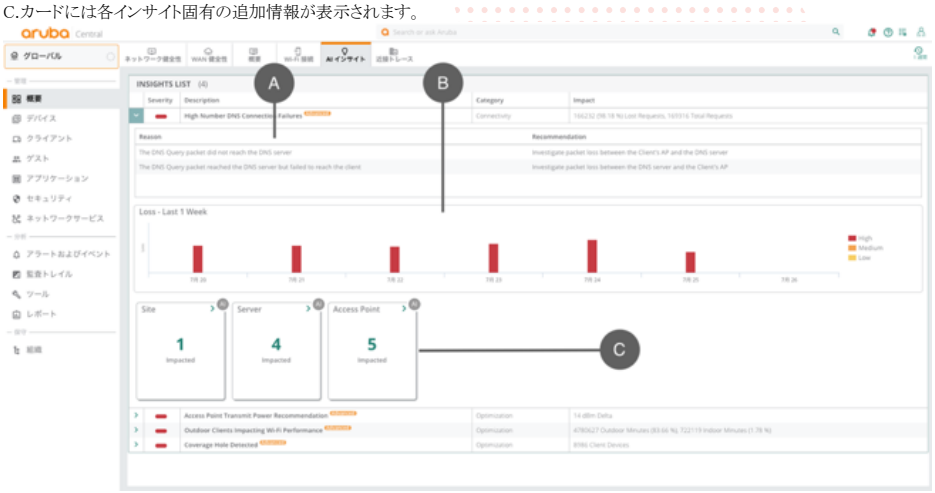
AI Insight の表示方法は Central で管理しているネットワーク、サイトごと、AP ごとの 3 通りあります。

A)　フィルターから“グローバル”を選択し、左メニューから“概要”をクリック
B)　左上メニュー“サイト”より、AI Insights を見たいサイトをクリック。左メニュー“概要”をクリック
C)　グローバルより、左メニュー“デバイス”をクリック。AI Insights を見たい AP をクリック。左メニュー“概要”をクリック。

①　“AI インサイト”タブをクリックし、各インサイトの矢印をクリックすると詳細を表示



② インサイトのタブについて
A.インサイトが生成された理由と推奨事項が表示されます
B.選択した時間範囲で発生したイベントをグラフで表示しています
C.カードには各インサイト固有の追加情報が表示されます。



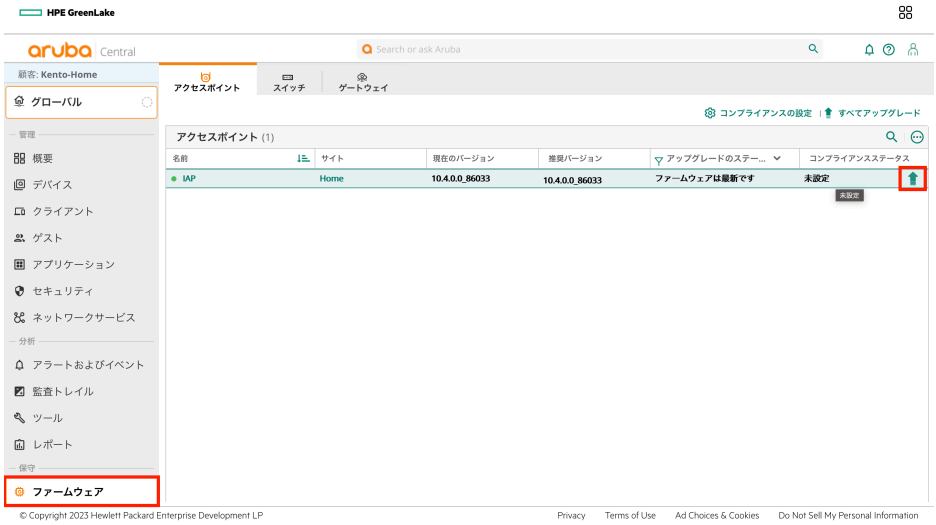
11 メンテナンス

11.1 Version UP について

Instant AP では異なる型番においても Version が同じものであれば、1 つのクラスタとして管理することができます。同一型番で統一している場合は、仮想コントローラを Version UP することにより全ての Instant AP の Version を一括で変更することが可能ですが、異なる型番とのクラスタを組んでいる場合は型番ごとに Version UP を行っていただく必要があります。ご注意ください。

Version UP 方法

① 左メニューから“ファームウェア”を選択し、アップグレードする VC を選択し“アップグレード”をクリック
複数の VC を選択してまとめてアップグレードすることも可能です



② ファームウェアのバージョン、アップデートする日時を選択し “アップグレード”をクリック
※AOS 10 から AOS 8 へダウングレードすることも適切なファームウェアを選択することで可能です。

コメントの追加 [YK9]: AOS10→AOS8 の手順も追加

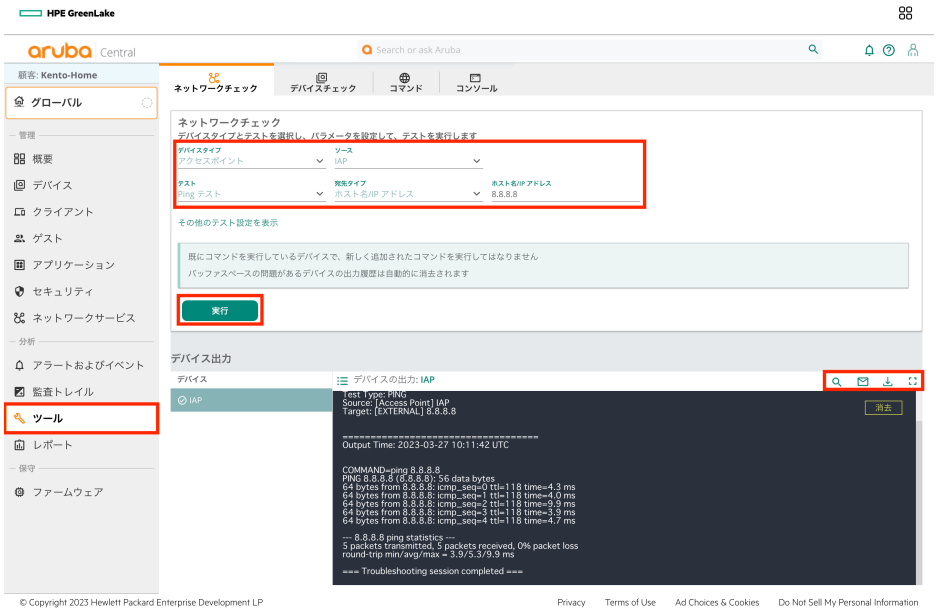
11.2　ツール

ネットワークチェック

デバイスタイプ、テストのタイプ、ソースを選択し、パラメータを設定してテストを実行できる

① 左のメニューより“ツール”を選択し、ネットワークチェックのタブをクリック

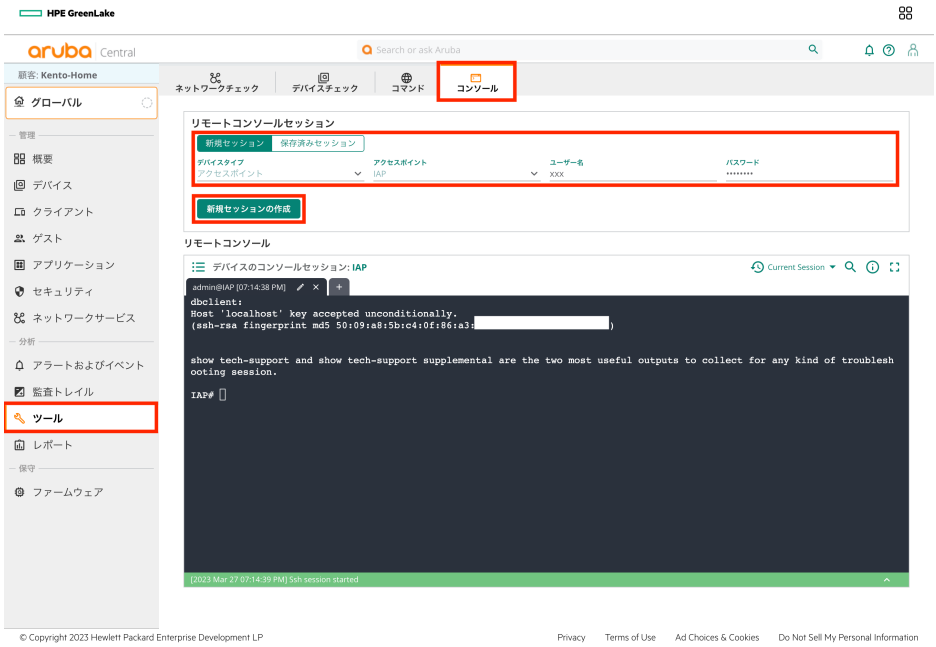
② デバイスタイプ、テスト項目、ソース等を指定し“実行”ボタンをクリックし、デバイス出力より結果を確認する。
デバイス出力は電子メールでの共有、あるいはテキストベースでのアウトプットが可能



11.3　リモートコンソール

Central では GUI から AP の CLI がひらけます

① 左メニューより“ツール”を選択し、“コンソール”タブを開きます。デバイスタイプとデバイス、ユーザ名とパスワードを入力し、“新規セッションの作成”をクリックするとリモートコンソールがスタートします。



13 AP の削除

グループからの削除方法
グループからデバイスを削除する方法は Aruba Central 基本操作ガイド 入門編を参照
https://www.arubanetworks.com/ja/resource/aruba-central-basic-operation-technical-guide/

デバイスインベントリからの削除方法
Aruba Central からデバイスを完全に削除することはできませんが、アーカイブにデバイスを移動させるか、デバイスのサブスクリプションを解除することはできます。

グループの削除
グループの削除は中身が空の状態の時のみ
詳しくは、Aruba Central 基本操作ガイド 入門編を参照
https://www.arubanetworks.com/ja/resource/aruba-central-basic-operation-technical-guide/

14 不具合かと思ったら

コメントの追加 [OY10]: 横山くんゴール

詳細な不具合内容、物理構成、不具合発生時のログ、コンフィグ、不具合再現方法をそろえた上で製品を購入した弊社販売代理店へご連絡ください。販売代理店側のサポート経由で弊社 TAC が対応をいたします。

解析に必須となるログ取得
全ての AP の “show tech support dump“ および、”show tech support dump supplemental ” は必須となります。

以上