

HPE Aruba Networking Central 基本操作ガイド

~IAP 編 (AOS6, AOS8)~

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

1.	. はじ	こめに	5
	1.1.	本資料について	5
	1.2.	注意事項	5
	1.3.	Software Version	5
2.	. Ins	tant AP へのアクセス	6
	2.1	Instant APとPCとの接続について	6
	2.2	電源の投入	6
	2.3	コンソールケーブルを用いての IP アドレス設定	6
	2.4	GUI からのアクセス	8
	2.4.	1 有線側 IP アドレスへの接続	8
	2.4.2	2 新線側 IP アドレスへの接続	9
	2.5	Instant AP へのログイン(GUI/CLI 共通)	10
3.	. Ins	tant AP の登録	.11
	3.1	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	11
	3.2	グループ・サイト・ラベルの作成方法	11
	3.3	初期状態の AP のプロビジョニング	11
	3.4	設定済み AP のプロビジョニング	12
4	Ins	tant AP 基本設定	13
	4.1	Instant AP 仮想コントローラの考え方	13
	4.2	仮想コントローラ名変更・仮想コントローラ IP 指定	13
	4.3	クラスタへの AP 追加	16
	4.4	各 AP の AP 名・IP アドレス設定	17
	4.5	優先マスター設定	19
	4.6	NTP 設定	22
	4.6.7	1 時刻同期の確認1(GUI)	.23
	4.6.2	2 時刻同期の確認2(GUIコンソール)	.24
	4.7.	ダイナミック Radius プロキシ	25
	4.8.	AppRF	27
	4.9.	工場出荷状態への戻し方	29
	4.9.7	1 グループを使った AP の初期化	.29
	4.9.2	2 リモートコンソールからの初期化	.29
	4.9.3	3 CLI からの初期化	.30
	4.9.4	4 リセットボタンからの初期化	.30
5	有新	泉ポート設定	32
6	SSI	ID の設定	36
	6.1	SSID の作成手順	36
	6.2	設定例)オープン認証(暗号/認証なし)	39
	6.3	設定例)WPA3-PSK	42

Technical Note

HPE Aruba Networking Central 基本操作ガイド IAP 編

6.4	設定例)WPA3-PSK+MAC 認証 (Cloud Auth)	45
6.5	。 設定例)802.1x Cloud Auth 利用	50
6.6	設定例)802.1x External Radius 利用	54
6.7	Dynamic VLAN(External Radius 利用)	57
6.8	設定例)Web 認証 規約ページのみ	61
6.9	ユーザ/パスワードでのログイン	64
6.10	0 Central ゲスト(メール認証)	69
6.11	1 SSID の隠蔽	77
6.12	2 ユーザ同士の通信制御(User Isolation)について	78
6.13	3 ゾーン設定について	79
6.14	4 時間ベースの SSID 制御	82
77	アラートとレポート	86
7.1	アラートの設定方法	86
7.2	レポートの出力方法	88
8 F	FLOORPLANS	91
9 A	AIOPs	95
10 >	メンテナンス	97
10.1	1 Version UP について	97
10.2	2 ツール	
10.3	3 リモートコンソール	
11 A	AP の削除	100
12 7	不具合かと思ったら	100





Technical Note

HPE Aruba Networking Central 基本操作ガイド IAP 編

以下の表に、本文書の修正点を示します。

表 1: 改訂履歴

主な変更内容
初版発行
Central 2.5.2における変更点を追加
Central 2.5.3における変更点を追加
Central 2.5.4における変更点を追加
テンプレート変更に伴う修正等

1. はじめに

1.1. 本資料について

本資料は HPE Aruba Networking Central におけるインスタントアクセスポイント(AOS6,AOS8)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 HPE Aruba Networking 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.hpe.com/psnow/doc/a00143744jpn

1.3. Software Version

本資料は HPE Aruba Networking Central 2.5.4 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。



HPE Aruba Networking Central 基本操作ガイド IAP 編

2. Instant AP へのアクセス

2.1 Instant AP と PC との接続について

Instant 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。

2.2 電源の投入

Instant 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

2.3 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が同梱されている製品および同梱されておらず別売りとなっている 製品の 2 つのパターンがありますので、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 Instant AP にコンソールケ ーブルを接続

Tera Term: Serial port setup							
Port:	COM3 -	ОК					
Baud rate:	9600 -						
Data:	8 bit 🔹	Cancel					
Parity:	none 👻						
Stop:	1 bit 🔹	Help					
Flow control:	none 👻						
Transmit delay 0 msec/char 0 msec/line							

2 電源の投入

アダプタもしくは、PoE から Instant AP に給電を行う

③ Boot の停止

Instant 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。



* "Hit <Enter> to stop autoboot:"は電源投入後、3,4秒で表示される



HPE Aruba Networking Central 基本操作ガイド IAP 編

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 を指定する

・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>

apboot> setenv ipaddr 10.215.212.20 apboot> setenv netmask 255.255.255.0 apboot> setenv gatewayip 10.215.212.1 apboot>	
 (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する	
COMS - Tera Term VT - X	
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)	
<pre>autostart=ves ^ bootfile=ipe806x.ari atdids=nandD=nandD ethaddr=80:8d:b7:c2:e9:02 NEHLSRL2=1 name=AP102 uap_controller_less=1 os_eartition=0 stdin=serial stdout=serial stdout=serial stdout=serial nachid=1260 ntdoarts=mtdoarts=nandD:0x2000000@0x0(acc0),0x2000000@0x2000000(acc1),0x4000000@0x 4000000(ubifs) partition=nandD.0 ntddevnum=0 ntddevnum=0</pre>	

*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

nt size: 512/65532 bytes

ddr=10.215.212.20 mask=255.255.255.0 екауір=10.215.212.1

"saveenv"コマンドで設定を書き込み、"boot"コマンドで再起動する



起動後 User:admin Password:admin または AP のシリアルナンバーで入り、" show ip interface brief "で設定した内容が反映されている ことが確認できる



2.4 GUI からのアクセス

Instant AP は GUI/CLI どちらを用いても設定が可能ですが、GUI からの設定が基本となります。

推奨のブラウザは以下の通りです。

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Firefox 48 or later on Windows 7, Windows 8, Windows 10, and Mac OS
- Apple Safari 8.0 or later on Mac OS
- Google Chrome

2.4.1 有線側 IP アドレスへの接続

DHCP サーバ または CLI より IP アドレスを確認し、Instant AP に割り当てられた IP アドレスヘブラウザからアクセスしてください。アドレスのみの場合は自動的に https ページへリダイレクトされます。

Instant	× +			- o >
→ C ▲ #####	ていない通信 https://10.215.212.20.434	3/login		€ ☆ @
		orubo	×	
		a Hewlett Packard		
		Enterprise company		
		Instant へようこそ		
		ユーザー作		
		129-5		
		0949		
		24		

*ログインボタン右下に言語設定があります。ブラウザの言語設定に対して表示されますが、必要によって言語を変更してください。

2.4.2 無線側 IP アドレスへの接続

初期設定では設定用に"SetMeUp-xx:xx:xx"(xx:xx: には IAP の MAC アドレス下 6 桁が入ります)という SSID が出力されています。この SSID に対して PC を無線接続した上で、ブラウザから <u>https://setmeup.arubanetworks.com</u>にアクセスします。
 2010 2-4 Malua - 2017 2-4 Malua - 2017



③ PCのIPアドレスを確認します。 Instant APでDHCPサーバが起動しています。SSID="SetMeUp-xx:xx:xx"に接続すると、PCにIPアドレスが振られます。



④ PC のブラウザから Instant AP にアクセスする
 "<u>https://setmeup.arubanetworks.com</u>"(もしくは、(2)で確認したゲートウェイ)にアクセスをします。



2.5 Instant AP へのログイン(GUI/CLI 共通)

初期設定では ユーザ名: admin パスワード: admin でログインすることができます。 AOS8.5 以降ではユーザ名: admin パスワード: AP のシリアルナンバー





3. Instant AP の登録

3.1 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

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 基本操作ガイド(入門編)を参照

https://www.hpe.com/psnow/doc/a00143744jpn

3.2 グループ・サイト・ラベルの作成方法

グループ・サイト・ラベルの作成方法に関しては、以下 Central 基本操作ガイド(入門編)を参照

https://www.hpe.com/psnow/doc/a00143744jpn

3.3 初期状態の AP のプロビジョニング

工場出荷状態の AP をプロビジョニングする方法です。この方法で AP をプロビジョニングした場合、AP の設定は Central に帰属するグループの設定へと上書きになるため、ご注意ください。

AP にある既存のコンフィグを Central にインポートしたい場合は、設定済み AP のプロビジョニングを参考にしてください。

* グループに VC を割り当てた時点で、その VC 配下にある AP は全てグループのコンフィグを反映させるためにリブートします。ただしグル ープ内のコンフィグと IAP のコンフィグに差分がない場合はリブートしません。

- ① ネットワーク操作アプリ内、右上の 👯 マークをクリック
- ② 追加する AP を Central のデバイスインベントリーに追加
- *詳しくは Central 基本操作ガイド(入門編)を参照(<u>https://www.hpe.com/psnow/doc/a00143744jpn</u>)
 ③ 追加したデバイスにサブスクリプションを割り当てる
- *詳しくは Central 基本操作ガイド(入門編)を参照(<u>https://www.hpe.com/psnow/doc/a00143744jpn</u>)
 (④ IAP を起動する * IAP に DNS の設定が必須です。詳しくは、<u>InstantAP へのアクセス</u>を参照 サブスクリブションの光たっている IAPは、記動プロセス中 Activate 接続のタイミングで自身が Control 配下の IAP

サブスクリプションの当たっている IAP は、起動プロセス中 Activate 接続のタイミングで自身が Central 配下の IAP であることを認識 し、自動的に Central へ接続しにいきます。

⑤ グループ管理画面から、プロビジョニング未完了デバイスとして IAP が認識されていることを確認 *グループに所属していないデバイスが Central で認識された場合、画面下部のようなアラートが出る

ଛ ″ଘ−./ĩル ୁ	キットワーク構造			
- 11 II				Q +
88 概要	設定が共通のデバイスを1	つのグループにまとめ、同じ設定を適用しま	r	
個 デバイス	▼ グループ名			
	> 接続されているすべてのデ/	でイス (14)		
LO VV1VVP	 プロビジョニング未了デバー 	17, (2)		
豊 ゲスト	デバイス名	タイプ	シリアル番号	MAC 7FLX
囲 アプリケーション	SetM	UAP		80
セキュリティ	VC-M	LA.P		20
18 2 ~ L D - 0 # - 17 7				
0. *********				
22前				
♪ アラートおよびイベント				
☑ 監査トレイル				
& ツール				
ゆ レポート	> de	0.00		
	> Ali	5 A C		
28.4	> ct	0		
◎ ファームウェア				
te AELAN				
▲ 2 個の既存の設定を持つデバー	イスがチェックインされていま	す。インボート		< 17

⑥ 新しいグループを作成、未割り当てのデバイスをとして認識されているデバイスをグループへ割り当て
 *詳しくは Central 基本操作ガイド(入門編)を参照(<u>https://www.hpe.com/psnow/doc/a00143744ipn</u>)



3.4 設定済み AP のプロビジョニング

既存のコンフィグを残したまま IAP を Central にプロビジョニングする方法です。 *この方法は既存のコンフィグを残すため、VC からグループを作成したとしても AP のリブートは起こりません。

- ① 初期状態の AP のプロビジョニング①~5まで同じ手順
- ② プロビジョニング未完了のデバイスを選択して、"グループのインポート"をクリック

皇 グローバル	た ネットワーク構造			
- 1112	← グループ (9)			Q (+)
88 概要	設定が共通のデバイスを 1	つのグループにまとめ、同じ設定を適用します		
🖻 デバイス	▼ グループ名			
- 	> 接続されているすべてのデ/	でイス (14)		
L0 221721	 プロビジョニング未了デバ・ 	イス (2)		
豊 ゲスト	デバイス名	タイプ	シリアル番号	MAC アドレス
囲 アプリケーション	SetMe	WP		40
O セキュリティ		w		× @
				グループロインボート
8 ネットワークサービス				
- 分析				
♪ アラートおよびイベント				
🖾 監査トレイル				1 itern(s) selected
& ツール				
ゆ レポート	> de	6.0		
	> Ali	6		
28.4	> ct	0		
◎ ファームウェア				
te Helwar				
▲ 2個の既存の設定を持つう	デバイスがチェックインされていま	す。インボート		< 1/1 >

③ グループ名を入力し、"追加"をクリック

④ IAP の設定がインポートされていることを確認し、設定済み IAP のプロビジョニングが完了

4 Instant AP 基本設定

4.1 Instant AP 仮想コントローラの考え方

同一 L2NW 内の Instant AP のうち 1 台が仮想コントローラの役割を行います。 仮想コントローラが起動している Instant AP に障害が発生 した場合は、 ネットワーク上にある他の Instant AP に仮想コントローラ機能が引き継がれ動作をし続けます。



Instant AP の動作条件は下記のとおりです。

・同一 L2NW のみでの稼動

・同一 L2NW 内で複数の Instant AP クラスタは作成できません。

・異なる型番の Instant AP でも Version が同一であれば管理可能(Version UP 時の制限あり)

・優先マスター設定をしていない場合、ネットワーク上で最初に立ち上がった Instant AP で"仮想コントローラ"がマスターとして動作を行います。

4.2 仮想コントローラ名変更・仮想コントローラ IP 指定

仮想コントローラ IP は設定しなくても問題ありませんが、設定をすることで常に この IP アドレスへアクセスすれば良くなりますので、管理性が向上します。Instant AP のネットワーク内で重複していないアドレスを付与することを推奨します。 ① フィルターよりグループを選択

◎ グローバル	0	 ネットワーク健全性	v	♀ VAN 健全性	国概要	w
@グロ −バル						
▼フィルタリスト						
ログループ		助サイト		クラベル		
		スカイツリー				
	63					
BGW-9004						
CAFE JOBA						
CAFE-OSK-AP				その他AP		
	តា					





③ 右側の"詳細を表示"をクリックし、システムタブをクリック 仮想コントローラを選択し、右の鉛筆マークをクリック

II CAFE-AP 이	び アクセスポイント スイッチ	ゆ ゲートウェイ			ul. ≔ ₩₩ 92.0 ₩2
- 1111	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 VPN サービス システム	IoT 說定監查	詳細を隠す
88 概要					
😑 デバイス	システム				
DB クライアント	∨ 一般				
<u>業</u> ゲスト	仮想コントローラ				
囲 アプリケーション	名前	IPアドレス	1Pv6 7 F L ス	N3-K	=
😧 セキュリティ	AUI-7F-IAP-VC			JP3	Z
- 分析	IAP-2F-POC			JP3	
アラートおよびイベント	5 10 25 50 1 ×-5/8.0	0			K < > X = 2 = 10
🛛 監査トレイル					
ヘ ツール	グループの国コードを設定する	:	JP3 - Japan	*	
回 レポート	タイムゾーン:		第1页 UTC+09		
- ^{保守} 〇 ファームウェア	優先周波数帯:		४ ≪र ▼		
	NTP サーバー :		ntp.nict.jp		
	仮想コントローラのネットマス	9:	1006.3006.3006.0005		
	部務ついとローラのゲーとか。	2.			



④ 名前と IP アドレスを入力し、"OK"をクリック

3	IP アドレスの編集		×
	名前:	IAP-VC	
	IP アドレス :	10.215.212.30	
	IPv6 アドレス :	2000020000	
ł	Ċ) IPv6 管理を有効にする必要があります。	
l	国コード:		
<u> : </u>	JP3 - Japan	▼	
):	キャンセル	ОК	

⑤ 内容を確認し"設定の保存"をクリック

다 CAFE-AP 이	1000000000000000000000000000000000000	ゆ ゲートウェイ			al. ≔ ∰ 925 ₩
- 世理	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 VPN サービス システ	A IoT 設定監査	詳細を隠す
88 概要					
😬 デバイス	システム				
ロ クライアント	∨ 一般				
豊 ゲスト	仮想コントローラ				
圏 アプリケーション	8.0	ゆアドレス	1Pv6 7 15 L Z	00 J - K	=
セキュリティ	IAP-VC	10.215.212.30		JP3	
- 分析	IAP-2F-POC			JP3	
☆ アラートおよびイベント	5 10 25 50 1 ×	あたり			K < > X <-9.10
■ 監査トレイル					
ヘ ツール	グループの国コードを設定	F & :	JP3 - Japan	•	
回 レポート	タイムゾーン:		RER UTC+09	*	
	優先周波数帯:		1442 V		
9 77-L7IF					
	NTP サーバー:		ntp.nict.jp		
					キャンセル 設定の保存



4.3 クラスタへの AP 追加

新しい Instant AP を仮想コントローラが立ち上がっている同一ネットワークに追加をするだけで自動的にクラスタへの AP 追加ができます。 Central 上管理するためには新しく追加した AP のデバイス追加とサブスクリプションの割り当て作業が必要となります。

- 追加したい AP をデバイスインベントリに追加
- *詳しくは Central 基本操作ガイド(入門編)を参照(<u>https://www.hpe.com/psnow/doc/a00143744jpn</u>)
- ② AP にサブスクリプションを割り当てる
 * 詳しくは Central 基本操作ガイド(入門編)を参照(<u>https://www.hpe.com/psnow/doc/a00143744jpn</u>)
- ③ APを仮想コントローラが立ち上がっている同一ネットワークに追加
- ④ フィルターより仮想コントローラが所属するグループを選択



⑤ デバイス一覧で追加した AP があることを確認する

티 CAFE-AP 이	10 ロ アクセスポイント スイッチ	ゆ ゲートウェイ					
- 1111 88 模要	アクセスボイント ・オン 5	/ライン ◎オフライ 5 0	ン ラジオ 11				
🥴 デバイス	アクセスポイント (5)						± ⊡
D クライアント	▼ デバイス名	ステータス	▼ 伝想コントローラ	Y 10 7 F	▼ モデ	マシリアル	ファームウェアバージョン
a stat	AU	Online	AUI	17	AP-535	CN.	8.6.0.9_79813
島 ゲスト	70:3	Online	IAP-	17	AP-225	CT	6.5.4.15_73677
圖 アプリケーション	MP-	Online	UAP-	17	AP-205	CA.	6.5.4.15_73677
Ø セキュリティ	7F-6	Online	AUI	10	AP-515	Ch.	8.8.0.1_80393
0.5	AUI-	Online	AUI	10	AP-555	Ch.	8.8.0.1_80393
 ↓ アラートおよびイベント 図 監査トレイル ヘ、ツール 山 ルポート - 保守 ② ファームウェア 							

- 注1) 新しい Instant AP にコンフィグが入っている場合でも、すでに立ち上がっている仮想コントローラを認識すると仮想コントローラにあるコンフィグに書き換えられます。
- 注2) 同一型番の Instant AP を追加する場合には仮想コントローラに入っている Version に合わされますが、異なる型番の場合には予め Version を合わせた上でネットワークに追加してください。



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

다 CAFE-AP 이	10 アクセスポイント	□ ŵ スイッチ ゲートウェイ					±. ₩ IJAN ₩2
- 11日 88 概要	アクセスポイント 5	・オンライン ●オフ 5 0	ライン ラジオ 11				
📴 デバイス	アクセスポイント	(5)					₹ ⊖
ロ クライアント	▼ デバイス名	ステータス	▼ 伝想コントローラ	Y 10 7 K	▼ モデ	▼ シリアル	ファームウェアバージョン
	AUF	Online	AUI	17	AP-535	Ch.	8.6.0.9_79813
塁 ゲスト	70:3	Online	IAP.	17	AP-225	CT	6.5.4.15_73677
■ アプリケーション	MPS .	Online	DAP-	17	AP-205	CA.	6.5.4.15_73677
セキュリティ	75-8	Online	AUR	10	AP-515	Ch-	8.8.0.1_80393
	AU	Online	AUR	10	AP-555	Ch-	8.8.0.1_80393
 ↓ アラートおよびイベント ■ 監査トレイル ▲ ツール ■ レポート ● ロボート ● ロボート 							

Technical Note HPE Aruba Networking Central 基本操作ガイド IAP 編

디 CAFE-AP 이	し アクセスポイント	ロ スイッチ	余 ゲートウェイ							iiii ا
- 1011	WLAN 77t2	ポイント ラジオ	インターフェイス	セキュリティ	VPN サービス	システム 10	T 設定監査			詳細を隠す
88 概要										
😕 デバイス	アクセスオ	イント (5)								Θ
- h= (7).1	名前	VC &	ステータス	IPアドレス	ゆ割り当て	4-14	タイプ	2.4GHz (∮†…	5GHz (チャネ	アクション
L0 994725	AUI	AI.	Up	172.31	DHCP	access	AP-535	Auto	Auto	
島 ゲスト	JAP-	LA	Up	172.31	STATIC	access	AP-205	Auto	Auto	
■ アプリケーション	70.	-	Up	172.31	DHCP	access	AP-225	Auto	Auto	1
	AUI	AJ	Up	10.215	DHCP	access	AP-555	Auto	Auto	
😯 セキュリティ	71-1	Al	Up	10.215	DHCP	access	AP-515	Auto	Auto	
- 分析										
♀ アラートおよびイベント										
🗹 監査トレイル										
� ツール										
回 レポート										
◎ ファームウェア										

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。再起動は行われません。

다 cafe-ap 이	10 ロ アクセスポイント スイッチ	\$ 7-1-71-1	
- 1212	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 VPN サービス システム IoT 設定監査	詳細を隠す
88 概要			
😁 デバイス	アクセスポイント / 70:3A:0E:C9	EF:6C	
ロ クライアント			
豊 ゲスト	基本情報 ラジオ 設置タイプ	アップリンク メッシュ	
■ アプリケーション			
🔮 セキュリティ	石町:	1442	
- 分析	AP ゾーン:		
D 77-18204421	RF ゾーン:		
	クラスタモード:	9529 T	
		Restort V	
	DALF C-F		
◎ ファームウェア	優先コンダクタ:		
	アクセスポイントの IP アドレス:	□ IP アドレスを DHCP サーバーから取得	
		 スタティック 	
	IP アドレス:	192.168.1.30 変更を有効にするには AP を再起動します。	
	ネットマスク:	255.255.255.0	
	デフォルトゲートウェイ:	192.168.1.1	
	DNS サーバー:	8.8.8.8	
	ドメイン名:		
		(Cancel Save Settings



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させる、

II CAFE-AP	していたいです。 アクセスポイント スイ	■ @ (ッチ ゲートウェイ					ıl. ₩₩ (33.5
1111 88 概要	アクセスボイント 5	・オンライン ●オフ 5 0	ライン ラジオ 11				
😑 デバイス	アクセスポイント (5))					± (
ロ クライアント	▼ デバイス名	ステータス	▼ 仮想コントローラ	Ÿ₽7ド	▼ モデ	マシリアル	ファームウェアバージョン
	70.34			17.	AP-225	0	6.5.4.15_73677
話 ケスト	AU1-2	 Online 	AUI-2F-IAP-VC	17:	AP-535	CP	8.6.0.9_79813
圓 アプリケーション	7F-Mi	 Online 	AUI-7F-IAP-VC	10.	AP-515	Ct	8.8.0.1_80393
セキュリティ	AUI-7	 Online 	AUII-7F-IAP-VC	10.	AP-555	CP	8.8.0.1_80393
0.85	WP-2	 Online 	IMP-2F-POC	17:	AP-205	C)	6.5.4.15_73677
コレポート							
単守							1 item(s) selected
g , , - M/L/							7408

⑤ 確認画面にて"はい"を選択し、再起動する

ľ		×
ds	この AP に接続しているすべてのクライアントが切断されます。 いいえ はい	
	設定ステータス Unsynchronized	š1.7

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。

4.5 優先マスター設定

"優先マスター"設定をしておくことで、仮想コントローラは常に指定した Instant AP で稼動をするようになります。 "優先マスター"に障害が 発生した場合は、一時的に他の Instant AP にマスターが引き継がれますが、 "優先マスター"が復旧した場合は設定した Instant AP に戻り ます。管理上必要な場合に設定を行います。

① フィルターからグループを選択





② デバイスメニューより設定アイコンをクリックし、優先マスターに設定する AP を選択し、右の鉛筆マークをクリック

II CAFE-AP O	79セスポイン)	コスイッチ	-+?x1						<u></u>	i≣ 9XF
12 II.	WLAN 798	スポイント ラジオ	インターフェイス	セキュリティ	VPN サービス	システム R	推进乐组 To			IT ALL S
8 概要										
デバイス	アクセス	ポイント (5)								6
	6.0	VC 6	ステータス	IP アドレス	IP割り出て	$\mathcal{L}\!=\!\mathbb{R}$	917	2.46Hz{\$7	56Hz(F773	アクション
1 271721	AU1-2	AUI-2F-UIP-VC	Up	175	DHCP	access	AP-535	Auto	Auto	
⊾ ゲスト	1AP-2	IAP-2F-POC	Up	175	STATIC	access	AP-205	Auto	Auto	_
アプリケーション	70:3a	WP-2F-POC	Up	175	DHCP	access	AP-225	Ado	Auto	1
	AL8-7	AUI-7F-IAP-VC	Up	10.	DHCP	access	AP-555	Auto	Auto	
* セキュリティ	215-Ma	AUI-7F-IAP-VC	Up	10.	DHCP	access	AP-515	Auto	Auto	
0 81										
フラートおよびイベント										
監査トレイル										
ツール										
コレポート										
89										
77-10-7										

③ "優先コンダクタ"を有効にして"設定の保存"をクリック

🖬 CAFE-AP 📀		@ 7-トウェイ	ni. 🗮 🧕
- 1112	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 VPN サービス システム IoT 設定監査	詳細を隠す
88 概要			
😁 デバイス	アクセスポイント / 70:3.		
ロ クライアント			
豊 ゲスト	基本情報 ラジオ 設置タイ	ブ アップリンク メッシュ	
囲 アプリケーション			
😧 セキュリティ	名称:	IAP2	
- 98	AP ゾーン:		
♪ アラートおよびイベント	RF ゾーン:		
■ 監査トレイル			
ヘ ツール	クラスタモード:	7727	
回 レポート	$LACP \equiv - F$	パッシブ	
- 保守	優先コンダクタ:	✓ 変更を有効にするには AP を再起動します。	
ファームウェア	アクセスボイントの IP アドレス:	● IP アドレスを DHCP サーバーから取卵	
			Cancel Save Settings



④ この設定を有効とするには AP の再起動が必要なため、デバイス一覧に戻って再起動する。

● 振天 5 0 11 ● グパイス アグセスポイント (5) ●	12 T	アクセスポイント	・オンライン ・オフ	ライン ラジオ				
デバイス アクセスボイント (5) マリアル マリアル マリアル マリアル ファームウェアバージョン マグライアント な グスト マグリアル マグリアル マリアル	19 概要	5	5 0	11				
▲ クライアシト ▼ デバイス名 ステークス ▼ 数型 シトローラ ♥ ピアド… ♥ モデ… ♥ シリアル ファムクェアバージョン ・ グスト ・ 〇 パパシ ・ ○ パッパシ ・ ○ パパシ	🖰 デバイス	アクセスポイント (5	5)					بلغ ا
P2x1 Online MA25FOC 1 AA225 C 6.5.4.15,73677 MAR2 • Online AJ&2F-MA-VC 17 AP535 C 8.6.0.9,79813 P7J97->>>> 7FM • Online AJ&7F-MA-VC 10 AP515 C 8.6.0.9,79813 P7J97 AMR7 • Online AJ&7F-MA-VC 10 AP515 C 8.8.0.1,80393 * 0** • Online AJ&7F-MA-VC 10 AP555 C 8.8.0.1,80393 * 0** • Online MA-25FPOC 17 AP.205 C 6.5.4.15,73677 *** • Online MA-25FPOC 17 AP.205 C 6.5.4.15,73677 *** • Online MA-25FPOC 17 AP.205 C 6.5.4.15,73677 *** *** • Online MA-25FPOC 17 AP.205 C 6.5.4.15,73677 *** *** •** •** *** *** *** *** *** *** ** ** *** </th <th>□ クライアント</th> <th>▼ デバイス名</th> <th>ステータス</th> <th>▼ 仮想コントローラ</th> <th>Ÿ₽7ド</th> <th>₹ €<i>7</i></th> <th>▼ シリアル</th> <th>ファームウェアバージョン</th>	□ クライアント	▼ デバイス名	ステータス	▼ 仮想コントローラ	Ÿ₽7ド	₹ € <i>7</i>	▼ シリアル	ファームウェアバージョン
AUR2 • Online AUR2/FIAP-VC 17. AP-535 C 8.6.0.9.79813 I アプリケーション 7F-M • Online AUR7/FIAP-VC 10. AP-535 C 8.8.0.1,80393 I セキュリティ AUR7 • Online AUR7/FIAP-VC 10. AP-535 C 8.8.0.1,80393 I セキュリティ AUR7 • Online AUR7/FIAP-VC 10. AP-535 C 8.8.0.1,80393 I セキュリティ WP-2 • Online MP-2FPOC 17. AP-205 C 6.5.4.15,73677 I 監査トレイル I Uパート IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		70.3a			17	AP-225	- C	6.5.4.15_73677
アプリケーション アF-M • Online AUE-7F-MP-VC 10. AP-515 C1 88.0.1_80393 * セキュリティ • Online AUE-7 • Online AUE-7F-MP-VC 10. AP-555 C1 88.0.1_80393 * ジート • Online AUE-7F-VP-VC 17. AP-205 C1 6.5.4.15_73677 * ジール • ジール • レポート * ジール • レポート • レポート <t< td=""><td>4 7 X F</td><td>AU1-2</td><td>Online</td><td>AUI-2F-IAP-VC</td><td>17:</td><td>AP-535</td><td>C?</td><td>8.6.0.9_79813</td></t<>	4 7 X F	AU1-2	Online	AUI-2F-IAP-VC	17:	AP-535	C?	8.6.0.9_79813
セキュリティ AUB-7 - Online AUB-77-VAP-VC 10. AP-555 CP 8.8.0.1_80393 900 - DPラートおよびイベント - Online VMP-26-POC 17. AP-205 CP 6.5.4.15_73677 10 エージー - DP - DP </td <td>目 アプリケーション</td> <td>7F-M6</td> <td>Online</td> <td>AUI-7F-IAP-VC</td> <td>10.</td> <td>AP-515</td> <td>C1</td> <td>8.8.0.1_80393</td>	目 アプリケーション	7F-M6	Online	AUI-7F-IAP-VC	10.	AP-515	C1	8.8.0.1_80393
WP-2 • Online WP-2F-POC 17. AP-205 CP 6.5.4.15_73677 2 空売ートおよびイベント 3 空売トレイル 2 空売 ・ Online レアント ・ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	0 セキュリティ	AUI-7	 Online 	AUI-7F-IAP-VC	10.	AP-555	Cf	8.8.0.1_80393
 アラートおよびイベント 聖査トレイル ツール レポート ⁽¹⁾ item(s) selects 	0.85	IAP-2	 Online 	IAP-2F-POC	17:	AP-205	C)	6.5.4.15_73677
3 監査トレイル シール 3 レポート 1 item(s) selector 4 つ) アラートおよびイベント							
レザール 1 レポート 1 item(s) selects	監査トレイル							
」レポート Rで	ツール							
1 item(s) selecte] レポート							
								1 item(s) selected



4.6 NTP 設定

IAP 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

ຂ ∕⁄⊐–/ໃλ	5 ネットワーク健全性	〇 WAN 開会性 概要	w
ミグローバル			
フィルタリスト			
ログループ	助サイト	03×11	
anp Getter	Сай 14 Ж£977- Ш?	CARE-37 1075 50 Branch Dema 4:08847	

② 左メニューよりデバイスを選択し、右上の 🍄 をクリック

티 CAFE-AP 이	アクセスポイント	□ ® スイッチ ゲートウェイ					1. 🗮 🗮
- 111 88 45.0	アクセスポイント 5	・オンライン 0オフ 5 0	ライン ラジオ 11				
デバイス	アクセスポイント	(5)					₹Θ
ロ クライアント	▼ デバイス名	ステータス	▼ 仮想コントローラ	Y IP 7 F	Y t7	マシリアル	ファームウェアバージョン
	AUR-	Online	AU	17	AP-535	0	8.6.0.9_79813
島 ゲスト	79:3	Online	64P	17	AP-225	CT	6.5.4.15_73677
圖 アプリケーション	MP-	Online	DAP.	17	AP-205	CA.	6.5.4.15,73677
Ø セキュリティ	27-A	 Online 	ALK	10	AP-515	0	8.8.0.1_80393
	AUI-	Online	AUX	10	AP-555	0	8.8.0.1_80393
 ○ アラートおよびイベント ○ 監査トレイル ヘ ツール ○ レポート - 保守 ○ ファームウェア 							



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"

II CAFE-AP	フクセスポイント スイッチ				uh. (⊟. (∰. (∰. (∰. (∰. (∰. (∰. (∰. (∰. (∰. (∰
- 112	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 VPN サービス システム	IoT 設定監査	詳細を隠す
88 概要				-	
🎯 デバイス	システム				
ロ クライアント	◇ 一般				
息 ゲスト	仮想コントローラ				
圓 アプリケーション	8.0	P アドレス	1Pv6 7 F L 2	(B) D -	=
セキュリティ	AUI-2F-IAP-VC			123	
- 分析	AUI-7F-IAP-VC			193	
アラートおよびイベント	IAP-2F-POC			JP3	
■ 監査トレイル	5 10 25 50 1-40-	ジあたり			IC C > N M-Stan
	クループの国コードを取り	EA 0 :	JP3 - Japan	· · ·	
· 37	タイムゾーン :		東京 UTC+09	•	
9 //-M/1/	優先周波数等:		রম্ব 🔻		

4.6.1 時刻同期の確認1(GUI)

 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

II CAFE-AP 이	8 ネットワークチェック	אעדב			
- 1111 88 根要	デバイスタイプとデバイス 7バイスタイプ アクセスポイント	(を選択し、コマン	ドを追加してコマンドを実行します ##FE&ながバイス 〜		
🖽 デバイス	1つ以上のカテゴリからコ	1マンドを選択して	ください		
□ クライアント	カテゴリ		ע אעצבγ		コマンドの運営
豊 ゲスト 囲 アプリケーション ♥ セキュリティ 	All Category Wreless Security Network Airgroup		AP 3G/4G Status AP Allowed Channels AP Allowed MAX-EIRP AP Association Table AP Client Match History	道加> < 削除 <すべて削除	AP BSSID Table
 ↓ アラートおよびイベント ◎ 監査トレイル ◆ ツール 	0		47 コマンド ・ 追加の必須フィルタをサポートします ・ 追加のオプションフィルタをサポートします ト - Cannot run with other commands		1.コマンド このコマンドリストは、その順序で実行されます。 (厳大は 20 です)
 レポート 保守	既にコマンドを実行し バッファスペースの問題 一部のコマンドでは、)	ているデバイスで、 1があるデバイスの 15力を表示するたけ	新しく追加されたコマンドを実行してはなりません < <p>(出力環理は自動的に消去されます めにログレベルをデバッグに設定する必要があります。</p>		
⊜ ファームウェア	**	Vtyk)		



4.6.2 時刻同期の確認2(GUI コンソール)

Central では GUI から AP のコンソールがひらけます

- ① グループを選択>ツール>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

🛱 CAFE-AP 📀	なットワークチェック コマンド コンソール
- 8.6	リモートコンソールセッション
88 概要	範規セッション 保存済みセッション
🖽 デバイス	91112017 V
ロ クライアント	
豊 ゲスト	
囲 アプリケーション	リモートコンソール
セキュリティ	注意 デバイスのコンソールセッション:AL ② No Session Found ▼ Q ③ C
- 98	admini@AU *
☆ アラートおよびイベント	Host 'localhost' key accepted unconditionally. (ssh-rsa fingerprint md5 14:50:03
図 監査トレイル	
≤ ツール	show tech-support and show tech-support supplemental are the two most useful outputs to collect for any kind of troubles hooting session.
ロレポート	AUI-7F-IAF-VC# show clock
- 99	Current Time :2021-06-26 04:53:30 AUI-77-IAP-VC#
ロファームウェア	



4.7. ダイナミック Radius プロキシ

外部の Radius サーバへ認証を行う際、ダイナミック Radius プロキシを利用することで、認証パケットは仮想コントローラを経由させることが できます。(この設定をしていない場合は AP 毎に外部 Radius に認証を行います。)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

金 グローバル	0 ネットワーク健全性	〇 WAN 健全性 概要 Wi
<i>≙グロ−バル</i>		
▼ フィルタリスト		
ログループ	助サイト	09KJL
anp Cott.AP	CNE VC 東京9万一 副子	CARE-39 10PS 50 Branch Demo 4:08849

② 左メニューよりデバイスを選択し、右上の ²³ をクリック

디 CAFE-AP 이	10 アクセスポイント ス・	ロ ゆ イッチ ゲートウェイ					#. <u>≡</u> ₩₩ ¹ 785
22 9 #2	アクセスボイント 5	・オンライン 0オフ 5 0	ライン ラジオ 11				
3 デバイス	アクセスポイント (5)					±€
3 クライアント	▼ デバイス名	ステータス	▼ 仮想コントローラ	Y IP 7 F	Y +7	マシリアル	ファームウェアバージョン
	AUF	Online	AU	17	AP-535	0	8.6.0.9_79813
1 グスト	79:3	Online	UAP-	17	AP-225	CT	6.5.4.15,73677
アプリケーション	MPS .	Online	MP.	17	AP-205	CA.	6.5.4.15_73677
サキュリティ	77-8	Online	ALE	10	AP-515	05	8.8.0.1_80393
	AU-	Online	ALE	10	AP-555	05	8.8.0.1_80393
 ○ アラートおよびイベント ○ 監査トレイル ヘ ツール ○ レポート ※? ● ファームウェア 							



③ "詳細を表示"をクリックし、システムタブをクリック
 "ダイナミック RADIUS プロキシ"を有効にし"設定の保存"

II CAFEAP O	77セスポイント スイッチ デートウェイ		al 🔠 🤮
- 111	WAN アクセスポイント ラジオ インターフェイス	10キュリティ VPN ワービス 5-3.74 107 副定覧意	詳細を除す
88 M.W.			
<u>6</u> FR12	システム		
D クライアント	✓ —#		
星 ゲスト			
圖 アプリケーション	Name Ipaddr	tpvfaddr Country	Actions 🗮
セキュリティ	AUX-2F-IAP-VC	193	
0 79-ba20462b	ALI-7F-IAP-VC	P3	
1 聖音トレイル	WP-2F-POC	<i>p</i> 3	
4 7−5	3 10 25 50 1-4-5/8±0		K < > > H A-MM
日レポート	グループの借コードを設定する	JPD - Japan	
- 87	タイムゾーン	RIE UTC-00	
Ø 77−49±7			
	张九月次回 号:		
	NTP 77-17-:	mpinict.jp	
	仮想コントローラのネットマスク:		
	仮想コントローラのグートウェイ:		
	仮想コントローラの DNS		
	仮想コントローラの VLAN:		
	DHCP ボブション N2 XML:	•	
	ダイナミック CPU 使用量:	0.00 ¥	
	自動振動モード:		
	Pv6 管理を許可:		
	アップリンクスイッチネイティブ VLAN:		
	ターミナルアウセス:		
	ログインセッションのタイムアウト:	5	
	コンソールアウセス:		
	WebUI 79±2:		
	Teinet 7 - / - :		
	LED WIR:		
	監要 550 :		
	展開なゾーン:		
		~	
	ユーザー開ロアリッジングを配合!		
	ローカルルーディングを影響:		
	ダイナミック NADIUS プロキシ :		
	ダイナミック TACACS プロキシ:		
	クラスタセキュリティ:		
	6.83 m		
		~	

4.8. 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 を付与したり、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

5	アクセスポイント 5	・オンライン ●オフ 5 0	ライン ラジオ 11				
デバイス	アクセスポイント (5)					ŧ
クライアント	▼ デバイス名	ステータス	▼ 仮想コントローラ	Y IP 7 K	▼ ₹ <i>F</i>	▼ シリアル	ファームウェアバージョン
	AUI-	Online	AU	17	AP-535	0	8.6.0.9_79813
7.7.1	79.3	Online	UNP-	17	AP-225	CT	6.5.4.15_73677
アプリケーション	MPN .	Online	MP.	17	AP-205	Ch.	6.5.4.15_73677
ビネッリティ	7F-8	Online	ALX	10	AP-515	05	8.8.0.1_80393
	AU	Online	AUX	10	AP-555	0	8.8.0.1_80393
アラートおよびイベント							
i査トレイル /=!!							



- 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

II CAFE-AP 이	つ アクセスポイント スイッチ グートウェイ	-	јШ УХР
- 1112	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 VPN サービス システム 167 設定監査		詳細を見
88 概要	> AirGroup		
😑 デバイス	> リアルタイム位置情報システム		
ロ クライアント	> OpenDNS		
豊 ゲスト	CALEA		
圃 アプリケーション			
セキュリティ	> ネットワーク統合		
- 52.01	> ダイナミック DNS		
♪ アラートおよびイベント	✓ AppRF™		
■ 監査トレイル	詳細なパケット検査: すべて ▼		
ヘッツール			
直 レポート	アプリケーションのモニタリ		
- 保守	ング:		
◎ ファームウェア	AirSlice ポリシー:		
	> SIP		

4.9. 工場出荷状態への戻し方

4.9.1 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 基本操作ガイド(入門編)を参照

https://www.hpe.com/psnow/doc/a00143744jpn

4.9.2 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

म ः	
- 112	リモートコンソールセッション
88 概要	新規セッション 保存済みセッション
デバイス	デバイスタイプ *
D クライアント	
塁 ゲスト	
囲 アプリケーション	リモートコンソール
セキュリティ	注意 デバイスのコンソールセッション: 20: ① Current Session ▼ Q ③ ○ ○
- 98	admin()21 (05:48:54 PM) 🖌 × + dbclient:
☆ アラートおよびイベント	Host 'localhost' key accepted unconditionally. (ash-rsa fingerprint md5 el:0e:aa:9e:ab:90:e4:9
図 監査トレイル へ ツール	show tech-support and show tech-support supplemental are the two most useful outputs to collect for any kind of troubles hooting session.
山 レポート	20:4c:0 Are you sure you want to erase the configuration? (y/n):
- 保守	
◎ ファームウェア	



4.9.3 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。



4.9.4 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



Technical Note HPE Aruba Networking Central 基本操作ガイド IAP 編

M COM5 - Tera Term VT \times _ ファイル(E) 編集(E) 設定(S) コントロール(Q) ウィンドウ(W) ヘルプ(H) APBoot 1.5.5.7 (build 56398) Built: 2016-09-08 at 14:21:29 Model: AP-31× DRAM: 491 MB SF: Detected MX25U3235F with page size 64 kB, total 4 MB Flash: 4 MB NAND: 132 MiB PCIE0: link up °CIE1: link up dev fn venID devID class 00 00 168c 0046 00002 MBARO MBAR1 MBAR2 MBAR3 rev 00 00000004 0000000 00000000 00000000 dev fn venID devID class MBARO MBAR1 MBAR2 MBAR3 rev 00 00 168c 0040 00002 00 00000004 0000000 00000000 00000000 Power: 802.3af POE serial In: Out: serial Err: serial Net: eth0 Radio: qca9983#0, qca9990#1 Reset: cold ***** Configuration Reset Requested by User **** Clearing state... Checking OS image and flags

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

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

顧客: Aruba Mina	ト ネットワーク健全性		Will a
◎ グローバル ○	ホットソーク隆王正	WAN RELL WAS	
黛グローバル			
▼ フィルタリスト			
はグループ	■サイト	<i>⊘</i> ラベル	
HOME-AOS10			-

② 左メニューよりデバイスを選択し、右上の ³³をクリック

顧客: Aruba Mina	う アクセスポイント						山田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田
ଘ номе-аоs10 이	アクセスボイント ・オンライ	イン •オフライン ラジオ					
- 管理	1 1	0 2					
88 概要	アクセスポイント (1)						₹ Θ
📴 デバイス	マ デバイス名	ステータス	▼ 仮想コントローラ	Ţ IP アドレス	▼ モデル	▽ シリアル	ファームウェアバージョン
クライアント	505H	Online		192	AP-505H	CNL	0.4.0.0_86033
塁 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							
🖾 監査トレイル							
🔦 ツール							
直 レポート							
- 保守							
◎ ファームウェア							
1: 組織							



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

顧客: Aruba Mina	う アクセスポイント	
路 номе-аоs10 이	WLAN アクセスポイント ラジオ インターフォ	パス セキュリティ サービス シス
- 管理		
88 概要	√ 有線	
<u></u> 「デバイス	有線ボートプロファイル (1)	
□ クライアント	Display Name	Actions
島 ゲスト	default_wired_port_profile	
用 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		
🖾 監査トレイル		
ペ ツール	┼ ボートブロファイルの追加	1 ポートプロファイル
画 レポート	> アップリンク	
- 保守		
⊕ ファームウェア		
b 組織		

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

顧客: Aruba Mina	0 アクサスポイント		11. 60.00	
업 HOME-AOS10 〇	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 股灾能変		詳細を隠す
- 管理				
88 概要	新しいネットワークの作成			
🧐 デバイス	 一般 ② VLAN ③ セキュリティ 	④ アクセス ③ 概要		
🗔 クライアント	名前-	test-portprofile		
二 ゲスト		contraction of the second seco		
■ アプリケーション	ports:	イーサネット =		
 セキュリティ 分析 	◇ 詳細設定			
♪ アラートおよびイベン	達度/デュプレックス・			
🖾 監査トレイル				
🗞 ツール	ポートモード:	ダウンリンク/非ポンディング状態		
回 レポート	Power over Ethernet (パワーオーバーイーサネット) :			
⑦ ファームウェア	管理ステータス:	稼動中 ▼		
社 相關	スパニングツリー:			
	無通信のタイムアウト:	1000		
	802.3az:			
	VLAN 内トラフィックを拒否:			
		*	ャンセル	(次へ)



⑤ モードをアクセスにし、"次へ"をクリック

顧客: Aruba Mina	し アクセスポイント	Ⅱ」 注 (1) 概要 リスト (1)2
업 HOME-AOS10 〇	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 設定販音	詳細を隠す
- 管理		ar was to not y
日2 概要	新しいネットワークの作成	
『デバイス	1 一般 2 VLAN ③ セキュリティ ④ アクセス ⑤ 概要	
ロ クライアント	7/147	
<u>ニ</u> ゲスト		
■ アプリケーション	トラフィック転送モード:	
♥ セキュリティ	アクセス VLAN: 1	
- 分析	VLAN の割り当てルール	
☆ アラートおよびイベント		
🛛 監査トレイル		
& ツール		
直 レポート		
ゆ ファームウェア		
5 · · · · · · · · · · · · · · · · · · ·	No data to display	
Le (BLATHY		
	+ ルールの窓加 0 ルール	
	> 名前付き VLAN を表示	
	キャンセル) 戻る 次へ

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

顧客: Aruba Mina		由概要	
ଘ HOME-AOS10 〇	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			
器 概要	新しいネットワークの作成		
@ デバイス	1 一般 2 VLAN 3 セキュリティ 4 アクセス ⑤ 概要		
ニ ゲスト	802.1X 認証 MAC 認証 ビジター オープン		
■ アプリケーション			
😯 セキュリティ	▲ これはセキュリティ保護されていないネットワークです。ユーザーは認証なしでネットワークに接続します。		
- 分析			
☆ アラートおよびイベント	Trusted ポート :		
🛛 監査トレイル			
& ツール	> 詳細設定		
🖬 レポート			
いた いた いた いた いた した した した した した した した した した し	キャンセル	戻る] <u></u> 次へ



 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

顧客: Aruba Mina	0 70+0 3#/2 V.k	山。	:■ ジスト 設定
ដ HOME-AOS10 🛛	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			
品 概要	新しいネットワークの作成		
◎ デバイス	1 一般 2 VLAN 3 セキュリティ 4 アクセス ⑤ 概要		
ロ クライアント			
ぷ ゲスト			
■ アプリケーション			
😯 セキュリティ	▲割限なし]オブションを選択すると、ネットワークへの完全なアクセスが許可されます。これによ		
- 分析	り、潜在的なセキュリティの問題が生じる可能性があります。		
♪ アラートおよびイベン…			
🛛 監査トレイル			
ペ ツール			
山 レポート			
- 保守			
☺ ファームウェア			
造 組織			
	キャンセル	戻る	次へ

⑧ 概要を確認し、間違いがなければ"終了"をクリック

顧客: Aruba Mina	う アクセスポイント			山. 注三 (概要 リスト (2)	<mark>3</mark> 徒
ដ HOME-AOS10 〇	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	vステム IoT 設定監査	詳細を履	隠す
- 管理					
品 概要	新しいネットワークの作成				
回 デバイス	1 一般 2 VLA	N 3 セキュリティ 4 アクセ	ス 5 概要		
ロ クライアント	ネットワーク概要				
ニ ゲスト	全般		VLAN		
■ アプリケーション	名前	test-wired	VLAN モード	access	
😯 セキュリティ	SPEED	auto	トラフィック転送モード	ブリッジ	
 分析 クーフラートやトバイベント 	デュプレックス	auto	VLAN	1	
□ F かんしくし	主な用途	employee			
	PoE	有効	セキュリティ		
	管理ステータス	稼動中	MAC 認証	無効	
- 保守	アップリンク	無効	アクセス		
@ ファームウェア			認証済みユーザーのロール割り当て	無効	
と 組織			MAC 認証のみのロールを強制	無効	
			認証前のロール	無効	
			コンピュータ認証を強制	無効	
					_
				キャンセル 戻る 終了	



SSID の設定 6

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
 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

顧客: Aruba Mina	で アクセスズ	ポイント										山 概要	:三 リスト 設定
ជ номе-аоѕ10 🛛	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													
品 概要	無約	泉SSID											
回 デバイス	4	名前 (プロファイル)		セキュリティ	アク	セスタイプ		トラフ	フィック転送	ŠŦ	ネットワーク有効		
ニ ゲスト							F.						
■ アプリケーション							Í.		E				
♥ セキュリティ													
- 分析							No data to	o displa	ay.				
♪ アラートおよびイベント													
🛛 監査トレイル													0.5510
ペ ツール	+	- SSID の追加											0.221D
向 レポート													
- 保守													
@ ファームウェア													
皆 組織													

④ 名前(SSID)を指定し、"次へ"をクリック

顧客: Aruba Mina		山	
다 номе-аоs10 〇	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			armer center y
品 概要	新しいネットワークの作成		
◎ デバイス	 一般 ジ VLAN ジ セキュリティ ④ アクセス ⑤ 概要 		
ロ クライアント	名前 (CCID)- tect		
ぷ ゲスト	עוורכן נאבי.		
■ アプリケーション	> 詳細設定		
€ セキュリティ			
- 分析			
♪ アラートおよびイベント	Г	キャンセル	次へ
🛛 監査トレイル			
ミ ツール			
山 レポート			
C SET 148			


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

<u>トラフィック転送モード</u>

"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。

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 を利用したり、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。

顧客: Aruba Mina	1 アクセスポイント 	Ⅰ :三 200 夏 リスト 設定
ជ HOME-AOS10 🛛	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		
H 概要	新しいネットワークの作成	
<i>◎ デバ</i> イス	1 一般 2 VLAN ③ セキュリティ ④ アクセス ⑤ 概要	
ロ クライアント	トラフィックを送来」に	
ぷ ゲスト		
■ アプリケーション	クライアント VLAN の割り当て: スタティック ダイナミック ● ネイティブ VLAN	
😯 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	キャンセル	える 次へ
ミ ツール		
山 レポート		
保守		
☺ ファームウェア		
と 組織		



Technical Note

HPE Aruba Networking Central 基本操作ガイド IAP 編

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

顧客: Aruba Mina	し アクセスポイント	山 :三 (2) 概要 リスト (2) 設定
ଘ HOME-AOS10 〇	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 loT 設定監査	詳細を隠す
- 管理		
品 概要	新しいネットワークの作成	
回 デバイス	1 一般 2 VLAN 3 セキュリティ 4 アクセス 5 概要	
ロ クライアント		
ぷ ゲスト	ロールペース、ネットワークペース、創限なし	
▦ アプリケーション		
€ セキュリティ	▲刺風なし]オプションを選択すると、ネットワークへの完全なアクセスが許可さ	
- 分析	れます。これにより、潜在的なセキュリティの問題が生じる可能性があります。	
♪ アラートおよびイベント		
🗷 監査トレイル		
ミ ツール		
鼠 レポート		
- 保守		
☺ ファームウェア		
と 組織		
	キャンセル	戻る次へ

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



Technical Note

HPE Aruba Networking Central 基本操作ガイド IAP 編

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
 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

顧客: Aruba Mina	で アクセス	う .ポイント										11. 概要) リスト
រំ номе-аоѕ10 💦	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;
行理													
概要	無	線SSID											
〕 デバイス		名前 (プロファイル)		セキュリティ	アク	セスタイプ		トラ	フィック転送	τ	ネットワーク有効		
クライアント													
ゲスト							F.						
] アプリケーション							('E	Ē	Ē				
セキュリティ							t.						
祈							No data te	o displa	ay				
、アラートおよびイベント													
監査トレイル													0.001
、ツール	+	- SSID の追加											U SSIL
レポート													
安													
⊧ ファームウェア													

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

顧客: Aruba Mina	70471	ポイント									山、	Ⅲ (②) リスト (②)	
ធ номе-аоѕ10	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			詳細を隠っ	す
管理													
品 概要	新しい	ヽネットワークの	作成										
回 デバイス) 一般 (2 VLAN	3 t‡	ュリティ	 アク 	セス	5	慨要				
ロ クライアント		名前 (SSID):			OP	-N	_						
ድ ゲスト		(310).				-14							
▦ アプリケーション	>	詳細設定											
😯 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											447200		
冬 ツール													
応 レポート													
- 保守													
⑦ ファームウェア													
と 組織													

Technical Note HPE Aruba Networking Central 基本操作ガイド IAP 編

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

顧客: Aruba Mina	1 アクセスポイント 概要 ジン	三 😥
篇 HOME-AOS10 〇	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	新しいネットワークの作成	
回 デバイス	 一般 2 VLAN 3 セキュリティ 4 アクセス 5 概要 	
「ロ クライアント	トラフィック転送モード・	
ぷ ゲスト		
聞 アプリケーション	クライアント VLAN の割り当て: ダイナミック ダイナミック ネイディブ VLAN	
😯 セキュリティ	VLAN ID: ▼ 複数の VLAN ID または単一の名前付き VLAN が許可されます。	
- 分析	> 名前付き VLAN を表示	
♪ アラートおよびイベント		
☑ 監査トレイル		
ミ ツール		
直 レポート	キャンセル 戻る	次へ
- 保守		
③ ノアームウェア		
と組織		

⑥ 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

顧客: Aruba Mina		山、枳実	
ជ номе-аоѕ10 〇	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			
H 概要	新しいネットワークの作成		
回 デバイス	1 一般 2 VLAN 3 セキュリティ 4 アクセス 5 概要		
ロ クライアント			
ぷ ゲスト	セキュリティレベル:		
■ アプリケーション	エンタープライズ パーソナル ビジター オープン		
😯 セキュリティ			
- 分析	🔬 これはセキュリティ保護されていないネットワークです。ユーザーは認証なしでネットワークに接続します。		
☆ アラートおよびイベント			
☑ 監査トレイル	キー管理: エンハンストオープン ▼		
ミ ツール	際早心・ カレ		
応 レポート	181 JU. NOV		
- 保守	> 詳細設定		
2 組織			
	キャンセル	戻る	次へ



Page 41

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
 第タンをクリック
 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

顧客: Aruba Mina	アクセス) ポイント										山、横要	∷≣ リスト 設定
법 НОМЕ-АОЅ10 〇	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													
品 概要	無約	線SSID											
回 デバイス	4	名前 (プロファイル)		セキュリティ	アク	セスタイプ		トラフ	フィック転送	送モ	ネットワーク有効		
ロ クライアント													
ニ ゲスト							-E.						
■ アプリケーション							(E		E				
😯 セキュリティ							\checkmark						
- 分析							No data to	o displa	iy				
♪ アラートおよびイベント													
🖪 監査トレイル													0.551D
ペ ツール	+	- 2210 の追加											0 5510
驘 レポート													
- 保守													
☺ ファームウェア													
b 組織													

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

顧客: Aruba Mina		山	Ⅲ ジスト 設定
ଘ HOME-AOS10 〇	アノビスポイント 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 設定能査		詳細を隠す
- 管理			
品 概要	新しいネットワークの作成		
ie デバイス	 一般 2) VLAN 3) セキュリティ 4) アクセス 5) 概要 		
ロ クライアント			
ヱ , ゲスト	43 B) (133/0).		
▦ アプリケーション	> 詳細設定		
♥ セキュリティ			
- 分析			
♪ アラートおよびイベント	ſ	***	
🛛 監査トレイル	L	++> 210	
ミ ツール			
応 レポート			
- 保守			
⑦ ファームウェア			
と 組織			



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

顧客: Aruba Mina	で アクセスポイント	山 :三 概要 リスト	and the
ដ номе-аоs10 ្	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	詳細を影	急す
- 管理			
88 概要	新しいネットワークの作成		
🧧 デバイス	1 一般 2 VLAN 3 セキュリティ ④ アクセス ⑤ 概要		
ロ クライアント	トニフィックEWAT-12。 ● ブリッグ トンスル 単会		
ぷ ゲスト			
■ アプリケーション	クライアント VLAN の割り当て:		
♥ セキュリティ	VLAN ID: 複数の VLAN ID または単一の名前付き VLAN が許可されます。		
- 分析	→		
↓ アラートおよびイベン			
☑ 監査トレイル			
� ツール			
ඛ レポート	キャンセル	戻る 次へ	
- 保守			۰.
ファームウェア			
皆 組織			

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

顧客: Aruba Mina		
ជ номе-аоs10 ្	VLAN 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		
88 概要	新しいネットワークの作成	
🧧 デバイス	1 一般 2 VLAN 3 セキュリティ ④ アクセス ⑤ 概要	
ロ クライアント		
ぷ ゲスト	セキュリティレベル:	
■ アプリケーション	エンタープライズ パーソナル ビジター オープン	
😯 セキュリティ		
- 分析	キー管理: WPA3 パーソナル ▼	
♪ アラートおよびイベン…		
🛛 監査トレイル	パスフレーズの形式: 8~63文字 🔻	
& ツール	パスフレーズ:	
直 レポート		
- 保守	舟入力:	
◎ ファームウェア	> 詳細設定	
b 組織		
	キャンセル	戻る次へ



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
 第タンをクリック
 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

顧客: Aruba Mina	0 7212.84225	li :Ξ 概要 リスト
ដ номе-аоs10 ្	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		
BB 概要	無線SSID	
回 デバイス	名前 (プロファイル) セキュリティ アクセスタイプ トラフィック転送モード ネットワーク有効	
ロ クライアント		
島 ゲスト		
圏 アプリケーション	il in E	
😯 セキュリティ		
- 分析	No data to display	
♪ アラートおよびイベン		
🛛 監査トレイル		
ペ ツール	+ 5510 0 JULIU	0 SSID
直 レポート		
- 保守		
☺ ファームウェア		
と 組織		

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

まま Aruba Mina ジャレ ジェレ ・ <th></th> <th></th> <th></th>			
・	顧客: Aruba Mina	0 7017215/215	山 注 🔮
 ● 現 ● 日 ● 日<th>ជ номе-аоs10 이</th><th>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</th><th>詳細を隠す</th>	ជ номе-аоs10 이	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
B 板	- 管理		
 ③ デバイス □ クライアント ③ クリアント ③ クリアント ③ クリアントション ④ アラレトおよびイベン… ③ 弦声トレイル ④ アラートおよびイベン… ● アール ● レポート ● マワームウェア ● 枢線 	BB 概要	新しいネットワークの作成	
□ クライアント ※ グスト ■ アブリケーション ② セキュリティ →# →# ● アラートおよびイペン ② 監査トレイル ④ アラートおよびイペン ② 監査トレイル ④ マラートなし ● ファームウェア 覧 服職	🧧 デバイス	 ① 一般 ② VLAN ③ セキュリティ ④ アクセス ⑤ 概要 	
 ▲ グスト ● ボート・ ● マラートおよびイペン ● ブラートおよびイペン ● レボート・ ● マラームウェア ● 枢線 	ロ クライアント		
 ■ アブリケーション > 詳細設定 > ジール ○ レポート ○ ファームウェア 資 組織 	ぷ ゲスト	名前 (SSID): WPX3-7-3/r1M4L80#E	
 ♥ セキュリティ かガー アラートおよびイベン アラートおよびイベン	■ アプリケーション	> 詳細設定	
 分析 ↓ アラートおよびイペン 図 監査トレイル キャンセル えへ ペ ツール ロ レポート (69) (7) アームウェア 注 組織 	♥ セキュリティ		
 ↓ アラートおよびイベン 図 監査トレイル キャンセル 本 ペ ツール ロ レポート (音)	- 分析		
 図 監査トレイル キャンセル キャンセル ペ ツール ロ レポート - 信守	↓ アラートおよびイベン…		
 ペ ツール ロ レポート (19) マアームウェア 注 組織 	🖸 監査トレイル		キャンセル 次へ
 ロレポート (10) レポート (10) マアームウェア (11) 組織 	🗞 ツール		
 □ (a) (a) (a) (a) (a) (a) (a) (a) (a) (a)	直 レポート		
 ファームウェア 	- 保守		
16 組織	⑦ ファームウェア		
	b 組織		



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

顧客: Aruba Mina	う アクセスポイント	山 注言 概要 リス	
ដ номе-аоs10	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			
88 概要	新しいネットワークの作成		
🙆 デバイス	 一般 2 VLAN ③ セキュリティ ④ アクセス ⑤ 概要 		
ロ クライアント			
ニ ゲスト	トラフィック転送モード: · · · · · · · · · · · · · · · · · · ·		
■ アプリケーション	クライアント VLAN の割り当て: ・ ・ スタティック ・ ダイナミック ネイティブ VLAN		
😯 セキュリティ	VLAN ID:		
- 分析	、 名前付き VI AN を表示		
♪ アラートおよびイベン…			
🗷 監査トレイル			
& ツール			
直 レポート	「キャンセル」「	戻る	次へ
- 保守			
◎ ファームウェア			
b 組織			

 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<u>こちら</u>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

顧客: Aruba Mina	0 7042#4/1	Ⅱ. 注: (3) 概要 リスト (2)
ଘ HOME-AOS10 〇	・ 「WAM 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 ワービス システム 101 設定を言	詳細を語す
- 管理		
88 概要	新しいネットワークの作成	
🙆 デバイス	 ① 一般 ② YLAN ③ 使年国リティ ④ 7クセス ④ 概要 	
ロ クライアント		
<u>ニ</u> ゲスト	ta+aJ9+4V	
田 アブリケーション	エンタープライズ パーソナル ビジター オープン	
😯 セキュリティ		
- 分析	キー管理: VMPA3 パーソナル ▼	
♀ アラートおよびイベント	4771 - TARM	
■ 監査トレイル		
	/\\\.7\L-\.7\:	
	再入力:	
77-4917		
1: 組織		
	MAC IEE:	
	再読証の問題: 0 分 🔻	
	DHCP の強制:	
	WPA3トランジション:	
	ブライマリサーバー: Cloud Auth ▼ +	
	④ 満連ローミング	
	年でンセル	戻る次へ

$\overline{\mathcal{O}}$ 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

顧客: Aruba Mina		は. 注 ⑧ 概要 リスト 第第
ដ HOME-AOS10 ្	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 設定販売	詳細を隠す
管理		
88 概要	新しいネットワークの作成	
📴 デバイス	 ① 一般 ③ セキュリティ ④ アクセス ⑤ 概要 	
ロ クライアント	70+71-0	
ぷ ゲスト		
■ アプリケーション	ロールペースネットワークペーム制度なし	
€ セキュリティ	△割限なし]オブションを選択すると、ネットワークへの完全なアクセスが許可されます。これによ	
- 分析	り、潜在的なセキュリティの問題が生じる可能性があります。	
♪ アラートおよびイベン…		
☑ 監査トレイル		
🔦 ツール		
園 レポート		
- 保守		
⑦ ファームウェア		
と 組織		
	キャンセル	夏 る 次へ

⑧ MAC アドレスの登録

HPE Aruba Networking 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

顧客: Aruba Mina	⑦ RAPIDS 課題および	。 びポリシー (♡ ゲートウェイ IDS/IPS ファイアウォール クライアントロール			1)。 概要	.≣ yz⊧	8 8 8
<i>粂 グローバル</i>								
- 管理			ポリシー					
品 概要			> 「、コーザーアクセスポリシー	1	ō			
回 デバイス			BEBBU ID ストアでIECHIレビンプリアントでBOSECU、ホットソーンパのアンビスで的DBFU ます。	# .*	HIRK			
ロ クライアント			、 巨乳 クライアントアクセスポリシー	î	Ō			
ぷ ゲスト			✓ LII MAC アドレスに基づいてネットワーク内のクライアントを認証し、プロファイリングに基づいてクライアントのアクセスを制御します。	編集	削除			
■ アプリケーション								
😯 セキュリティ								
& ネットワークサービス								
- 分析								
2 監査トレイル								
≪ ツール								
直 レポート								
二三日 アプリカタログ								
-保守								

の ファームウェア 1g 組織





⑨ +ボタンから MAC アドレスを登録する

() RAPIDS	認証およびポリシー	⊖ ゲートウェイ IDS/IPS	⊕ ファイアウォール	口口 クライアントロール						山。 ::: (東 リス	
		MAC 認証 ネットワーク上のクライア	ントを MAC アドレスに	基づいて管理、認証します。							
		許可された MAC アド クライアントデバイスの	レス (2) MAC アドレスがネット	ワークへのアクセスを許可さ	されました。			ຊ + ≩⊺±			
		MAC アドレス			2	ライアント名					
		90			CI	ient-1					
		01			Te	st			-		
							Items per page: 5	1-2 of 2			
		クライアントプロファ	・イルタグとクライ	アントロールのマッピン	ング (1)			1+			
		クライアントプロファイル	レタグをクライアントD	コールに関連付け、優先順位の	の高いものから順番に	並べます。					
		クライアントプロ	/アイルタグ			authenticated		~			
						A					
		Wi-Fi Easy Connect™ は、V Wi-Fi Easy Connect™ は、V	サービス WI-FIO ネットワークに	機器を接続する際の複雑さを	と軽減し、ユーザーエク	マスペリエンスを向上させま	ξŦ,				
		WLAN で使用									
		Select an option	~								
		無効 🖸									
		キャンセル									
_											
ł N	MAC ベー	スのクライ	「アント	を追加							
				<u> </u>							
Ι.	ACT IN LO										
	AC 7 P D										
	000111124		45.53.00								
19	g: 0123456785	MAS まだは 01:23	045757,897	18							
,	クライアント	名*									
	lient-X										
-											
				++	ンセル		保存				



MAC アドレス一覧に追加されていることを確認する

(C) RAPIDS	(ご) 課証およびポリシー	⊘ ⊕ ⊡ がートウェイ IDS/IPS ファイアウォール クライアントロール		山 注 🛞
J		MAC 認証 ネットワーク上のクライアントモ MAC アドレスに基づいて管理、認証します。		
		許可された MAC アドレス (3) クライアントデバイスの MAC アドレスがネットワークへのアクセスを許可されました。	Q + ↑ <u>↓</u>	
		MAC アドレス	クライアント名	
		90	Client-1	
		01:	Test	
		00:00:11:11:22:22 (New)	client-x	
			Items per page: 5 Y 1 - 3 of 3 ()	
		クライアントプロファイルタグとクライアントロールのマッピング(1) クライアントプロファイルタグをクライアントロールに関連付け、優先階位の高いものから得	十 語に並べます。	
		クライアントプロファイルタグ	クライアントロール	
		不特定	authenticated 🔺 🗸	
		Wi-Fi Easy Connect [™] サービス Wi-Fi Easy Connect [™] は、Wi-File ネットワークに積易を提載する際の複雑さを発達し、ユーザ WLAN で使用 Select an option Aruba 100 センサー 4890	ーエクスペリエンスを向上させます。	

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

「⑦		■L 注Ξ 概要 リスト	() 101
MAC 睽証			
ネットワーク上のクライアントを MAC アドレスに基づいて管理、認証します。			
許可された MAC アドレス (3)			
クライアントデバイスの MAC アドレスがネットワークへのアクセスを許可されました。	V + T &		
MACアドレス クライアント名			
90 Client-1			
01 Test			
00:00:11:11:22:22 (New) client-x			
Items per page: 5	✓ 1-3 of 3 < >		
クライアントプロファイルタグとクライアントロールのマッピング(2) クライアントプロファイルタグをクライアントロールに架連付け、毎年時位の高いものから原母に並べます。	+		
クライアントプロファイルタグ クライアントロール			
[Mobile & Gadgets] V WPA3-PSK+MAC	~		
不時定	~		
Wi-Fi Easy Connect™ サービス Wi-Fi Easy Connect™ は、Wi-File ネットワークに機能を接触する際の増強さを経済し、ユーザーエクスペリエンスを向上させます。			
WLAN C'ER			
Select an option			
Andra 100 # 249-			
無効 Z			
キャンヤル	保存		

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 ³ 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

顾客: Aruba Mina	<mark>。</mark> アクセスポイント						
ដ HOME-AOS10 ្	WLAN アクセスボイ	シト 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	oT 設定監査
- 管理							
믬 概要	新しいネットワ	ークの作成					
🧧 デバイス	1 一般	2 VL	AN 3 ta	キュリティ	(4) 77	セス	5 概要
ロ クライアント	名前 (SSI	01:			Dot	1x-CloudAu	th
ぷ ゲスト		~}-					
囲 アプリケーション	> 詳細設定						
♥ セキュリティ							
- 分析							
♀ アラートおよびイベン							
🛛 監査トレイル							
� ツール							
直 レポート							
保守							
☺ ファームウェア							
t; 組織							



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

顧客: Aruba Mina	ほ アクセスポイント	II. ∷⊟ 🥸 ₩₩ IJスト 🙀
ដ HOME-AOS10 ្	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		
器 概要	新しいネットワークの作成	
🧧 デバイス	 1 一般 2 VLAN 3 セキュリティ 4 アクセス 3 概要 	
ロ クライアント	トラフィック販送モード: ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	
ぷ ゲスト		
■ アプリケーション	クライアント VLAN の割り当て: ダイナミック ダイナミック ネイティブ VLAN	
♥ セキュリティ	VLAN ID:	
- 分析	> 2. Sentes VI AN See	
♀ アラートおよびイベン		
🛛 監査トレイル		
≪ ツール		
向 レポート	キャンセル	戻る次へ
- 保守		
◎ ファームウェア		
と 組織		

 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

顧客: Aruba Mina	つ アクセスポイント	
ជ HOME-AOS10 이	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
- 管理		
88 概要	新しいネットワークの作成	
🙆 デバイス	1 —般 2 VLAN	3 セキュリティ ④ アクセス ⑤ 概要
ロ クライアント		
島 ゲスト	セキュリティレベル:	0
囲 アプリケーション		エンタープライズ パーソナル ビジター オープン
😯 セキュリティ		
- 分析	キー管理:	WPA3 エンタープライズ (CCM 128)
♀ アラートおよびイペン	プライマリサーバー・	Cloud Auth
🗹 監査トレイル	224 ¥ 22 = //-:	
& ツール	> 詳細設定	
直 レポート		
- 保守		
☺ ファームウェア		
と組織		

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

顧客: Aruba Mina	B	d. 100	
ជ номе-аоs10 O	アクセスポイント 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 loT 設定監査		詳細を隠す
- 管理			
88 概要	新しいネットワークの作成		
🙆 デバイス	 ① 一般 ② セキュリティ ④ アクセス ⑤ 概要 		
D クライアント ダスト アブリケーション セキュリティ フラートおよびイベン 監査トレイル ペ、ツール レポート ィータ ファームウェア 推 組織	アクセスルール ロールベース ネットワークベース 制限なし 小制限なし]オブションを選択すると、ネットワークへの完全なアクセスが許可されます。これによ り、着在的なセキュリティの問題が生じる可能性があります。		
	キャンセル) 戻 る	次へ

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 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

顧客: Aruba Mina (つ) RAPIDS (認証およびポリシー			11. 夜天	.⊞ 931⊧	() () () () () () () () () () () () () (
<i>℗ グローバル</i> ○					
- 管理	-				
品 概要 、 同	ユーザーアクセスポリシー	ō			
@ デバイス	** 距離の ID ストアを使用してクライアントを認証し、ネットワークへのアクセスを明確します。 ■集	刑除			
ロ クライアント	クライアントアクセスポリシー	ô			
※ ゲスト	MACアドレスに基づいてネットワーク内のクライアントを認証し、プロファイリングに基づいてクライアントのアクセスを制御します。 編集	削除			
アプリケーション					
😵 セキュリティ					
& ネットワークサービス					
- 分析					
☆ アラートおよびイベン					
☑ 監査トレイル					
<i>� ツ</i> −ル					
直 レポート					
- 起動					
アプリカタログ					
- 保守					
@ ファームウェア					
と 組織					



 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

RAPIDS	〇〇 認証およびポリシー	⊘ ⊕ ゲートウェイ IDS/IPS ファイアウォール クラ	丘 ライアントロール		山	1000 UZF	
	ユーザー	RIDE					
	組織の ID ス	トアを使用してクライアントを認証し、ネットワークへのアクセ	スを制御します。				
	~ _	ゲー情報はどこに保存されていますか?		🔥 Microsoft Azure AD 接続済み 🧻			
	ID 7	JK19					
	Δ	Microsoft Azure AD 🗸 🗸	Microsoft Azure AD 向けクイックスタートガイド				
	テナ 9da(v F ID 0485-3098-42a0-8180-c360acaa4a48	クライアント ID d39857e6-061f-4dde-9fb7-26efa369048f				
		表示					
	25	イアント秘密キー					
		リタイレクト URI のコピー	供約				

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

д -	ー ザーグループとクライアントロールのマッピング (1) ストアのユーザーグループをクライアントロールに関連付け、優先順位の高いものから順番に並べ	z. Ţ.	+
	ユーザーグループ	クライアントロール	
	不特定	Dot1x-CloudAuth \lor	

ネットワークプロファイル

コンピューターやスマート デバイスにネットワーク プロファイルをインストールして、ネットワークへの接続を容易にすることができます。Aruba Onboard アプリケーションを使用して、プロフ ァイルを自動的にインストールし、ダウンロード可能なリンクをユーザーと共有します。

組織名 Aruba Minami

Aruba Onboard モバイルアプリプレビュー

非 Passpoint クライアント用の WLAN

Dot1x-CloudAuth

Aruba Minami 服務更新日:2日秋 中的期間: 03/23/2024

MPSK

ユーザーは、クライアントをネットワークに接続するための独自の Wi-FI パスワードを持つことができます。パスワードは、パスワードポータルからログインした後、各ユーザーが利用できます。

MPSK WLAN は使用できません 🕦

キャンセル





6.6 設定例)802.1x External Radius 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 ³ 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

顧客: Aruba Mina	
ដ номе-аоร10	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
- 管理	
88 概要	新しいネットワークの作成
ie デバイス	 一般 2 VLAN 3 セキュリティ ④ アクセス ⑤ 概要
□ クライアント	
≗ ゲスト	名則 (SSID): Dot1x-external
■ アプリケーション	> 詳細設定
😯 セキュリティ	
- 分析	
♀ アラートおよびイペン	
図 監査トレイル	
≪ ツール	
直 レポート	
- 保守	
③ ファームウェア	
2 組織	

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

			_
顧客: Aruba Mina		山、東東	
ដ HOME-AOS10 ្	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			
器 概要	新しいネットワークの作成		
🙆 デバイス	1 一般 2 VLAN 1 セキュリティ ④ アクセス ⑤ 概要		
ロ クライアント			
ニ ゲスト	セキュリティレベル:		
■ アプリケーション	エンタープライズ パーソナル ビジター オープン		
😯 セキュリティ			
- 分析	キー管理: WPA3 エンタープライズ (CCM 128) 🔻		
♪ アラートおよびイベン…			
🛛 監査トレイル	ブライマリサーバー: - 潮沢 ▼ + このフィールドは必須です。		
� ツール	<		
直 レポート	/ ITTHEM/N		
- 保守			
@ ファームウェア			
ध 組織	キャンセル	戻る	次へ



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

ーバータイプ:	RADIUS V	名前:	CPPM	
adSec:		IP アドレス/FQDN:	192.168.11.100	
有キー:		NAS IP アドレス:	オブション	
一の再入力:	••••••	NAS ID:	オプション	
试行回数:	3	認証ボート:	1812	
イムアウト (秒):	5	アカウンティングボート:	1813	
ービスタイプフレーミン: ーザー: MAC/キャプティブ?	ゲ	RADIUS サーバーのステータ スの照会 (RFC 5997): 認証		
		アカウンティング		

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

顧客: Aruba Mina		Ⅱ. 注 ⑧
ដ HOME-AOS10 ្	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		
88 概要	新しいネットワークの作成	
🧧 デバイス	1 一般 2 VLAN 1 セキュリティ 2 アクセス 3 概要	
ロ クライアント	7/1+7.11.	
ぷ ゲスト		
アプリケーション	ロールヘース ネット・ソークペース 初後なし	
😯 セキュリティ	▲朝殿なし]オブションを選択すると、ネットワークへの完全なアクセスが許可されます。これによ	
- 分析	り、潜在的なセキュリティの問題が生じる可能性があります。	
↓ アラートおよびイベン…		
☑ 監査トレイル		
� ツール		
直 レポート		
保守		
ファームウェア		
と 組織		
	キャンセ	ル 戻る 次へ

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)

- 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
 第タンをクリック
 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

energie de la construcción de la													
顧客: Aruba Cafe	で アクセス	<mark>う</mark> 、ポイント										山根要	
ជ Cafe-AP 이	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	VPN	サービス	システム	loT	設定監査			詳細を隠す
- 管理													
品 概要	無	線SSID											
回 デバイス		名前 (プロファイル)		セキュリティ	アクセ	スタイフ	P	ゾーン			ネットワーク有効		
カライアント		aruba-cafe-admin		wpa3-sae-aes	制限な	сU					はい		
ぷ ゲスト		aruba-cafe-guest		wpa3-sae-aes	制限な	кU					はい		
■ 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													2.5510
ペ ツール	H	- SSID の追加											2 3310
山 レポート													
保守													
☺ ファームウェア													
论 組織													

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

顧客: Aruba Cafe	アクセス	う スポイント												山	:≡ IJZŀ	20 10
🛱 Cafe-AP 🕓	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	VPN	サービス	システム	IoT	設定監査	i I				8	羊細を隠
- 管理																
品 概要	新し	いネットワーク	の作成													
回 デバイス		1 一般	2 VLA	N 3 t‡	ュリティ	4	アクセス	5	概要							
ロ クライアント						Dyn	amicVI AN									
ぷ ゲスト		13 HJ (3510).				Dyn										
■ アプリケーション		> 詳細設定														
♥ セキュリティ																
- 分析																
♪ アラートおよびイベント														(+ +) + H		100
☑ 監査トレイル														++> 00		
ペ ツール																
山 レポート																
- 保守																
☺ ファームウェア																
b 組織																



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

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

割り当てルール欄の"+ルールの追加"をクリ

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

顧客: Aruba Cafe		li 概要	注: リスト 設定
ជ Cafe-AP 이	VLAN 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 VPN サービス システム IoT 設定監査		詳細を隠す
- 管理			
品 概要	新しいネットワークの作成		
回 デバイス	 一般 VLAN マキュリティ アクセス 振要 		
ロ クライアント	クライアント IP の割り当て: Instant AP 割り当て 例部 DHCP サーバー割り当て		
ぷ ゲスト			
👪 アプリケーション	クライアント VLAN の割り当て:		
♥ セキュリティ	VLAN の割り当てルール		
- 分析	デフォルト VLAN: 1		
♪ アラートおよびイベント			
🛛 監査トレイル			
冬 ツール			
直 レポート			
— 保守 ————			
⑦ ファームウェア			
と 組織	1		
	> 名前付き VLAN を表示		
	キャンセル	戻る	次へ

新しい VLAN の割り	り当-	てルール				
属性:		オペレータ:		文字列:	VLAN:	
Tunnel-Private-Grou	▼	次に一致	▼	VLAN-ID	VLAN20(20) ×	•
キャンセル						





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

顧客: Aruba Cafe			11. 三 (3) 概要 リスト (2)を
ជ Cafe-AP 이		ス セキュリティ VPN サービス システム IoT 設定監査	詳細を隠す
- 管理			A Line of the A
品 概要	新しいネットワークの作成		
回 デバイス	1 —般 2 VLAN 3 セ	キュリティ ④ アクセス ⑤ 概要	
🗔 クライアント			
ぷ ゲスト	セキュリティレベル:	0	
■ アプリケーション	エンター	ープライズ パーソナル ビジター オープン	
😯 セキュリティ			
- 分析	キー管理:	WPA3 エンタープライズ (CCM 128) ▼	
♪ アラートおよびイベント	プライフリサーバー・	InternalServer	
☑ 監査トレイル	2 2 1 2 2 9 5 - X		
ミ ツール	ユーザー:	0 ユーザー ユーザーの管理	
値 レポート		 	
- 保守		05 7 0	
☺ ファームウェア	> 詳細設定		
皆 組織			
		±	キャンセル 戻る 次へ

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

サーバータイプ:	RADIUS V	名前:	CPPM
RadSec:		IP アドレス/FQDN:	10.215.212.61
共有キー:		NAS IP アドレス:	オプション
キーの再入力:		NAS ID:	オプション
可試行回数:	3	認証ポート:	1812
タイムアウト (秒):	5	アカウンティングポート:	1813
亭止時間 (分):	5		
RP IP:		DRP マスク:	



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)Web 認証 規約ページのみ

- 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
 第タンをクリック
 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

顧客: Aruba Cafe	アクセス	う ポイント										ll. 概要	:三 リスト ◎ 設定
ជ Cafe-AP 이	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	т VPN	サービス	システム	loT	設定監査			詳細を隠す
- 管理				1									
品 概要	無	線SSID											
回 デバイス		名前 (プロファイル)		セキュリティ	アク	セスタイフ	1	ゾーン			ネットワーク有効		
カライアント		aruba-cafe-admin		wpa3-sae-aes	制图	ねし					はい		
ぷ ゲスト		aruba-cafe-guest		wpa3-sae-aes	制图	ねし					はい		
■ 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													2.5510
≪ ツール	H	- SSID の追加											2 3310
直 レポート													
- 保守													
ファームウェア													
跲 組織													

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

顧客: Aruba Cafe	アクセス	う 、ポイント								
다 Cafe-AP 〇	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	VPN	サービス	システム	IoT	設定監査
- 管理		•								
品 概要	新し	いネットワークの	D作成							
回 デバイス		1 一般	2 VLAI	N 3 t‡	・ュリティ	4	アクセス	5	概要	
ロ クライアント		名前 (SSID)·				Web	auth			
ぷ ゲスト		-169 (5510).				1150	JULII			
■ アプリケーション	:	> 詳細設定								
😯 セキュリティ										
一 分析										
♪ アラートおよびイベント										
☑ 監査トレイル										
ペ ツール										
応 レポート										
- 保守										
⑦ ファームウェア										
论 組織										



 ⑤ 本設定では、Instant AP の DHCP サーバを利用する クライアント IP の割り当てにて、"InstantAP 割り当て"を指定

顧客: Aruba Cafe		山 :三 概要 リスト	設定
ជ Cafe-AP 〇	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 VPN サービス システム IoT 設定監査	詳	細を隠す
管理		н	ind C has a
品 概要	新しいネットワークの作成		
回 デバイス	 一般 2 VLAN 3 セキュリティ 4 アクセス 5 概要 		
ロ クライアント	クライアント IP の割り当て		
ぷ ゲスト			
■ アプリケーション	クライアント VLAN の割り当て: ● 内部 VLAN)カスタム		
😯 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	キャンセル	戻る ジ	r^
冬 ツール			
応 レポート			
- 保守			
☺ ファームウェア			
ध 組織			

⑥ 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"内蔵キャプティブポータル" "承認済み"を選択

顧客: Aruba Cafe	 アクセスポイント		山	注 リスト 設定
🛱 Cafe-AP 🔅	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 VPN サービス システム IoT 設定監査		詳細を隠す
- 管理				
品 概要	新しいネットワークの作成			
回 デバイス	1 一般 2 VLAN 3 セキュリティ	④ アクセス ⑤ 概要		
ロ クライアント				
ぷ ゲスト	セキュリティレベル:			
■ アプリケーション	エンタープライズ	バーソナル ビジター オープン		
♥ セキュリティ				
- 分析	ネットワークにアクセス			
♪ アラートおよびイベント	タイプ:	内部キャプティブポータル ▼		
☑ 監査トレイル	キャプティブポータルの場所	→認済み ▼ キャプティブポータルのカスタマイズ		
ペ ツール		(3.00%)		
応 レポート	暗号化:			
- 保守	土 一管理·	エンハンストオーブン ▼		
	-1 In Az.			
比 利日/400	> 詳細設定			
		キャンセル	戻る	次へ



Page 6	33
--------	----

⑦ 必要によって、"キャプティブ	「ポータルのカスタマイズ"をクリックして、認証後にリダイレクトをする URL を入力する	
キャプティブポータル		×
スプラッシュページのプロパティ		
ポリシーテキスト:	Please read and accept terms and conditions and デフォルトテキストの読み込み then login.	
上部バナーのタイトル:	Welcome to Guest Network デフォルトテキストの読み込み	
ヘッダーの塗りつぶし色:	#e9e9e9	
初期画面のテキスト:	This network is not secure and use it at your own risk.	
ページの塗りつぶし色:	#fffff	
リダイレクト URL:		
ロゴイメージ:		
	プレビュー cancel 保	存

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

顧客: Aruba Cafe		Ⅱ. 注三 (2) 概要 リスト (2)定
디 Cafe-AP 이	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 VPN サービス システム IoT 設定監査	詳細を隠す
- 管理		
品 概要	新しいネットワークの作成	
回 デバイス	1 一般 2 VLAN 3 セキュリティ 4 アクセス 3 概要	
ロ クライアント		
ぷ ゲスト		
■ アプリケーション		
😯 セキュリティ	▲制限なし] オプションを選択すると、ネットワークへの完全なアクセスが許可されます。 これにトレー港なかからキャーリーティの問題が作りて可能性がよります。	
一 分析	これにより、潜江的なビギュリナイの问題が主じる可能注が効ります。	
☆ アラートおよびイベント		
☑ 監査トレイル		
ペ ツール		
直 レポート		
い 知嫌		
C 初日和秋		
	キャンセル	〕 戻る 次へ

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=Webauth が作成され、全ての Instant AP から出力される

この SSID に接続をすると、Instant AP の DHCP サーバから IP アドレスが割り当てられ、Instant AP で NAT が行われて通信を行うようになる



6.9 ユーザ/パスワードでのログイン

- 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
 第タンをクリック
 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

顧客: Aruba Cafe	マクセス	う ポイント										山根要	
ជ Cafe-AP 이	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	T VPN	サービス	システム	IoT	設定監査			詳細を隠す
管理													
出 概要	無	線SSID											
回 デバイス		名前 (プロファイル)		セキュリティ	アク	7セスタイン	P	ゾーン			ネットワーク有効		
クライアント	i	aruba-cafe-admin		wpa3-sae-aes	制图	艮なし					はい		
ぷ ゲスト	-	aruba-cafe-guest		wpa3-sae-aes	制图	艮なし					はい		
■ 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	5												3 5510
冬 ツール	H	- SSID の追加											2 220
直 レポート													
- 保守													
☺ ファームウェア													
℃ 組織													

④ 任意の SSID を設定します。本設定では"Webauth2"という SSID とし、"次へ"をクリック

顧客: Aruba Cafe		山 注 袋 機要 リスト
ជ Cafe-AP 〇	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 VPN サービス システム IoT 設定監査	詳細を隠す
管理		
品 概要	新しいネットワークの作成	
<i>▣ デ</i> バイス	 ① 一般 ② VLAN ③ セキュリティ ④ アクセス ⑤ 概要 	
ロ クライアント	2 th (cs(n)-	
ぷ ゲスト		
■ アプリケーション	> 詳細設定	
♥ セキュリティ		
分析		
♪ アラートおよびイベント		キャンセル 次へ
☑ 監査トレイル		
冬 ツール		
直 レポート		
- 保守		
☺ ファームウェア		
と 組織		





⑤ 本設定では、Instant AP の DHCP サーバを利用します。クライアント IP の割り当てにて、"InstantAP 割り当て"を指定

顧客: Aruba Cafe	う アクセスポイント	山 注 谷 概要 リスト 設定
ជី Cafe-AP 🛛	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 VPN サービス システム IoT 設定監査	詳細を隠す
- 管理		
品 概要	新しいネットワークの作成	
回 デバイス	 1 一般 2 VLAN 3 セキュリティ 4 アクセス 5 概要 	
カライアント	クライアント IP の割り当て 今部 DHCP サーバー割り当て	
ぷ ゲスト		
■ アプリケーション	クライアント VLAN の割り当て: の部 VLAN カスタム	
😯 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	キャンセル	戻る次へ
冬 ツール		
山 レポート		
- 保守		
◎ ファームウェア		
造 組織		

⑥ 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"内蔵キャプティブポータル" "認証済み"を選択

顧客: Aruba Cafe	う アクセスポインル		山 注 😳
ជ Cafe-AP 〇	アクセスポイント ラジオ インタ-	フェイス セキュリティ VPN サービス システム IoT 設定監査	詳細を隠す
- 管理			R L HAR GE DAN 2
品 概要	新しいネットワークの作成		
◎ デバイス	1 一般 2 VLAN	3 セキュリティ ④ アクセス ⑤ 概要	
□ クライアント			
ぷ ゲスト	セキュリティレベル:		
■ アプリケーション		エンターブライズ パーソナル ビジター オーブン	
😯 セキュリティ			
一分析 ————————————————————————————————————	ネットワークにアクセス		
□ アラートおよびイベント	タイプ:	内部キャプティブポータル ▼	
	キャプティブポータルの場所:	認証済み 💙 キャプティブボータルのカスタマイズ	
- 保守	プライマリサーバー:	InternalServer V +	
⑦ ファームウェア	users:	0 users ユーザーの管理	
皆 組織		 登録済みユーザー(タイプ'ゲスト)のみがこのネットワークにアクセスでき 	
		£9.	
	暗号化:		
	キー管理:	エンハンストオープン	
	> 詳細設定		
			キャンセル 戻る 次へ



⑦ ユーザーの管理をクリックして"+ユーザーの追加"からユーザを追加 タイプは"ゲスト"とする





⑧ 必要によって、"キャプティブポータルのカスタマイズ"をクリックして、認証後にリダイレクトをする URL を入力する

キャプティブポータル		×
スプラッシュページのプロパティ		
ポリシーテキスト:	Please read and accept terms and conditions and then login.	デフォルトテキストの読み込み %
上部バナーのタイトル:	Welcome to Guest Network	デフォルトテキストの読み込み
ヘッダーの塗りつぶし色:	#e9e9e9	
初期画面のテキスト:	This network is not secure and use it at your own risk.	デフォルトテキストの読み込み %
ページの塗りつぶし色:	#ffffff	
リダイレクト URL:		
ロゴイメージ:		プレビュー cancel 保存



⑨ 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

顧客: Aruba Cafe	ら アクセスポイント	山横要	
ជ Cafe-AP 이	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 VPN サービス システム IoT 設定監査		詳細を隠す
- 管理			
品 概要	新しいネットワークの作成		
<i>◎ デ</i> バイス	1 一般 2 VLAN 3 セキュリティ 4 アクセス 5 概要		
ロ クライアント			
ぷ ゲスト			
■ アプリケーション	ロールバーム ネットソーソハーム 前版なし		
😯 セキュリティ	<u>(</u> 制限なし]オプションを選択すると、ネットワークへの完全なアクセスが許可されます。		
- 分析	これにより、潜在的なセキュリティの同題が生じる可能性があります。		
♪ アラートおよびイベント			
☑ 監査トレイル			
� ツール			
値 レポート			
- 保守			
🕲 ファームウェア			
と 組織			
	キャンセル	戻る	次へ

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=Webauth2 が作成され、全ての Instant AP から出力され る

この SSID に接続をすると、Instant AP の DHCP サーバから IP アドレスが割り当てられ、Instant AP で NAT が行われて通信を行うように なる

6.10 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: HPE Aruba Networking 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

顧客: Aruba Cafe	同 ゲストアクセス			④ Ⅰ. 注 袋 3時間 標要 リスト 設定
ជ Cafe-AP 〇	スプラッシュページ ビジター			
- 管理				
맘 概要	ゲストアクセス > スプラッ	シュページ		+
回 デバイス				
カライアント	スプラッシュページ (1)			
🕺 ゲスト	名前	タイプ	状態	=
■ アプリケーション	default	匿名	共有	
😯 セキュリティ	5 10 25 50 1ページあた	٥		< < >> > → →:1/1
- 分析				
♪ アラートおよびイベント				
☑ 監査トレイル				
ミ ツール				
山 レポート				
- 保守				

- ◎ ファームウェア
- **ध** 組織





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

顧客: Aruba Cafe			Ð	ili 🗮	(j)
🛱 Cafe-AP	ゲストアクセス フブラッシュ ページ ビジター		3 時間		設定
- 管理					
品 概要	新しいスプラッシュページ				
回 デバイス	1 設定 2 カスタマイズ 3 ローカリゼーション				
「ロ クライアント					
<u> ポ</u> ゲスト	名前:	mail-auth			
■ アプリケーション	タイプ:				
セキュリティ		匿名 認証済み Facebook Wi-Fi			
♪ ♪ ♪ ♪ ♪ ♪ ♪ ♪ ♪ ♪	ユーザー名/パスワード:				
☑ 監査トレイル					
冬 ツール	自己登録:				
直 レポート	検証が必要:				
保守	電子メールペース:				
⑦ ファームウェア					
比 組織	電話ペース:				
	有効期限:	日時間分			
		● 無制限			
	M. Suell The Asso				
	ッーシャルロウイン.				
	失敗した場合にインターネットを許可				
	コモンネームを上書き				
	認証に成功した場合の動作:	 元の URL に戻る 			
		○ リダイレクト URL			
	認証失敗の入りモージ				
	セッションのタイトアウト・				
	MAC キャッシュの有効化				
	このプロファイルを共有:				
	同時ログイン制限	無制限 ▼			
	日次使用制限:	●無制限			
		時間基準 時間 分			
		· データ基準 MB ユーザーごと ▼			
	許可リスト URL:		+ URLをさらい	こ追加	
	スポンサーされたゲスト:				
			ſ		_
			l	キャンセル	RA



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

顧客: Aruba Cafe	 ゲストアクセス			◆ 3 時間	山 概要	10 11 11	8 15
ជី Cafe-AP 🔅	スプラッシュページ ビジター						
- 管理							
品 概要	新しいスプラッシュページ						
回 デバイス	① 設定 2 カスタマイズ	③ ローカリゼーション					
ロ クライアント							
<u> ポ</u> ゲスト	レイアウト:	横型、コンピュータ向け ▼					
■ アプリケーション	背景色:	#ffffff					
😯 セキュリティ	all have see the	HODOCHC					
- 分析	ホタンの色:	#009606					
<u> <u> </u> <u> </u> アラートおよびイベント </u>	ヘッダーの塗りつぶし色:						
▶ 監査トレイル	ページのフォントの色:	#bbbbbb					
	口ゴ:	参照					
	北口ノノード	40.1122					
⑦ ファームウェア	月京1メーン:	\$2 M					
皆 組織	(+) 使用条件の設定						
	(+) 広告の設定						
				キャンセ	n b	ミる 次/	



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

顧客: Aruba Cafe				iii (8)
Cafe-AP	アストアクセス スプラッシュページ ビジター		3.时間 機要	RE RE
- 管理				
品 概要	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		
CD クライアント	がっし ポーカリ ホニシリ レニナフ しをつ ニカニノブ (明明) ナフトル	ホナブシュンフィーリン		
III アプリケーション	ログインセクション			
🔮 セキュリティ	ログインボタンのタイトル:	サインイン		
分析	ネットワークログインのタイトル:			
✿ アラートおよびイベント	ログインページのタイトル:			
国 監査トレイル ペ ツール	アクセス拒否ページのタイトル			
直 レポート				
- 保守	ロジョン彼のジョトル:			
◎ ファームウェア	ユーザー名ラベル:			
论 組織	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:			
	知期両面のテキスト・			
			<i>a</i>	
	ログイン失敗メッセージ:		4	
	ログイン後のメッセージ:			
			6	
	登録セクション		●ビラノールジェキテナスカスカルズのキーパ	
	電話のヘルフメッセーシ:		電話フィールトに表示するガスダムスツゼージ	
	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	
	確認マードのラベル·			
	催認コードのフレースホルダ:			
	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 11.の201000			
	ネットワークログインメッセージ:			
			キャンセル 戻る ブレビュー	終了
サインイン

ユーザー名	
パスワード	
•	ナインイン
	登録 >

Ø JA

- 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
 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

顧客: Aruba Cafe	ła	ล											ih	:≡ ©
Cafe-AP	アクセス	ポイント											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 \	/PN	サービス	システム	IoT	設定監査			詳細を隠す
- 管理														
品 概要	無	線SSID												
🙆 デバイス		名前 (プロファイル)		セキュリティ		アクセスタ	マイプ		ゾーン			ネットワーク有効		
クライアント		aruba-cafe-admin		wpa3-sae-aes		制限なし						はい		
ぷ ゲスト		aruba-cafe-guest		wpa3-sae-aes		制限なし						はい		
■ 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														3.5510
≪ ツール	H	- SSID の追加												2 2210
山 レポート														
保守														
ファームウェア														
跲 組織														

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

顧客: Aruba Cafe		山 標要	:三 (3) リスト 設定
ជ Cafe-AP 〇	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 VPN サービス システム IoT 設定監査		詳細を隠す
管理			
器 概要	新しいネットワークの作成		
◎ デバイス	 一般 2) VLAN 3) セキュリティ 4) アクセス 5) 概要 		
ロ クライアント			
ぷ ゲスト	と思う(25m); Intelleand		
■ アプリケーション	> 詳細設定		
😯 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		++>+	
ミ ツール			
山 レポート			
- 保守			
☺ ファームウェア			
と 組織			



⑨ 本設定では、Instant AP の DHCP サーバを利用します。クライアント IP の割り当てにて、"InstantAP 割り当て"を指定

顧客: Aruba Cafe	う アクセスポイント	IL 注 @ 概要 IJスト 設定
ជី Cafe-AP 🛛	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 VPN サービス システム IoT 設定監査	詳細を隠す
- 管理		
品 概要	新しいネットワークの作成	
回 デバイス	 一般 2 VLAN 3 セキュリティ 4 アクセス 5 概要 	
カライアント	クライアント Ip.の割り当て. 0.5km DHCP サーバー割り当て.	
ぷ ゲスト		
■ アプリケーション	クライアント VLAN の割り当て: ● 内部 VLAN)カスタム	
😯 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	キャンセル	戻る次へ
ペ ツール		
山 レポート		
- 保守		
☺ ファームウェア		
₿ 組織		

 10 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

顧客: Aruba Cafe	し アクセスポイント	山、概要	
ជ Cafe-AP 〇	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 VPN サービス システム IoT 設定監査		詳細を隠す
- 管理			
品 概要	新しいネットワークの作成		
回 デバイス	 一般 VLAN 3 セキュリティ ④ アクセス ⑤ 概要 		
ロ クライアント			
ぷ ゲスト	セキュリティレベル:		
■ アプリケーション	エンタープライズ パーソナル ビジター オープン		
😯 セキュリティ			
- 分析	ネットワークにアクセス		
♪ アラートおよびイベント	タイプ: クラウドゲスト 🔻		
☑ 監査トレイル			
ペ ツール	ゲストキャプティブポータルのプロファイル: mail-auth 🔻		
山 レポート	暗号化:		
- 保守			
⑦ ファームウェア	キー管理: オープン ▼		
と 組織			
	> 詳細設定		
	キャンセル	戻る	次へ

① 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

顧客: Aruba Cafe		■1. 注三 (2) 概要 リスト (2)定
ជ Cafe-AP 이	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 VPN サービス システム IoT 設定監査	詳細を隠す
- 管理		
品 概要	新しいネットワークの作成	
🧧 デバイス	 一般 VLAN セキュリティ アクセス 3 概要 	
カライアント		
ぷ ゲスト		
■ アプリケーション	ロールベーム ネットワークベーム 制限なし	
😯 セキュリティ	△制限なし] オブションを選択すると、ネットワークへの完全なアクセスが許可されます。	
- 分析	これにより、潜在的なセキュリティの同題が生じる可能性があります。	
♪ アラートおよびイベント		
☑ 監査トレイル		
ミ ツール		
心 レポート		
- 保守		
◎ ファームウェア		
论 組織		
	++:	パセル 戻る 次へ

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 Instant AP から出力される

この SSID に接続をすると、Instant AP の DHCP サーバから IP アドレスが割り当てられ、Instant AP で NAT が行われて通信を行うように なる

6.11 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"よりその他をクリック ステイルスモードを有効にする

顧客: Aruba Cafe			ル :三 (②) 概要 リスト (②)
ជ Cafe-AP 〇	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	イ VPN サービス システム IoT 設定能音	詳細を隠す
- 管理			
器 概要	新しいネットワークの作成		
デバイス	1 一般 2 VLAN 3 セキュリティ	④ アクセス 5 概要	
ロ クライアント	名前 (SCID)-	tast	
ぷ ゲスト	(טובט).		
■ アプリケーション	◇ 詳細設定		
♥ セキュリティ			
- 分析	(+) 送信レート (レガシーのみ)		
♪ アラートおよびイベント	⊕ ビーコンレート		
☑ 監査トレイル	(ナ) ゾーン		
冬 ツール	+ 帯域幅制御		
直 レポート	↔ Wi-Fi マルチメディア		
- 保守 (ゆ) ファームウェア	○ その他		
造 組織	ESSID:	test	
	周波数带:	2.4 GHz 5 GHz 6 GHz	
	6GHz メッシュで無効化:		
	コンテンツフィルタリング:		
	主な用途:	 混合トラフィック 音声のみ 	
	無通信のタイムアウト:	1000 秒	
	ステルスモード:		



6.12 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、"ユーザ間のブリッジを禁止" 項目を有効にする

顧客: Aruba Cafe	し アクセスポイント		山	:三 (② リスト 設定
업 Cafe-AP 이	WLAN アクセスポイント ラジオ インターフェイス セキュリラ	ティ VPN サービス システム IoT 設定監査		詳細を隠す
- 管理				
品 概要	新しいネットワークの作成			
回 デバイス	 一般 2 VLAN 3 セキュリティ 	④ アクセス ⑤ 概要		
	名前 (SSID):	test		
ぷ ゲスト				
アプリケーション	→ 詳細設定			
セキュリティ	 ・ ブロードキャスト/マルチキャスト 			
⑦ アラートおよびイベント				
☑ 監査トレイル	(+) ビーコンレート			
ペ ツール				
直 レポート				
- 保守				
🕲 ファームウェア				
跲 組織	ESSID:	test		
	周波数带:	✓ 2.4 GHz ✓ 5 GHz 6 GHz		
	6GHz メッシュで無効化:			
	コンテンツフィルタリング:			
	主な用途:	 混合トラフィック 音声のみ 		
	無通信のタイムアウト:	1000 秒		
	ステルスモード:			
	ネットワークの無効化:			
	最大クライアント数のしきい値:	64		
	ローカルプローブ要求のしきい値	自動 ● 手動 0		
	認証要求の最小 SNR:	Automatic Manual 0		
	無通信状態の端末へ deauth を送信:			
	アップリンクなしで使用可能:			
	ユーザー間のブリッジを禁止:			

6.13 ゾーン設定について

複数台管理されている Instant AP において、場所ごとに出力したい SSID を分けて運用したい場合はゾーン設定を行います。



(運用例)

① 作成されている SSID を選択し、鉛筆マークをクリックして編集する

顧客: Aruba Cafe	う マクセンポイント				山、標裏	
디 Cafe-AP 〇	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	VPN サービス システム	IoT 設定監査		詳細を隠す
- 管理						
品 概要	無線SSID					
<i>◎ デ</i> バイス	名前 (プロファイル)	セキュリティ	アクセスタイプ	ゾーン	ネットワーク有効	
ロ クライアント	aruba-cafe-admin	wpa3-sae-aes	制限なし		はい	
ぷ ゲスト	aruba-cafe-guest	wpa3-sae-aes	制限なし		はい	
■ アプリケーション	DynamicVLAN	wpa3-aes-ccm-128	制限なし		はい	
😯 セキュリティ	Webauth	キャプティブポータル(int	制限なし		はい	
- 分析	Webauth2	キャプティブポータル(int	制限なし		はい	
♪ アラートおよびイベント	mail-auth	キャプティブポータル(ext	制限なし		(d U)	
☑ 監査トレイル	test	wpa3-sae-aes	制限なし		tu 🦻 🖊 🗖	
ペ ツール	+ SSID の追加					7 SSID
応 レポート	ネットワーク概要					
- 保守	一般			セキュリティ		
◎ ファームウェア	ESSID	DynamicVLAN		セキュリティレベル	エンタープライズ	
と 組織	マルチキャスト最適化	無効		認証サーバー 1	СРРМ	



② "詳細設定"を表示し、ゾーン項目にユニークな文字列を入力したら"設定の保存"をクリック

顧客: Aruba Cafe	し アクセスポイント	l. ∷⊟ 🕸 腰 リスト 歳
디 Cafe-AP 〇	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 VPN サービス システム IoT 設定監査	詳細を隠す
- 管理		
品 概要	一般 VLAN セキュリティ アクセス 概要	
◎ デバイス	ECCID- test	
ロ クライアント		
ぷ ゲスト	✓ 詳細設定	
■ アプリケーション	 ・ ブロードキャスト/マルチキャスト 	
😯 セキュリティ	(→ 送信レート (レガシーのみ)	
一 分析	⊕ ビーコンレート	
♪ アラートおよびイベント		
☑ 監査トレイル	V>/- MeetineRoom	
ペ ツール	inequipition.	
応 レポート	 → 帯域幅制御 	
- 保守	(→) Wi-Fi マルチメディア	
☺ ファームウェア	- (中) その他	
论 組織	() 時期範囲のプロファイル	
@ Comministe 2027 Linuslate Devised D		設定の保存

③ "アクセスポイント"タブよりアクセスポイントを選択し、鉛筆マークをクリックして編集する

顧客: Aruba Cafe	704	う フポイント										山板要	:≡ IJZ.Þ	
ជ Cafe-AP 〇	WLAN	アクセスポイント	ラジオ	1-1-1-1-	セキュリティ	VPN #-P	システム	IoT 設定監査						洋細た隠す
- 管理	WEAR	77 22/11/1	724	122 211	241774	VIN 5 C2		IOT DOCT						计加口 2 185 9
品 概要	7	⁷ クセスポイント	(3)											\odot
◎ デバイス	Y	名前 🖓	VC 名	ステータス	∀ IP <i>7</i>	IP 割り当	τ =-I	· 9-	イプ 2.4	IGHz (チャ	5GHz (チャネ	6 GHz (チャネ		
		VC		O Offline		STATIC	access	AP-5	605 Auto	0	Auto	-		
D クライアント		vc		O Offline		STATIC	access	AP-5	605 Auto	0	Auto	-		1
ぷ ゲスト		VC		O Offline		STATIC	access	AP-5	i05 Auto	0	Auto	-		
■ 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														
ペ ツール														
値 レポート														
- 保守														
ファームウェア														

ф // Ц/

8 組織

- ④ AP ゾーンの項目に WLAN 設定で入力したものと同じ文字列を入力
 - "設定の保存"をクリックすると、ゾーン設定を行った SSID は、同じゾーン設定を行っている Instant AP のみで出力されるようになる ゾーン設定を行っていない SSID は全ての Instant AP から出力される

顧客: Aruba Cafe	う アクセスポイント		II. ∷三 概要 リスト 設定
ជ Cafe-AP 이	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 VPN サービス システム IoT 設定監査	詳細を隠す
- 管理			
品 概要	アクセスポイント / 505		
◎ デバイス			
ロ クライアント	基本情報 ラジオ 設置タイプ アッ	プリンク メッシュ	
ニ ゲスト			
■ アプリケーション	名前:	505	
♥ セキュリティ	AP ゾーン:	MeetingRoom	
- 分析 介 アラートおよびイベント	RF ゾーン:		
☑ 監査トレイル	クラスタモード:	クラスタ ▼	
ミ ツール	LACP モード	パッシブ 🔻	
 Lポート 保守 	優先コンダクタ:		
@ ファームウェア	アクセスポイントの IP アドレス:	── IP アドレスを DHCP サーバーから取得	
と 組織		Cancel	Save Settings



6.14 時間ベースの SSID 制御

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 ⁽²⁾ ボタンをクリック

顧客: Aruba Cafe	アクセン	<mark>う</mark> スポイント												山、概要	:三 リスト 設定
ជ Cafe-AP 🛛	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	VPN +	サービス	システム	loT	設定監査					詳細を隠す
- 管理															
出 概要	7	クセスポイ:	ント (3)												\odot
回 デバイス	Y	名前	▼ VC 名	ステータス	Ţ IP 77	IP	割り当て	÷	-ド	9	イプ	2.4GHz (チャ	5GHz (チャネ	6 GHz (チャネ	
ロ クライアント			VC	O Offline		STA	ATIC	acce	ess	AP-	505	Auto	Auto	-	
ぷ ゲスト			VC	Offline		STA	ATIC	acce	ess	AP-	505	Auto	Auto	-	
■ 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															
冬 ツール															
山 レポート															
- 保守															
☺ ファームウェア															
跆 組織															

③ "詳細の表示"をクリックして、システムタブを開きます

顧客: Aruba Cafe	う アクセスポイント									山、概要	:三 (② リスト 総定
ជ Cafe-AP 이	WLAN アクセスオ	ペイント ラジオ									詳細を表示
管理											AT MALE DOUGH
品 概要	アクセスポー	イント (3)									\odot
回 デバイス	▼ 名前	▼ VC 名	ステータス	Υ IP <i>ア</i>	IP 割り当て	モード	タイプ	2.4GHz (チャ	5GHz (チャネ	6 GHz (チャネ	
「 クライアント	505-3	VC	O Offline	10.215.201.93	STATIC	access	AP-505	Auto	Auto		
	505	VC	O Offline	10.215.201.91	STATIC	access	AP-505	Auto	Auto	-	
ヱ ゲスト	505-2	VC	O Offline	10.215.201.92	STATIC	access	AP-505	Auto	Auto	·	
■ 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											
冬 ツール											
応 レポート											
- 保守											
⑦ ファームウェア											
诰 組織											



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

顧客: Aruba Cafe		
ជ Cafe-AP 〇	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 VPN サービス システム IoT 安定告告	詳細を隠す
- 管理	ЭЛ Г А	a transfer Control
昭 概要	> 一般	
回 デバイス	〉管理者	
カライアント		
ニ ゲスト		
■ アプリケーション	◇ 時間ペースのサービス	
♥ セキュリティ	→ この機能は NTP が必要です。	
- 分析		
♪ アラートおよびイベント		
☑ 監査トレイル	名前 時刻 アソシエーション 三	
≪ ツール		
山 レポート		
- 保守		
⑦ ファームウェア		
跲 組織	表示するデータがありません	



Technical Note

新しいプロファイル		×
名前:	employee	
タイプ:	定期的 ▼	
繰り返し:	• 毎日 毎週	
日付範囲:	● 月曜日~日曜日 (全日) 月曜日~金曜日 (平日) 土曜日~日曜日 (週末)	
開始時刻:	時間 8 ▼ 分 0 ▼	
終了時刻:	時間 19 ▼ 分 0 ▼	
	キャンセル のK	

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

顧客: Aruba Cafe	7047	<mark>)</mark> オイント										11. 概要	יגע	
ជ Cafe-AP 〇	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	VPN	サービス	システム	IoT	設定監査				詳細を隠す
- 管理														
品 概要	無	線SSID												
◎ デバイス		名前 (プロファイル)		セキュリティ		アクセ	マスタイプ		V	`ーン	ネットワーク有効			
ロ クライアント		aruba-cafe-admin		wpa3-sae-aes		制限な	÷С				はい			
ぷ ゲスト		aruba-cafe-guest		wpa3-sae-aes		制限な	к し				はい			
■ アプリケーション		DynamicVLAN		wpa3-aes-ccm-	128	制限な	r l				はい			
😯 セキュリティ		Webauth		キャプティブボ	ータル(int	制限な	к し				はい			
- 分析		Webauth2		キャプティブポ	ータル(int	制限な	с .				はい			
♪ アラートおよびイベント		mail-auth		キャプティブボ	ータル(ext	制限な	:L				はい			
☑ 監査トレイル		test		wpa3-sae-aes		制限な	<i>د</i> ل				はい			
ペ ツール		+ SSID の追加												7 SSID
しポート														
- 保守														
☺ ファームウェア														
皆 組織														



 (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。

顧客: Aruba Cafe	<u>「</u> アクセスポイント	Ⅱ. 注目 (2) 標要 リスト (2)20
ជ Cafe-AP 🔅	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 VPN サービス システム IoT 設定監査	詳細を隠す
管理		
品 概要	ネットワーク > 設定 - test	
デバイス		
ロ クライアント	一般 VLAN セキュリティ アクセス 概要	
ぷ ゲスト	ESSID: test	
■ アプリケーション		
😯 セキュリティ	✓ 詳細設定	
- 分析		
☆ アラートおよびイベント	(→) 送信レート (レガシーのみ)	
☑ 監査トレイル		
ペ ツール	 (+) ゾーン 	
ඛ レポート	 → 帯域幅制御 ● 	
- 保守	(+) Wi-Fiマルチメディア	
	(+) その他	
L。 組織	○ 時間範囲のプロファイル	
	 この機能は NTP が必要です。 	
	時間範囲のプロファイル ステータス	
	employee (Periodic Daily 08:00 - 19:00) 有効 🔻	
	十 新しい時間範囲プロファイル	
	★・ 可畑化はほぼ1時間でとに行われます。	
	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23	
	有効な接続時間 無効な接続時間	
	キャンセル	設定の保存

7 アラートとレポート

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 AP の接続が切断された際に、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

顧客: Aruba Mina	0 77-1	1021				1. 82	10 11 11	8
♀ グローバル ○								
- 管理	アラート重	重大度と通知			検索			۹
昭 概要							_	
回 デバイス	ユーザ	デー アクセスボイント スイッチ ゲート	フェイ 接	読 監査 サイト		Default Recipients	すべて!	有効
ロ クライアント	(j [+] 7	?イコンをクリックすると、デフォルトの通知ボリシ-	ーに沿って通知	目をすばやく生成できます。また、タイルをクリックして;	ポリシーを定義する	こともできます。 了解		
ぷ ゲスト								
■ アプリケーション	新しい	v仮想コントローラが検出されました	+	仮想コントローラの提続が解除されました	~	新しい AP が検出されました	+	·
🛛 セキュリティ			_					
& ネットワークサービス	AP 切	NF	+	不正 AP の検知	~	インフラストラクチャ攻撃が検出されました	+	
- 分析			_					
ク アラートおよびイベン…	クライ	(アント攻撃が検出されました	+	アップリンクが変更されました	+	モデムが接続されました	+	
🗷 監査トレイル								
ペ ツール								
園 レポート	tTA	◇の接続が解除されました	+	供給電力が不定しています	+	个明なラジオを持つ AP	+	
- 起動 ● フゴリトクログ								
- @g	AP CP	PU 使用率	+	AP メモリ使用率	+	ラジオチャネル使用率	+	
ファームウェア								
比 組織	ラジオ	トノイズフロア	+	VC毎の接続クライアント数	+	AP毎の接続クライアント数	+	



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、アクセスポイント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

顧客: Aruba Mina					<u>al.</u>	UZF	
♀ グローバル ○	アクセスポイント > AP 切断						_
- 管理							
88 概要			~ ~ ~ ~				
『 デバイス	重大度:	 クリティカル 	×9*-	717-	. ##		
ロ クライアント							
塁 ゲスト	接続時間:	0 分					
アプリケーション	デバイスフィルタオプション:						
👽 セキュリティ	グループ:	× HOME-AOS10	· ·				
& ネットワークサービス							
- 分析	ラベル:	ラベルを選択					
🗘 アラートおよびイベン							
🛛 監査トレイル	サイト:	サイトを選択	•				
🔦 ツール	デバイス:	デバイスを選択	•				
回 レポート							
- A230	通知オプション:	デフォルトの受信者(1) ろ	その他の受信者	@hna.com			
⑦ アプリカタログ	HB 2 21-72	• • • • • • • • • • • • • • • • • • •	1 10 10 10 X IN TH	enpecum			
- 保守	Webhook						
◎ ファームウェア							
は 組織					キャンセル	傳	

7.2 レポートの出力方法

HPE Aruba Networking Central では現在 5 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

顧客: Aruba Mina			u. ∷≣ ≪a yzt	0
<i>逾 グロ−バル</i> ○	F		_	
- 管理				
88 概要				
回 デバイス	参照	管理	作成	
ロ クライアント	レポートを閲覧します	スケジュールされたレポートを管理します	レポートを作成し、スケジュールを設定します	
ニ ゲスト	L.M		(💼)	
囲 アプリケーション	L_h	0		
♥ セキュリティ			_	
& ネットワークサービス	0 生成したレポート	○ スケジュール読みレポート	5 カテゴリ	
- 分析	〇 過去7日間に生成	〇 今後7日間に実行	24 LIR-FOIT	
↓ アラートおよびイベン				
🗹 監査トレイル				
� ツール			TPAK	
🙃 レポート				
- 起助				
アプリカタログ				
- 保守				
ファームウェア				
と 組織				

② どのタイプのレポートを作成するのかを選択し、次へ

顧客: Aruba Mina	n L#-b						1. ≣≣ 9.2.1×	8
☺ グローバル ○								
- 管理	クライアントインペントリ	·デンツ (一)に何を含めますか?	期間 いつまで用りますか?	() #91 L#	高し ートの保度は?			
88 概要	クライアント	インフラストラクチャ				セキュリティコンプラ	< 7 7 7 7	
デバイス								
ロ クライアント		£1	\mathbf{X}	0	0		1	
二 ゲスト	クライアント インペントリ セッション 使用量	キャバシティブランニン グ	設定と監査	インフラインベントリ	ネットワーク	PCIコンプライアンス	RAPIDS	
アプリケーション								
😯 セキュリティ	ði (:	\oplus	Ö	(ċ		0		
🞖 ネットワークサービス	ゲスト 概要	厳しいインフラインペン トリ	リソース使用量	NF 健全性	スイッチキャパシティブ ランニング	セキュリティコンプラ イアンス		
- 分初								
♪ アラートおよびイベン…		0	\bigcirc	0	0			-
🖾 監査トレイル	インサイト	WAN 可用性	WAN インベントリ	WAN コンプライアンス	WAN トランスポート正	アプリケーション		
& ツール	⊕				M12	c"		
🔝 レポート	胆外クライアント	0	\bigcirc			AppRF		
- 8280		WAN 使用量	WAN Web コンテンツの					
⑦ アプリカタログ			27.48					
- 保守								
⑦ ファームウェア								
と 組織								_
	キャンセル						次へ	I

③ レポートを作成する確認対象を確定させ、次へ

顧客: Aruba Mina	() (#- b				. @# IJZŀ
@ グローバル ○					
管理	⑦ 市成対象 クライアントインベントリ	(2) #22対象 コンテキスト: グループ	() L#-188	(⑦) スケジュール:今下ぐ Mar 23, 2023	
88 概要	コンテキスト	<i>d</i> = 7	連用フィルク	1	
回 <i>デバ</i> イス		<i><i>w</i>-<i>y</i></i>	X8/6 / 1 ///7		
0 クライアント	(●) グループ	Q. 11h-7317+169	() &L		
ゲスト	○ ラベル	Ali	0 =-7/		
] アプリケーション	0 941	default	🔿 ssib		
セキュリティ		Family Mart			
ネットワークサービス					
<i>й</i> — — — — — — — — — — — — — — — — — — —		HOME-AOS10			
アラートおよびイベン		HOME-AOS8			
監査トレイル		Home-Ryogoku			
ツール					
レポート					
80					
アプリカタログ					
£6i	キャンセル				₩ 6 X^
ファームウェア					
組織					

④ レポートに出力する期間を指定する

顧客: Aruba Mina					1. ***	1000 U.S.F	() 10.2
@ グローバル 〇	-	-					
 一世理 部 概要 ② デバイス □ クライアント エ ゲスト ■ アプリケーション ② セキュリティ ※ セキュリティ ※ ネットワークサービス - 分析 △ アラートおよびイベン 	外点は株 ウライフントインバントリ レポート期間 作日 透去7日時 通去30日期 単純用月 ① カスタム範囲	##27# 227#3.1:98-7	(6) 上市一部署 点生 30 注意	 			
	キャンセル				RA	次へ	1
- #280							1
⑦ アプリカタログ							
- 保守							
◎ ファームウェア							
1: 組織							



⑤ レポートを出力する日時を指定し、生成をクリック

繰り返し	レポート情報
● 1回(今すぐ)	レポートライトル Client Inventory
() 1回(後で)	
() 毎日	電子メール連進角 Bhpe.com
() 毎週	
()每月	電子メール形式 🗹 PDF 🗹 CSV

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

顧客: Aruba Japa				() ()
☞ グローバル ○				
- 管理				
88 概要				
回 デバイス	参照	管理	作成	
□ クライアント	レポートを閲覧します	スケジュールされたレポートを管理します	レポートを作成し、スケジュールを設定します	
ニ ゲスト	Ľ۳,		(👘)	
アプリケーション	ĽĽ	Co		
😯 セキュリティ			-	
🞖 ネットワークサービス	556 生成したレポート	2 スケジュール済みレポート	5 <i>カテゴ</i> リ	
- 分析	過去7日間に生成	1 今後 7 日間に実行	24 レポートタイプ	
↓ アラートおよびイベン…				
🛛 監査トレイル	* 5	*3	作成	
� ツール				
🔝 レポート				
- 起助				
アプリカタログ				
- 保守				
@ //-491/				
t; 組織				

8 FLOORPLANS

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

🗈 AiCT-ArubaOffice 🛆	間日 サイト健全性	(1) 概要	-1 wi-ri 接続	〇 WAN 健全性	AI 72771	ト税ジ		88	iii yab
- 1222	1								- 1
88 概要									- 1
アバイス									- 1
D クライアント									- 1
囲 アプリケーション									- 1
😯 セキュリティ									- 1
惑 ゲスト									- 1
- 分析									
♪ アラートおよびイベント									
↓ ライブイベント									
む ツール									
直 レポート									
- 99									
◎ ファームウェア					0				
				10.00	U 12707###	1 = ++ L			
				attan 1	ロアの追加	r a. 12 Ni			

② "新しいフロアプラン"をクリック

■D A棟	間日 サイト鍵全性	日根東	인 Wi-Fi接続	↓ WAN 健全性	0 AI 12711	_ ►#ПУ	FLOORPLANS		
88 概要	7077	ゲラン	インボート					Exit Edi	t Mode
 デバイス ロ クライアント 	AR							A棟 プロパティ 表示 編集	
囲 アプリケーション ② セキュリティ ニ ゲスト								アクション すべて選択 テレアす	
分析 アラートおよびイベント								新しいフロアプラン	



) サイトの図面をアップロードする。 新しいフロアプラン	jpg、jpeg、gif、bmp、pdf、png 形式をサオ	[°] −トしています。 , 区
フロアプランファイル	選択 ファイルが選択され	ていません。
サポートされるファイル形式: jpg、jp	beg、gif、bmp、pdf、およびpng。	
フロア名	フロア 1	
フロア番号	1.0	
	Save	Cancel

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)

ND ASK	間: 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日		
11日	AM > 7071	新しいフロアの定義	
B デバイス	0	② 地址 ③ CAD L-イヤー	
3 クライアント	Center (myTpc)	③ アクセスポイント	
) アプリケーション	今届いたラインの長さは 59.48 です。た 国立した影響の音波はどれだけですからの フィート)	フロアフランの寸法	
9 セキュリティ		《 测正	
ゲスト	OK Cancel	4% 201.500	ft.
	2 2 7 5 4 L 28 9 7 5 4 L	高さ 160.240	ft.
ライブイベント	2期エレベータホール	R ^	
ツール	0		
] レポート	2階男子トイレ 2階男子トイレ DEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE		
	(2) HPE教育サービス		

HPE Aruba Networking Central 基本操作ガイド IAP 編

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

サイト健全性	(II) 概要	つ Wi-Fi 接続	Q WAN 健全性	0 N-1>911	。 作素ロジ	FLOORPLANS		
20	アブラン	インボート					Exit Edit Mode	
A∰ >	フロア 3 2開女子 2開知子 HPE教育社	my IT Pro Center ()	ductivity nyITpc) 2751				新しいフロアの定義 ① 拡大振小 ② 地域 ③ CAD レイヤー ④ アクセスポイント AP 展開を計画しますか、またはすでに展開されている AP を追加しますか? AP の計画 展開済み AP タイプ Aruba AP 515 回数 0 展開時間 	



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。





HPE Aruba Networking Central 基本操作ガイド IAP 編

9 AIOPs

AIOPs について

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。

Al Insights

Al 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。

Al Insights の表示方法

Al 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。



10 メンテナンス

10.1 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

111					10 コンプライアンスの	BCE # 14(79790-
概要	アクセスボイント (12)					Q
デバイス	68 IL	サイト	ファームウェアバ	推開パージョン	▼ アップグレードのステー… マ	コンプライアンスステータス
h= / 71.1	• as-l	未割り当て	6.5.4.20_80109	6.5.4.15_73677	ファームウェアは最新です	未設定
クライアント	AUI	CAFE	8.6.0.9_79813	8.6.0.9_79813	ファームウェアは最新です	未設定
ゲスト	AU		8.8.0.1_80393	8.6.0.9_79813	ファームウェアは最新です	*82
アプリケーション	 HS- 	Aruba Tokyo	8.6.0.5_75979	8.6.0.9_79813	新しいファームウェアを利用でき	未設定 アップグレー
	• MPC	үк	6.5.4.18_77207	6.5.4.15_73677	ファームウェアは最新です	未設定
セキュリティ	• MP	CAFE	6.5.4.15_73677	6.5.4.15_73677	ファームウェアは最新です	末設定
ネットワークサービス	• OSF	Aruba Osaka	8.6.0.9_79813	8.6.0.9_79813	ファームウェアは最新です	末設定
ę	Set	末割り当て	8.6.0.14_81691	8.6.0.9_79813	ファームウェアは最新です	末設定
アラートおとだイベント	Set	CAFE	8.8.0.1_80393	8.6.0.2_73853	ファームウェアは最新です	未設定
///////////////////////////////////////	Set	AICT-ArubaOffice	8.7.1.0_77203	8.6.0.9_79813	ファームウェアは最新です	未設定
監査トレイル	• TH:	未割り当て	8.7.1.1_78245	8.6.0.2_73853	ファームウェアは最新です	未設定
ツール	Virt	識子	8.7.1.3_79817	8.6.0.9_79813	ファームウェアは最新です	未設定

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





10.2 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

ହ ମସ- <i>ମ୍ୟା</i> ି	
- 1012	ネットワークチェック デバイスタイプとテストを選択し、パラメータを設定して、テストを実行します
デバイス	サバスタイプ ソース アクセスポイント ACT-Aruba-315
ロ クライアント	Pスト 発気・ダブ ネスト&# 97ドレス Ping デスト ホスト名パP アドレス 8.8.8.8</th></tr><tr><th>国 アプリケーション</th><th>その他のテスト設定を表示</th></tr><tr><th>セキュリティ</th><th>版にコマジトを実行しているデバイスで、新しく通知されたコマジトを実行してはなりません パッファスペースの問題があるデバイスの出力展開は自動的に消去されます</th></tr><tr><th>8: ネットワークサービス - 分析</th><th>実行</th></tr><tr><th>☆ アラートおよびイベント</th><th>デバイス出力</th></tr><tr><th>🛛 監査トレイル</th><th>デバイス III デバイスの出力: AICT-Aruba-315 Q 🖸 🛓 🗘</th></tr><tr><th> マール レポート 保守 ファームウェア 組織 </th><th>O ACT-Aruba-315 2021-10-21 10:50:20 UTC Test Type: NMG Surve: [Access Point] ACT-Aruba-315 Target: [EXTERNAL] & 8.8.8 Output Time: 2021-10-21 10:50:25 UTC COMMAND-pring 8.8.84 PMG 8.8.8 (8.8.8.8): 56 data bytes 64 bytes from 8.8.8.81 kmp_seq=101-13 time=16:7 ms 64 bytes from 8.8.8.81 kmp_seq=20 ms 64 bytes from 8.8.8.81 kmp_seq=4 til-113 time=20:9 ms 64 bytes from 8.8.8.81 kmp_seq=4 til-113 time=3.9 ms 64 bytes from 8.8.8.81 kmp_seq=4 til-113 time=13:9 ms </th></tr></tbody></table>





10.3 リモートコンソール

Central では GUI から AP の CLI がひらけます

<i>≌ グロ−バル</i> ○	22 10 10 10 10 10 10 10 10 10 10 10 10 10
- 世世 - ビー - ジー - ジ	ますトワークチェック デバイスチェック コマント コンソール 変接性トレージング リモートコンソールセッション 家院セッション 保存済みセッション デバイスタイプ リモートコ リモートコ ジール ・ ・ ・ ・ ・ ・ ・ ・ ・
 ・ ネットワークサービス 	<pre>dbolimeit dbolimeit Rost 'localhost' key accepted unconditionally. (ssh-rsa fingerprint mdS d4:0d:ad:0d:51:13:b5:38: show tech-support and show tech-support supplemental are the two most useful outputs to collect for any kind of troubl eshooting session. 7F-Mesh-Point-Cafe#</pre>
 □ レポート - 余守 ● ファームウェア ▶ 組織 	



Technical Note

HPE Aruba Networking Central 基本操作ガイド IAP 編

11 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 HPE Aruba Networking Central 基本操作ガイド 入門編を参照

https://www.hpe.com/psnow/doc/a00143744jpn

デバイスインベントリからの削除方法

HPE Aruba Networking 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、HPE Aruba Networking Central 基本操作ガイド 入門編を参照

https://www.hpe.com/psnow/doc/a00143744jpn

12 不具合かと思ったら

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 Instant AP の "show tech-support " および、 "show tech-support supplemental " は必須となります。

以上

