



Ruckus Smart Start Guide

Unleashed ネットワーク構築ガイド ver. 200.8

2020 年 4 月発行

3. 目次

3. 目次	1
4. はじめに	4
1 Unleashed システム概要	5
1.1 基本構成	5
1.2 サポート AP 数と同時接続クライアント数	6
1.3 複数拠点における展開例	7
2 Unleashed セットアップ	8
2.1 Master AP セットアップ	9
2.1.1 設定 PC を Unleashed AP へ接続	9
2.1.2 セットアップウィザードの実行	10
2.1.3 作成した WLAN へ接続し、Unleashed へログイン	13
2.2 Member AP セットアップ	15
2.3 AP 状態の確認	16
3. Unleashed AP の基本動作	17
3.1 ブロードキャスト ハートビート による情報交換	17
3.2 Unleashed AP の起動	18
3.3 Master AP 基本動作シーケンス	18
3.4 Member AP 動作基本シーケンス	20
4 システムマネージメント	21
4.1 管理 VLAN と アクセス VLAN	21
4.2 Master AP と管理 IP アドレス	21
4.2.1 Management Interface の利用	21
4.2.2 Prefer Master	22
4.2.3 Role の固定化	23
4.2.4 管理インターフェイスへのアクセス制限	24
4.3 Unleashed イベント管理	25
4.3.1 Alarms	25
4.3.2 Events	26
4.3.3 Logs	27
4.3.4 Syslog	27
4.4 Unleashed Multi-Site Manager による管理	29
4.5 SNMP による管理	29
4.6 マルチ言語のサポート	31
5 WLAN サンプルコンフィグ	32

5.1	Open PSK.....	32
5.2	WPA2-PSK-AES と MAC アドレス認証.....	33
5.3	802.1X EAP	35
5.3.1	WLAN サバイバビリティ	37
5.4	AP 設定	38
5.5	WLAN のチューニング	41
5.5.1	Master AP のクライアント接続制限	41
5.5.2	Member AP のクライアント接続制限	41
5.5.3	OFDM Only	42
5.5.4	bss-minrate.....	43
5.5.5	パフォーマンス、スティッキー端末の改善設定の例.....	44
6	Unleashed M510 LTE バックホール セットアップ	45
6.1	M510 各部の説明.....	46
6.1.1	各種アンテナの接続	46
6.1.2	SIM の挿入.....	46
6.1.3	電源供給.....	47
6.2	Unleashed M510 セットアップ	48
6.2.1	設定 PC を Unleashed AP へ接続	48
6.2.2	セットアップウィザードの実行.....	49
6.3	その他の LTE 設定	54
6.3.1	LTE パラメータ入力	54
7	その他.....	59
7.1	ファームウェア アップグレード.....	59
7.2	デバッグ情報の取得.....	59
7.3	クライアント・トラブルシューティング ツール	60

変更履歴

変更年月	理由
2017 年 10 月	初版
2017 年 11 月	オンラインヘルプのご案内を追加
2019 年 5 月	200.7 アップデートに伴う改定
2019 年 8 月	無線接続からの初期セットアップへ変更 M510 の LTE バックホール接続の設定追加 その他
2020 年 4 月	200.8 アップデートに伴う改定

4. はじめに

この資料は Ruckus Unleashed AP の操作方法、設計基準をご理解いただくために作成されたもので、動作を保証するものではありません。
あらかじめご了承ください。

また、Unleashed Online Help が提供されておりますのでご活用ください。

<http://docs.ruckuswireless.com/unleashed/200.8/index.html>

1 Unleashed システム概要

1.1 基本構成

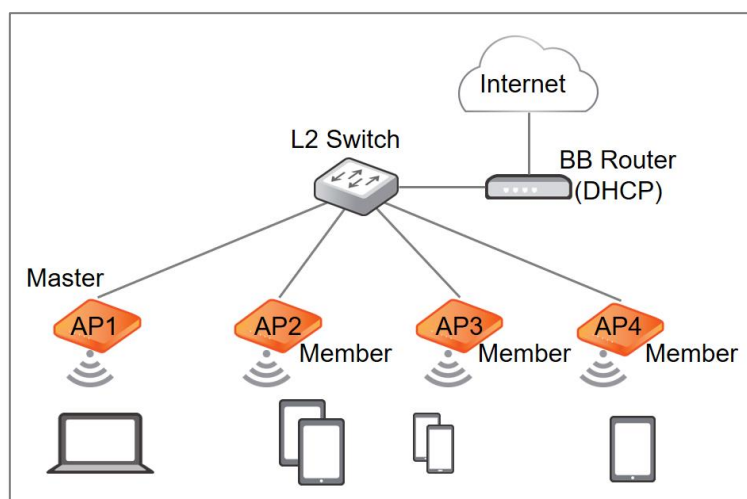
Ruckus Unleashed は小規模でシンプルな無線 LAN ネットワークを容易に提供することを前提に設計されており、システムの拡張性は以下の通りです。なお、最大数は、802.11ac wave 2 AP 又は Wi-Fi 6 AP を使用し、かつ Bridge モードによる動作環境の場合です。

- 最大 128 台の AP 数 (1 台の Master AP と最大 127 台の Member AP)
- 最大 2,048 台の 同時接続クライアント数
- 全ての AP の管理 VLAN は同じサブネットに属する

Unleashed のシステム管理は、1 台の Master AP が AP 機能と同時にコントローラ機能を実行し、同じサブネット内の全ての Member AP を一元的に管理します。Master AP が何らかの理由によってオフラインとなった際には、1 台の Member AP が Master AP に代わり、その役割を行います。

また、Master AP が存在するサブネットに Unleashed AP を接続することで、自動的に Member AP として Join し、設定内容などを反映してシステムを自動構築します。

Unleashed ネットワーク基本構成



このように、コントローラの機能を提供しつつも AP ライセンスが不要であるため、価格を重視されるお客様への提案にご活用いただけます。

ただし、コントローラ専用機である ZoneDirector シリーズと比較すると、以下の制限があるのでご注意ください。

- すべての Unleashed AP が同じ管理 VLAN で動作
- Management VLAN の指定はできず、Native VLAN として扱う
- レイヤー3 のローミングに対応していない
- トンネリングされた WLAN はサポートせず、全て AP 折り返し構成
- ロールベースのアクセス制御にはサポートしていない
- IPv6 は非サポート
- SCI、SPoT、North Bound Interface との連携は非サポート

1.2 サポート AP 数と同時接続クライアント数

Unleashed 200.8 より、最大 128 AP、2,048 同時接続クライアントにキャパシティが拡張されました。これは、R510 や R610 などの IEEE802.11ac Wave2 AP 以降にリリースされた AP で、かつ Bridge モードでシステム構築した場合に限ります。R500 などの IEEE802.11ac Wave1 AP が混在したシステム、又はゲートウェイモードでは、これまでのキャパシティである、最大 50 AP、1,024 同時接続クライアントとなりますのでご注意ください。

なお、システムがサポートする最大 AP 数は、以下の WebUI より確認することが可能です。

WebUI より、Access Point >

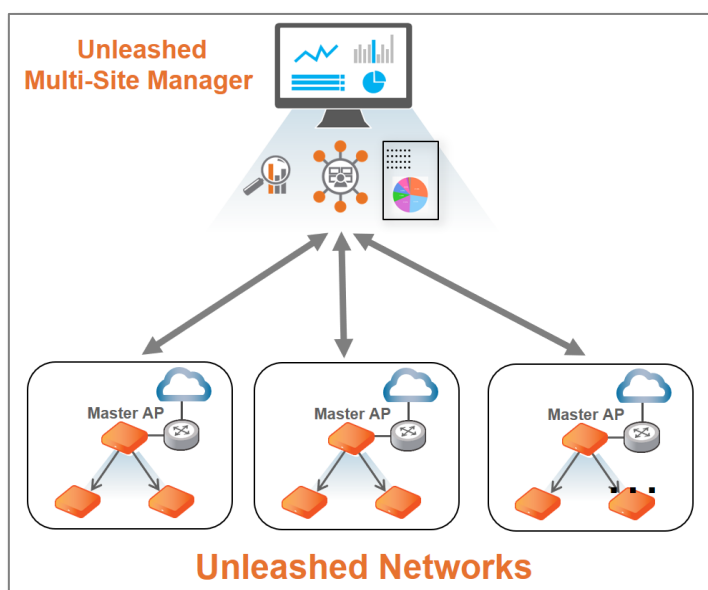


1.3 複数拠点における展開例

基本構成のように、シンプルで小規模なネットワークが複数存在するような、例えば店舗展開などにおいても、Master AP を店舗ごとに配置することで Unleashed による構築が可能です。

このようなマルチサイト環境において管理者の負担を軽減するため、一元管理が行えるよう、Unleashed Multi-Site Manager (UMM) はオプションツールとして用意されております。1 台の UMM で最大 300 の Unleashed ネットワーク (7,500 AP) の管理が可能です。

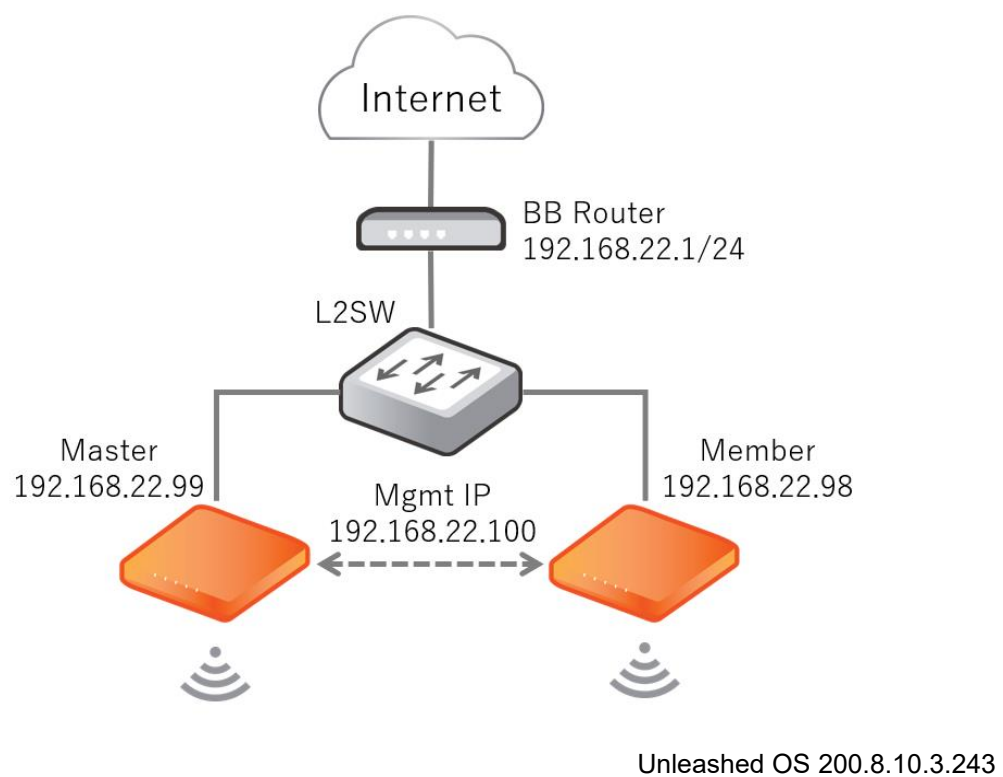
複数拠点の Unleashed を UMM で管理



2 Unleashed セットアップ

各 Unleashed AP のローカル IP は DHCP によって動的に IP アドレスを割当てて構築できますが、導入実績の多くは Static IP を設定している場合が多いため、以下の構成を例にセットアップ方法を解説します。なお、クライアントの IP アドレスは BB Router などの DHCP サーバーから動的に割り当てられることとします。

Unleashed セットアップ構成



2.1 Master AP セットアップ

2.1.1 設定 PC を Unleashed AP へ接続

工場出荷時設定の Unleashed AP の設定を実施するには、以下の手順で設置用 PC を Unleashed AP へ接続します。

1. 工場出荷時の Unleashed AP を、PoE 又は AC アダプタで給電し、起動します。
2. 電源投入後、約 2 分経過すると、暗号化されていない一時的な SSID「Configure.Me-XXXXXX」が立ち上がります。
XXXXXX は、AP の背面に記載されている MAC の下 6 桁です。
3. 設定用 PC の Wi-Fi 設定にて、「Configure.Me-XXXXXX」を選択して帰属します。

設定用 PC の Wi-Fi 設定例 (Windows 10)



4. Web ブラウザ (ie, firefox 推奨) を起動し、以下の URL を入力します。
unleashed.ruckuswireless.com
5. セットアップウィザードにリダイレクトされます。

2.1.2 セットアップウィザードの実行

① Unleashed Install

Language にて「Japanese (日本語)」、「一般的なインストール」を選択し、「次へ」をクリックして次の画面へ進みます。



Unleashed インストール バージョン: 200.8.10.3.243

言語: Japanese (日本語) Web UI で使用する言語を選択してください。

☒ 一般的なインストール これは、UMM を使用しない場合の最も一般的なインストール方法です

☐ UMM インストール UMM からのイメージを使用して Unleashed ネットワークをインストールしてください

UMM Domain/IP: Unleashed ネットワークが構成を取得できる UMM アドレス

構成テンプレート名: Unleashed ネットワーク用に構成テンプレートが事前保存されました

システム名: Ruckus-Unleashed 英数字で最大半角 32 文字を使用してシステムに名前を付けます。空白文字は使用できません。

☐ ローカル アップグレード この Unleashed アクセス ポイントをローカル イメージ ファイルからアップグレードしてください

次へ

① システム設定

システム名を入力し、日本国内で使用する場合には必ず **Japan** を選択します。他国を選択した場合には電波法違反となる場合がありますのでご注意ください。



1 システム 2 IP 設定 3 ワイヤレス LAN 4 管理者 5 レビュー

バージョン: 200.8.10.3.243

名前: Ruckus-Unleashed 英数字で最大半角 32 文字を使用してシステムに名前を付けます。空白文字は使用できません。

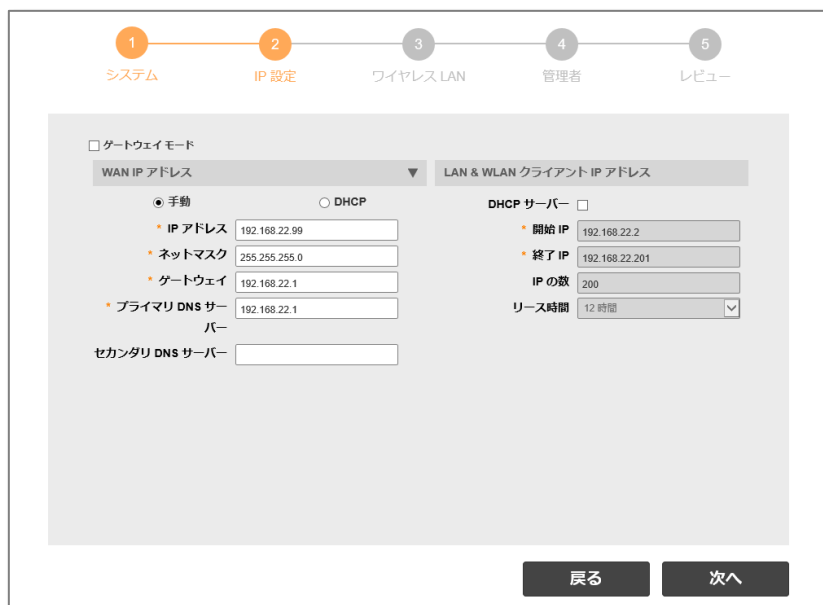
国コード: Japan Unleashed ネットワークに既定の国コードを選択してください。

メッシュ: ☐ Unleashed ネットワークでメッシュを有効にするには、このチェックボックスにチェックを付けます。

戻る **次へ**

② IP 設定

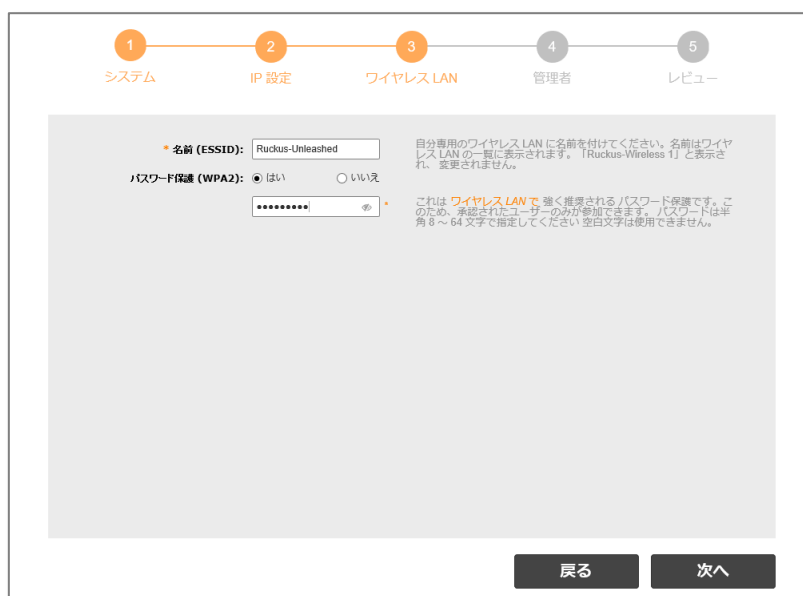
多くのお客様では、IP アドレスを固定で利用されているため、例では、スタティック IP を設定します。また、ゲートウェイモード は Disabled (デフォルト) とし、DHCP サーバーのチェックも外してください (デフォルト)。



③ ワイヤレス LAN 設定

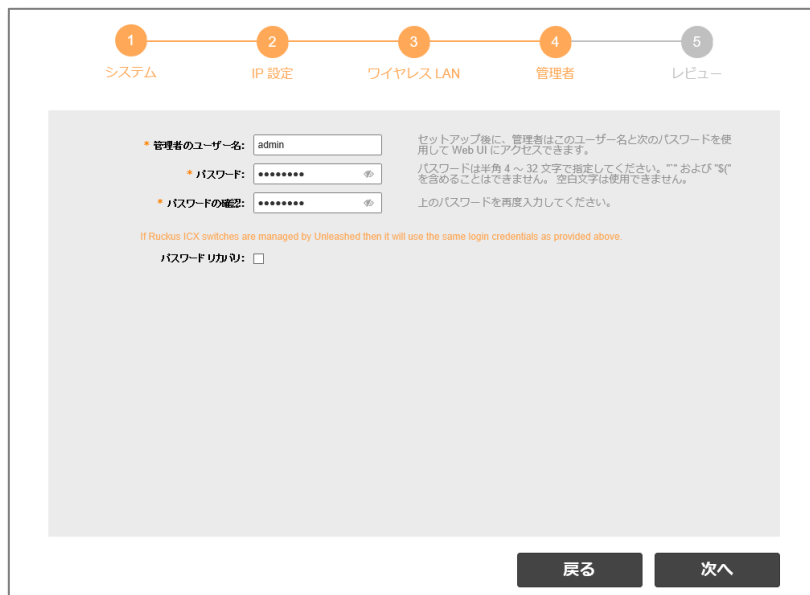
WPA2-PSK の WLAN 設定を行います。実際に使用しない場合でも作成する必要があり、不要な場合にはセットアップウィザード終了後に削除してください。

SSID と パスフレーズを設定し、「次へ」をクリックして次の画面へ進みます。



④ 「管理者」設定

システムの管理者アカウントとパスワードを設定します。アカウント名とパスワードを入力し、「次へ」をクリックして次の画面へ進みます。



⑤ レビュー画面

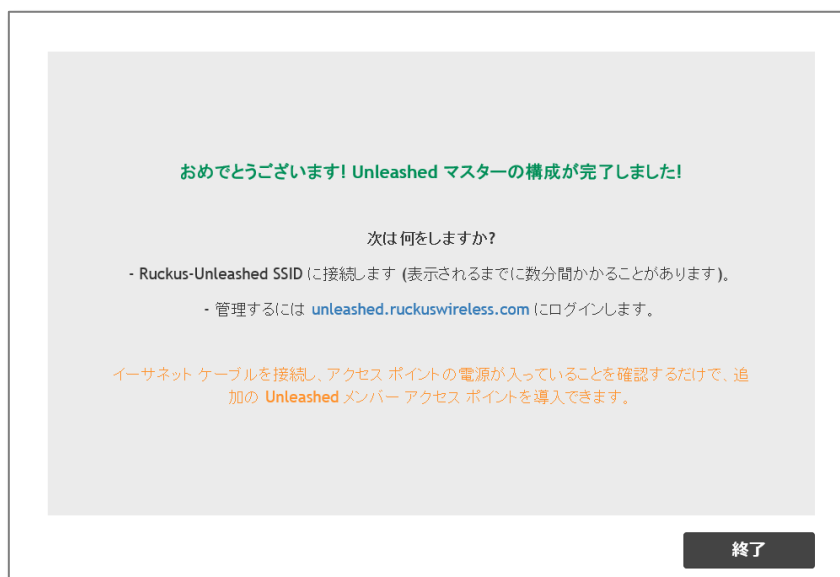
セットアップウィザードで設定した内容が表示されます。内容を確認し、「終了」をクリックするとシステムが再起動されます。再起動後、セットアップ完了画面が表示されるので、「終了」をクリックして下さい。

設定が完了したら、ネットワークに接続して動作確認を実施します。



以下の情報を確認し、[終了] をクリックして構成してください	
システム名	Ruckus-Unleashed
国コード	Japan
内部ゲートウェイ	無効
IP モード	静的 (手動)
IP 設定	192.168.22.99
ワイヤレス LAN	Ruckus-Unleashed
管理者のユーザー名	admin
管理者パスワード	***** ☐ パスワードを表示
パスワードリカバリ	無効
メッシュ	無効
システム時刻	システム時刻は自動設定されています。 (現在の PC 時刻は 2020年4月17日 14:16:54 です)

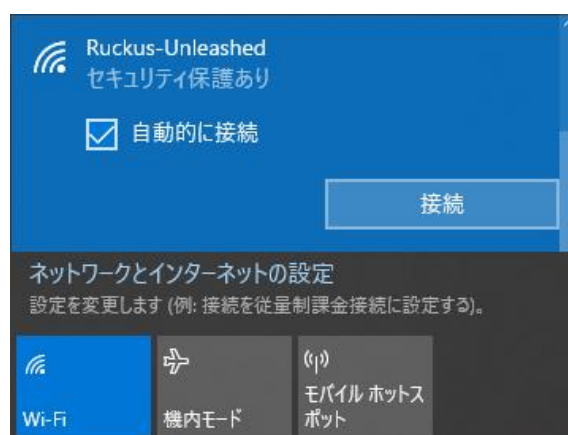
⑥ セットアップ完了



2.1.3 作成した WLAN へ接続し、Unleashed へログイン

この例では、WLAN: Ruckus-Unleashed を作成しました。

接続テストも兼ねて、設定用 PC の Wi-Fi 設定にて、「Ruckus-Unleashed」を選択して無線接続を行います。



Web ブラウザ (ie, firefox 推奨) を起動し、以下の URL を入力し、設定した管理者アカウントにてログインします。

unleashed.ruckuswireless.com



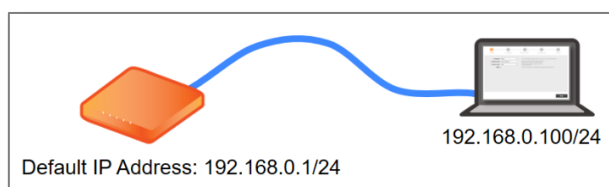
ログインすると、以下のような管理画面が表示されます。



2.2 Member AP セットアップ

DHCP サーバーが存在する環境では、ネットワークに接続することで IP アドレスを取得し、Master AP から WLAN などのグローバル設定を自動的に同期し、起動します。この例では、キッティング作業を想定し、DHCP ではなく、Member AP にあらかじめローカル IP を設定し、その後、ネットワークに接続して Master AP と設定情報の同期を実施します。

設定用 PC と工場出荷時の Unleashed AP を直接イーサネットケーブルで接続し、Unleashed AP を起動します。Unleashed AP 起動後、PC のターミナルソフトを使用して SSH にて <192.168.0.1> へアクセスし、CLI ログインを行います。



CLI ログイン時の注意ですが、AP の起動には約 3 分が必要です。PWR LED が遅い点滅、CTL LED が速い点滅になったのを確認し、実施してください。

- Unleashed CLI

```
Please login: super
Password: sp-admin

Welcome to Ruckus Wireless Unleashed CLI Setup Wizard

Would you like to start the Setup Wizard? [yes/no]: no

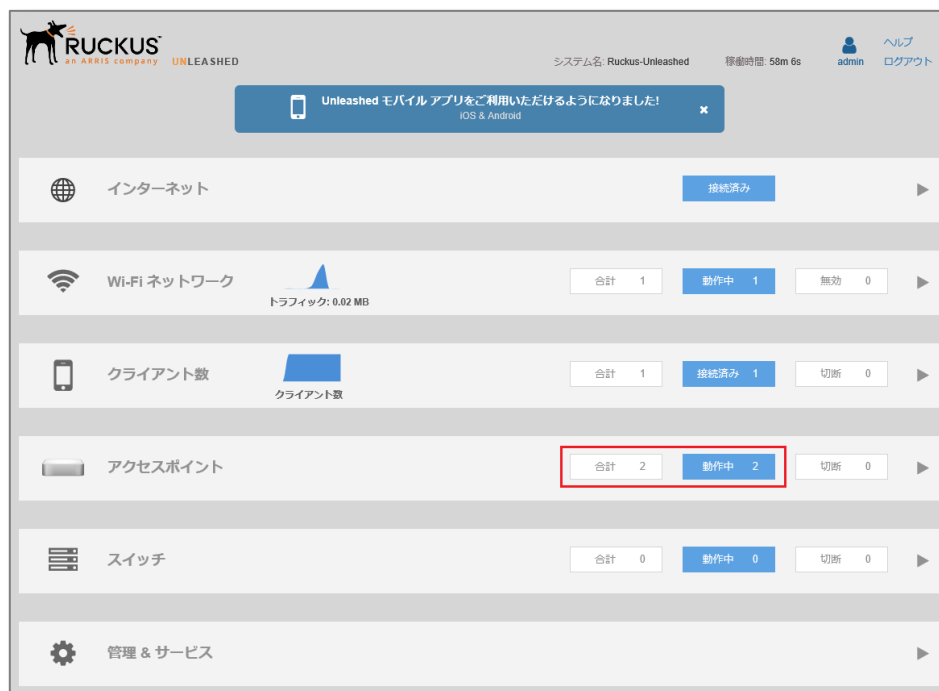
ruckus> enable
ruckus# ap-mode
You have all rights in this mode.
ruckus(ap-mode)# set ipaddr wan 192.168.22.98 255.255.255.0 192.168.22.1
```

上記のコマンドを投入した時点で AP の IP アドレスが変更されるため、SSH 接続が切断されます。

設定した Member AP を Master AP と同じ Unleashed ネットワーク (同一サブネット) に接続し、ジョインさせてください。

2.3 AP 状態の確認

MemberAP を Unleashed ネットワークに接続すると、MemberAP は MasterAP を自動的に発見し、MasterAP からグローバル設定が同期され、Wi-Fi サービスを開始します。



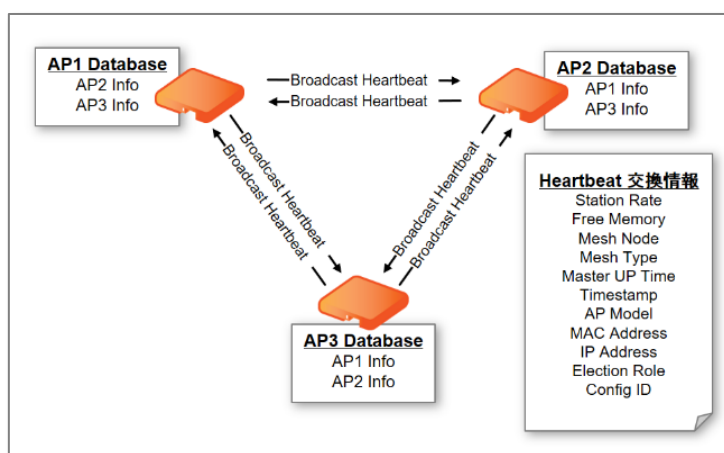
以下は 管理画面の「アクセスポイント」で表示される AP ステータスです。表示される AP を確認してください。



3. Unleashed AP の基本動作

3.1 ブロードキャスト ハートビート による情報交換

Unleashed AP は、その AP の役割 (role) として Master 又は Member のいずれかにアサインされます。同一セグメント上に配置された Unleashed AP は、Role に関わらずブロードキャストによるハートビートを行い、互いの存在、リソース状況、Config ID などを交換し、各 AP の内部データベース (AP DB) へ保存します。ハートビートパケットは、UDP:60000 ポート宛に 5 秒間隔 及び L2 パケットで 10 秒間隔でブロードキャストします。



AP DB の確認は、“get election” コマンドで確認することができます。

```
ruckus (ap-mode) # get election
```

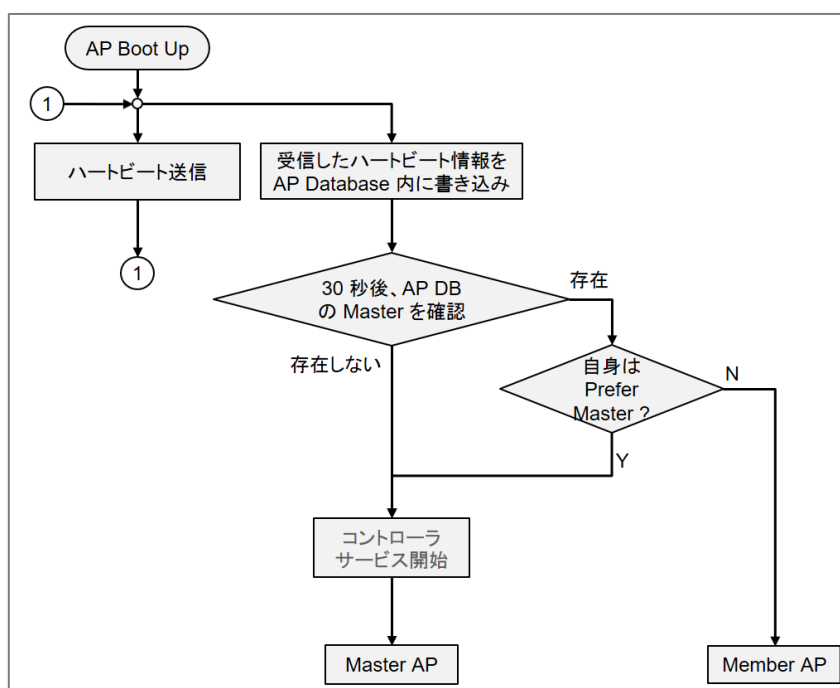
The local AP's ip address is 192.168.22.99, Election role is master, Fix role is NO, Debug level is ERROR, Prefer master is 00:00:00:00:00:00

MacAddress	IpAddress	Role	CfgID	StaRate	FreeMem	MeshEna	MeshNode	MeshNodeType
Model	ActiveVer	BackupVer	SysTime	BoardType	UpTime	LastSeen		
ec:8c:a2:16:69:00	192.168.22.99	master	6	59	294540	0	0	0
R510	200.8.10.3.243	110.0.0.0.663	9503	r510-5-31-4bss	[2 hrs 39 mins 58 secs]			
[Fri Apr 17 08:59:16 2020]								
ec:8c:a2:16:5f:10	192.168.22.98	member	6	60	346884	0	0	0
R510	200.8.10.3.243	114.0.0.0.1360	0	r510-5-31-4bss	[1 hr 54 mins 40 secs]			
[Fri Apr 17 08:59:18 2020]								
OK								

3.2 Unleashed AP の起動

過去に稼働実績がある Unleashed AP は、AP 内部にバックアップファイルとして保存されている設定情報を元に起動します。起動後、ブロードキャストハートビートの送信を開始すると同時に、他の Unleashed AP からのブロードキャストハートビートも受信し、AP DB を構築します。起動して 30 秒後、AP DB より、すでに稼働中の Master AP の存在を確認し、他に Master AP が存在しない場合には自身の Role を Master とします。AP DB 内に Master AP が存在する場合には自身の Role を Member としますが、自身が Prefer AP として設定されている場合には Master とします。

Unleashed AP 基本起動シーケンス



3.3 Master AP 基本動作シーケンス

設定変更が行われると、設定内容をバックアップファイルに保存し、ハートビートでアドバタイズする Config ID 情報を更新します。

また、Master AP が重複しないよう、30 秒毎に AP DB 内に Master AP が存在しないかのチェックを行います。DB 内に Master AP が存在し、それが Prefer Master 又はマスター選択アルゴリズム (MSA) で他 AP が Master AP となった場合には、自身の Role を Member AP へ変更し、再起動します。

また、60 秒毎に Free Memory の確認を行い、100Mbyte 以下の場合にはマスター選択アルゴリズムに従い新たな Master AP を選択します。

なお、マスター選択の優先順位は以下の順に従います。

- 1) Station Rate
- 2) Free memory
- 3) Mesh role と Mesh node
- 4) Up time
- 5) MAC Address (大きい値が優先)

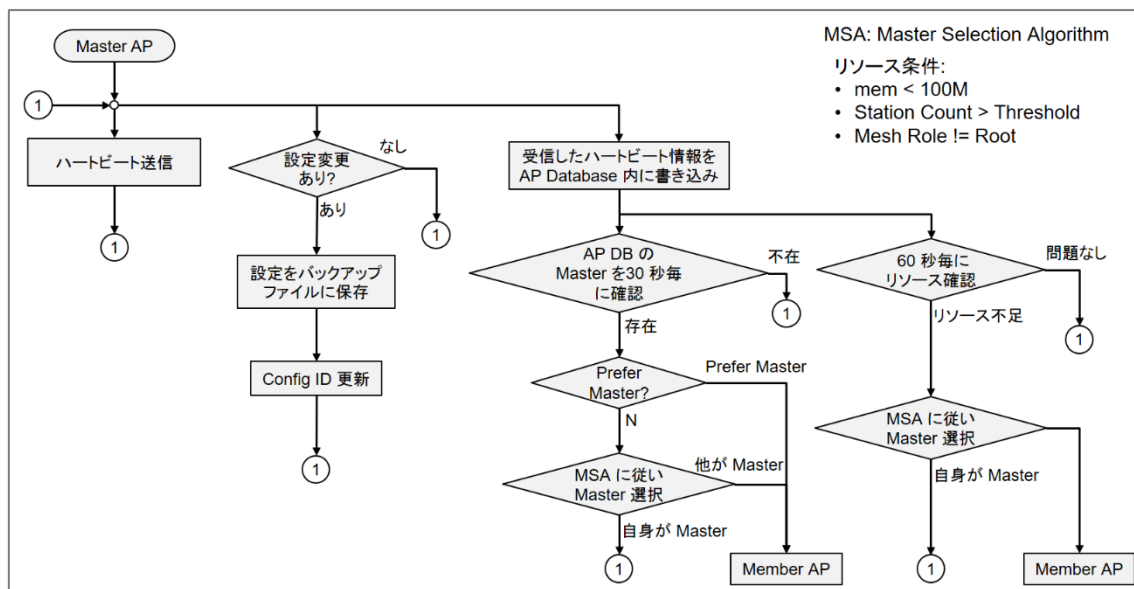
Station Rate は、AP 負荷状況を表す値で大きいほど優先順位が高くなります。

これは、AP のハードウェアスペックによって定められている AP max capacity から、実際に帰属している端末数をマイナスした値となります。

Station Rate = AP max capacity – online station

AP max capacity: R720 (72), R710 (60), R610 (66), R510 (60), R310 (46)

Master AP 基本動作シーケンス

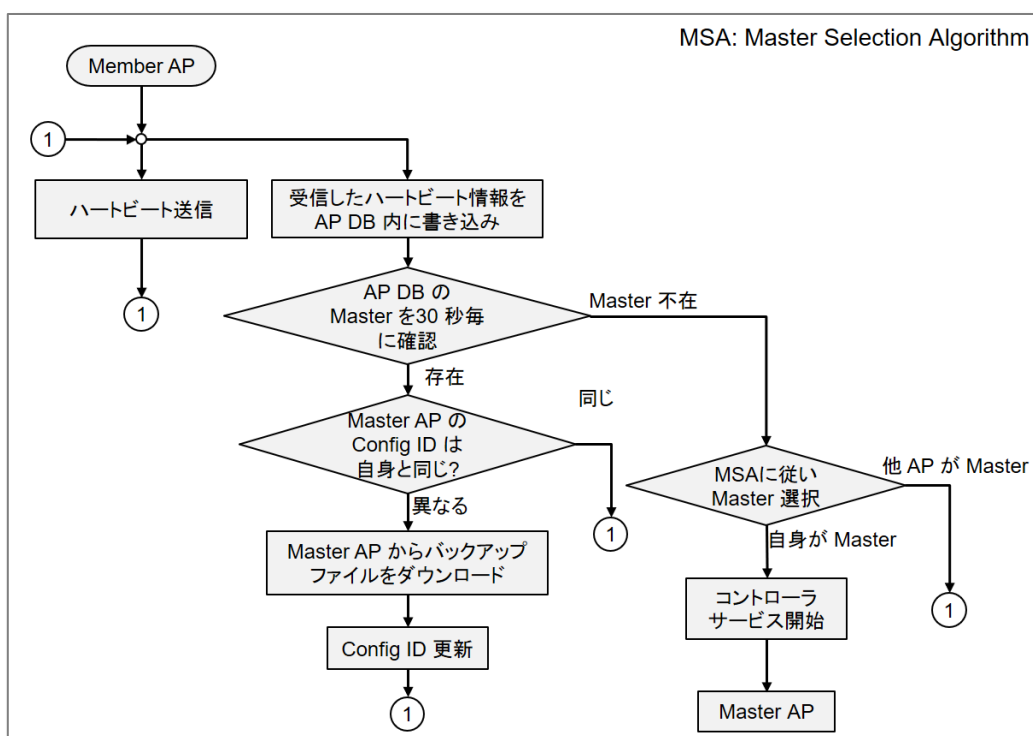


3.4 Member AP 動作基本シーケンス

Role が Member の場合であっても、30 秒毎に AP DB 内の Master AP の存在を確認します。

Master と自身の Config ID が異なる場合には、Master AP のバックアップファイルを自身のバックアップファイルへコピーし、設定内容をメモリに反映し、Config ID を更新します。Master AP が存在しない場合は、マスター選択アルゴリズム (MSA) を用いて Master AP の選択を行います。自身が Master AP に選択した場合には、Role を Master へ変更します。

Member AP 基本動作シーケンス



4 システムマネージメント

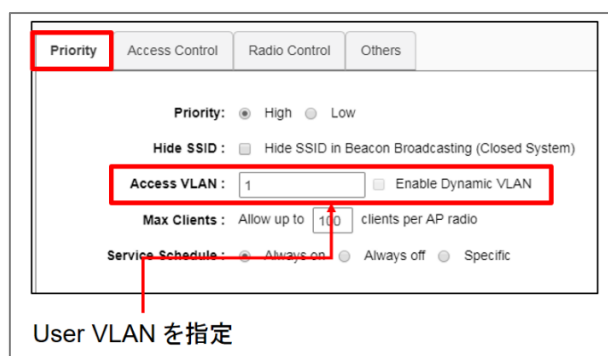
4.1 管理 VLAN と アクセス VLAN

Unleashed AP の Ethernet ポートはトランクポートとして動作し、管理 (Management) VLAN は UnTag であるため、スイッチ側のポート設定が、Native VLAN となるものが管理 VLAN となります。

また、無線ユーザが利用するアクセス VLAN は、WLAN (SSID) 毎にアサイン可能で UnTag 及び Tag をサポートしてます。無線ユーザ VLAN と管理 VLAN を分離したい場合には、以下の WebUI より Access VLAN を指定します。これは WLAN ごとに設定することが可能です。

なお、VLAN ID 1 (デフォルト) は UnTag VLAN として認識します。

WiFi Networks > [Create] [Edit] > Show Advanced Options



アクセス VLAN の指定

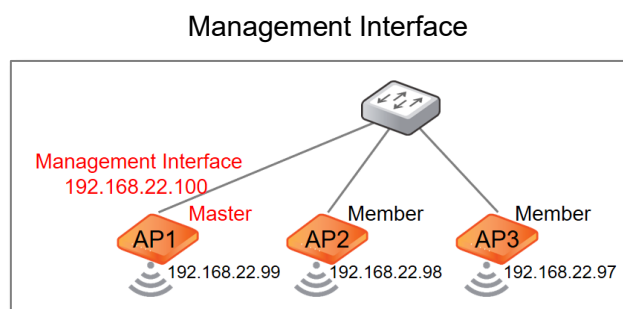
4.2 Master AP と管理 IP アドレス

WebUI で Unleashed システムの管理を行うには、Master AP のローカル IP アドレスに Web アクセスをします。Member AP へ Web アクセスしても自動的に Master AP へリダイレクトされます。

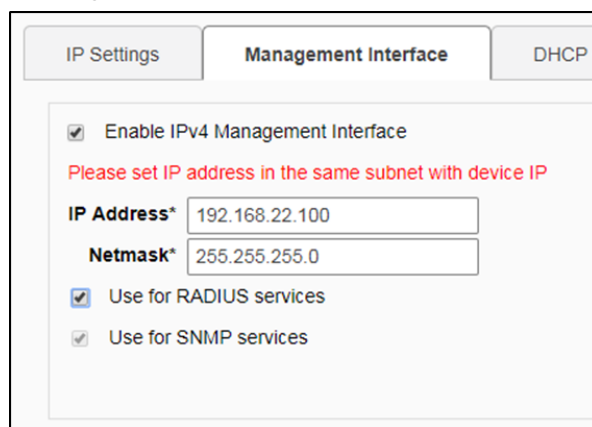
4.2.1 Management Interface の利用

複数の Unleashed AP を管理する場合は、Management Interface の利用をお勧めしま

す。ローカル IP アドレスとは別の IP アドレスを Management Interface として設定することで、Master AP へアクセスできる共通の管理インターフェイスとして動作します。これは、Master AP が変更された場合でも同じ IP アドレスで Master AP へアクセスでき、RADIUS Server へのアクセスや SNMP ターゲット IP としても使用されます。ただし、SNMP Trap は、ローカル IP アドレスが用いられます。なお、Management Interface の IP アドレスは、ローカル IP と同じセグメントの IP アドレスである必要があります。このように Management Interface は、管理用 IP を固定化するために用いられます。



System > IP Setting > Management Interface



Management Interface の設定

4.2.2 Prefer Master

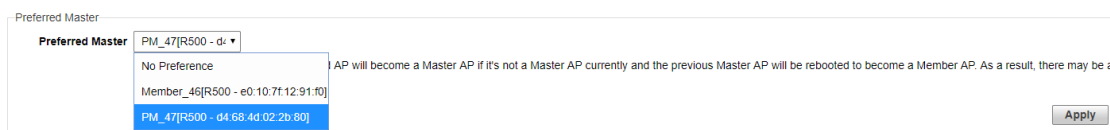
Unleashed システムは、Master AP が何らかの理由によりオフラインになった場合、Member AP の 1 台が Master Role となります。その後、元々 Master として動作していた AP がオンラインになっても、後で Master となった AP が引き続き Master Role を

続します。

Prefer Master は、特定の AP に Master AP を優先させたい場合に利用します。Prefer に設定されている AP が復旧すると Master AP として動作し、先の Master AP は Member へ戻る動作を行います。

Prefer Master の指定は、WebUI から指定することができ、以下のように稼働中の Unleashed AP のひとつから選択します。

System Info > Preferred Master



Prefer Master の指定

設定が反映されると、CLI から Prefer master の登録状態が確認できます。

```
rkscli: get election
```

```
The local AP's ip address is 192.168.22.98, Election role is member, Fix role is NO, Debug level is ERROR, Prefer master is d4:68:4d:25:35:30
```

```
mac_address ipaddress role configID station_rate free_memory mesh_enabled mesh_node
mesh_node_type model version bak_version systime board_type uptime last_seen
```

```
-----
d4:68:4d:02:34:a0 192.168.22.98 member 29 48 181060 0 0 0 R500 200.5.10.0.179 3.6.0.99.499
0 zf7752-3-29-4bss 1 day 1 hr 44 mins 34 secs Fri Sep 22 09:38:48 2017
d4:68:4d:25:35:30 192.168.22.99 master 29 48 170992 0 0 0 R500 200.5.10.0.179 3.6.0.99.499
92784 zf7752-3-29-4bss 2 days 14 mins 27 secs Fri Sep 22 09:38:46 2017
OK
```

4.2.3 Role の固定化

クライアント接続数が多い AP は Master として動作させず、Member AP として固定させたい場合、以下のコマンドで設定することができます。

```
set election {options}
```

```
-> role <0=Clear 1=Member 3=Master>
```

```
-> debug <1=ERROR 2=WARN 4=INFO 8=DEBUG>
```

```
rkscli: set election role 1
```

```
Fix role set ok
```

```
OK
```

```
rkscli: get election
```

```
The local AP's ip address is 192.168.22.98, Election role is member, Fix role is member,  
Debug level is ERROR, Prefer master is d4:68:4d:25:35:30
```

```
mac_address ipaddress role configID station_rate free_memory mesh_enabled mesh_node  
mesh_node_type model version bak_version systime board_type uptime last_seen
```

```
-----  
d4:68:4d:02:34:a0 192.168.22.98 member (Fix) 29 48 180636 0 0 0 R500 200.5.10.0.179  
3.6.0.99.499 0 zf7752-3-29-4bss 1 day 1 hr 49 mins 5 secs Fri Sep 22 09:43:15 2017  
d4:68:4d:25:35:30 192.168.22.99 master 29 48 170704 0 0 0 R500 200.5.10.0.179 3.6.0.99.499  
93056 zf7752-3-29-4bss 2 days 18 mins 59 secs Fri Sep 22 09:43:12 2017  
OK
```

オプションで debug 時の出力レベルを指定することが可能です。通常運用時に設定する必要はなく、トラブルシューティングでご活用ください。

Master AP を固定したい場合は、前述の Prefer Master の利用を推奨します。

4.2.4 管理インターフェイスへのアクセス制限

管理者アクセスを特定のネットワークからのみにすることで、セキュリティを向上させることが可能です。必要に応じて以下の手順で実施してください。

なお、Unleashed システムでは、CLI より管理インターフェイスへのアクセス制御の設定が可能です。WebUI 経由での設定は受け付けておりません。

- 1) Mgmt-ACL を作成
- 2) アクセス許可するアドレスを以下のいずれかで登録
 - IP アドレス : restrict-type single ip-addr <ip address>
 - サブネット単位 : restrict-type subnet ip-subnet <ip Network address> <mask>
 - IP アドレスレンジ : restrict-type range ip-range <開始 ip address> <終了 ip address>

以下は、192.168.22.0/24 からのみ管理アクセスを許可する設定の例です。

```
Please login: admin
Password:
Welcome to Ruckus Unleashed Network Command Line Interface
ruckus> enable
ruckus# config
You have all rights in this mode.
ruckus(config)# system
ruckus(config-sys)# mgmt-acl mgmt-subnet
ruckus(config-mgmt-acl)# restrict-type subnet ip-subnet 192.168.22.0 255.255.255.0
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-mgmt-acl)# show
Management ACL:
    Name= mgmt-subnet
    Restriction Type= subnet
    IP subnet= 192.168.22.0/255.255.255.0
ruckus(config-mgmt-acl)# end
The management ACL 'mgmt-subnet' has been updated and saved.
Your changes have been saved.
ruckus(config-sys)#
```

4.3 Unleashed イベント管理

Unleashed は、動作変更時や障害時など、イベント情報を目的ごとに管理しています。ここでは以下の管理について解説します。

- Alarms
- Events
- Logs
- Syslog
- SNMP
- Debug info

4.3.1 Alarms

Member AP が Master AP との接続性が失われた時や、認証サーバーとの到達性が失われた時など、システムにとって重要なイベントが発生した際にアラームとして表示します。このアラームメッセージは、以下の WebUI にて確認することができ、AP が再起動しても引き続き表示され、管理者が意図的にクリアしない限り表示されます。

Admin & Services > Administer > Diagnostics > All Alarms

All Alarms	Events	Debug Info	Logs	Remote Troubleshooting																														
All Alarms This workspace lists all uncleared alarms. If all listed alarms have been cleared or are no longer valid, click Clear All. <table> <tr> <th>Date/Time</th><th>Name</th><th>Severity</th><th>Activities</th><th>Action</th></tr> <tr> <td>2017/10/10 18:12:28</td><td>AP Has Joined</td><td>High</td><td>AP[d4:68:4d:02:34:a0] joins with uptime [63] s and last disconnected reason [AP Restart : application reboot]</td><td>Clear</td></tr> <tr> <td>2017/10/10 16:23:57</td><td>AP Has Joined</td><td>High</td><td>AP[d4:68:4d:25:35:30] joins with uptime [57] s and last disconnected reason [AP Restart : application reboot]</td><td>Clear</td></tr> <tr> <td>2017/10/10 16:22:34</td><td>AP Has Joined</td><td>High</td><td>AP[d4:68:4d:25:35:30] joins with uptime [63] s and last disconnected reason [AP Restart : application reboot]</td><td>Clear</td></tr> <tr> <td>2017/10/10 12:46:07</td><td>AP Has Joined</td><td>High</td><td>AP[d4:68:4d:02:2b:80] joins with uptime [155] s and last disconnected reason [AP Restart : power cycle]</td><td>Clear</td></tr> <tr> <td>2017/10/10 12:46:06</td><td>AP Has Joined</td><td>High</td><td>AP[e0:10:7f:12:91:f0] joins with uptime [159] s and last disconnected reason [AP Restart : power cycle]</td><td>Clear</td></tr> </table> Search terms restart ☒ Include all terms ☐ Include any of these terms Refresh Clear All 1-5 (5)					Date/Time	Name	Severity	Activities	Action	2017/10/10 18:12:28	AP Has Joined	High	AP[d4:68:4d:02:34:a0] joins with uptime [63] s and last disconnected reason [AP Restart : application reboot]	Clear	2017/10/10 16:23:57	AP Has Joined	High	AP[d4:68:4d:25:35:30] joins with uptime [57] s and last disconnected reason [AP Restart : application reboot]	Clear	2017/10/10 16:22:34	AP Has Joined	High	AP[d4:68:4d:25:35:30] joins with uptime [63] s and last disconnected reason [AP Restart : application reboot]	Clear	2017/10/10 12:46:07	AP Has Joined	High	AP[d4:68:4d:02:2b:80] joins with uptime [155] s and last disconnected reason [AP Restart : power cycle]	Clear	2017/10/10 12:46:06	AP Has Joined	High	AP[e0:10:7f:12:91:f0] joins with uptime [159] s and last disconnected reason [AP Restart : power cycle]	Clear
Date/Time	Name	Severity	Activities	Action																														
2017/10/10 18:12:28	AP Has Joined	High	AP[d4:68:4d:02:34:a0] joins with uptime [63] s and last disconnected reason [AP Restart : application reboot]	Clear																														
2017/10/10 16:23:57	AP Has Joined	High	AP[d4:68:4d:25:35:30] joins with uptime [57] s and last disconnected reason [AP Restart : application reboot]	Clear																														
2017/10/10 16:22:34	AP Has Joined	High	AP[d4:68:4d:25:35:30] joins with uptime [63] s and last disconnected reason [AP Restart : application reboot]	Clear																														
2017/10/10 12:46:07	AP Has Joined	High	AP[d4:68:4d:02:2b:80] joins with uptime [155] s and last disconnected reason [AP Restart : power cycle]	Clear																														
2017/10/10 12:46:06	AP Has Joined	High	AP[e0:10:7f:12:91:f0] joins with uptime [159] s and last disconnected reason [AP Restart : power cycle]	Clear																														

Alarms

4.3.2 Events

以下の WebUI より、Unleashed 内部に保存されるログファイルの直近 64 イベントを表示します。アラームと比較し、重要度が低いメッセージが含まれ、不正 AP 検出、AP チャネル変更、コンフィグ同期、クライアント帰属などがイベントとして表示されます。Unleashed 200.7 からの拡張機能によって、表示するイベントレベルの設定が可能になりました。Any (全て)、Critical & Warning、Critical Only から選択可能です。

Admin & Services > Administer > Diagnostics > Events

All Alarms

Events

Debug Info

Logs

Remote Troubleshooting

Client Troubleshooting

Events Settings

Select severity level of events to be show in next Events section

Event Log Level:

Any

Critical & Warning

Critical Only

Apply

Events

This workspace displays the most recent records in Unleashed's internal log file. (For information on saving this information to a syslog server, see the Online Help.)

Date/Time	Severity	User	Activities
2019/04/23 16:56:32	High		User[90:94:97:e5:28:43] が AP[e0:10:7f:12:91:f0] から WLAN[UN-HN] に参加しようとして、連続して何度も認証に失敗しています。User[90:94:97:e5:28:43] は [30 seconds] によりシステムから一時的にブロックされます。
2019/04/23 14:14:09	High		User[f4:cb:52:49:8d:e3] が AP[d4:68:4d:02:2b:80] から WLAN[UN-HN] に参加しようとして、連続して何度も認証に失敗しています。User[f4:cb:52:49:8d:e3] は [30 seconds] によりシステムから一時的にブロックされます。

Events

4.3.3 Logs

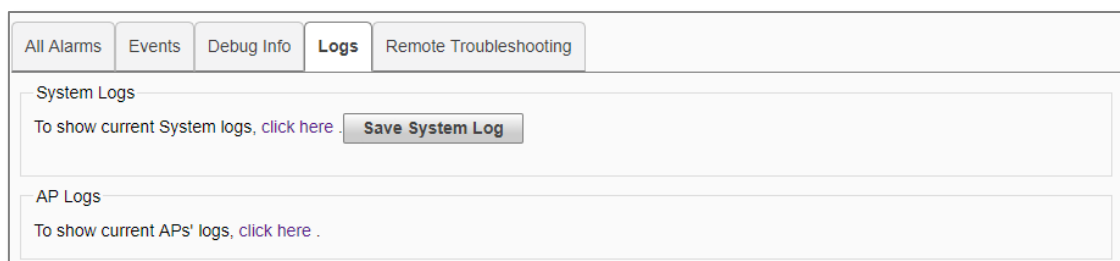
- System Logs

システムログは、Alarms, Events, AP Logs 全てを含んでいるログ情報です。WebUI では、システムログの表示とシステム内に保存しているログのダウンロードを提供します。なお、システムログは、10,000 行のテキストファイルを .tar 形式で圧縮して保存し、最大 21 ファイルを Unleashed システム内に保存することが可能です。

- AP Logs

以下の WebUI より、AP に関連するログの表示を提供します。

Admin & Services > Administer > Diagnostics > Logs



Logs

4.3.4 Syslog

Unleashed システム内に保存可能なログ情報には上限があるため、ログ情報の保存が重要な場合には、外部 Syslog サーバーを用いることをお勧めします。Syslog サーバーの登録は Command Line Interface (CLI) から 1 台に限り可能です。

Syslog メッセージは、コントローラに関する情報は Master AP から送信され、AP に関する情報は各 Member AP から送信されます。また、送信元 IP アドレスは Management Interface は使用されず、ローカル IP が用いられます。

設定パラメータ

server <IP-ADDR>	Syslog サーバアドレスを登録
facility <FACILITY NAME>	Syslog facility (local0 - local7) を設定
priority <PRIORITY LEVEL>	Syslog レベル (emerg, alert, crit, err, warning,

	notice, info, debug) を設定
ap-facility <FACILITY NAME>	AP Syslog facility (local0 - local7) を設定
ap-priority <PRIORITY LEVEL>	AP Syslog レベル (emerg, alert, crit, err, warning, notice, info, debug) を設定

以下は、Syslog サーバーの設定例です。

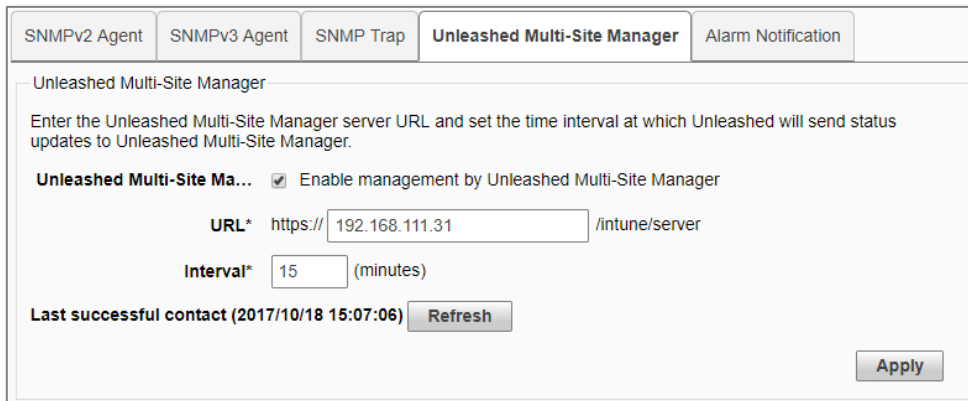
```
ruckus(config)# system
ruckus(config-sys)# syslog
ruckus(config-sys-syslog)# server 192.168.222.183
ruckus(config-sys-syslog)# facility local0
The syslog settings have been updated.
ruckus(config-sys-syslog)# ap-facility local1
The syslog settings have been updated.
ruckus(config-sys-syslog)# priority warning
The syslog settings have been updated.
ruckus(config-sys-syslog)# ap-priority warning
The syslog settings have been updated.
ruckus(config-sys-syslog)# end
The syslog settings have been updated.
Your changes have been saved.
ruckus(config-sys)# show
Country Code:
  Code= Japan
Identity:
  Name= Ruckus-Unleashed
Session Statistics:
  Enable= false
  Limited Unauthorized Session= true
NTP:
  Status= Enabled
  Address= ntp.ruckuswireless.com
  Timezone= GMT+9
Log:
  Status= Enabled
  Address= 192.168.222.183
  Facility= local0
  Priority= warning
  AP Facility= local1
  AP Priority= warning
  event log level= 1
--- 省略 ---

ruckus(config-sys)#
```

4.4 Unleashed Multi-Site Manager による管理

以下の WebUI より Unleashed Multi-Site Manager (UMM) の登録を行います。

Administer > Network Management > [Unleashed Multi-Site Manager]



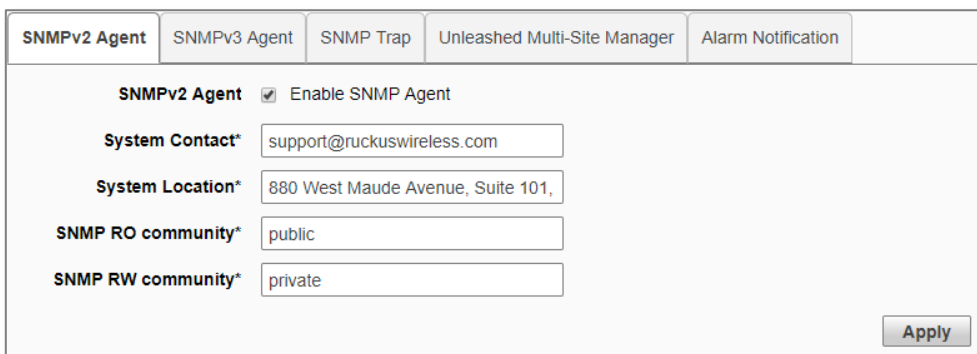
The screenshot shows the 'Unleashed Multi-Site Manager' configuration page. At the top, there are tabs: 'SNMPv2 Agent', 'SNMPv3 Agent', 'SNMP Trap', 'Unleashed Multi-Site Manager' (selected), and 'Alarm Notification'. Below the tabs, the page title is 'Unleashed Multi-Site Manager'. The main content area contains the following text: 'Enter the Unleashed Multi-Site Manager server URL and set the time interval at which Unleashed will send status updates to Unleashed Multi-Site Manager.' Below this, there is a section 'Unleashed Multi-Site Ma...' with a checkbox 'Enable management by Unleashed Multi-Site Manager' which is checked. Underneath, there is a 'URL*' field with the value 'https://192.168.111.31/intune/server' and an 'Interval*' field with the value '15 (minutes)'. At the bottom left, it says 'Last successful contact (2017/10/18 15:07:06)' with a 'Refresh' button. At the bottom right, there is an 'Apply' button.

Unleashed Multi-Site Manager 設定画面

4.5 SNMP による管理

Unleashed では、SNMP v2 / v3 および、SNMP Trap をサポートしております。SNMP Trap を行うには、以下の WebUI より Protocol, Community, Trap 先の Server を指定し、MIB ツールなどを使って SNMP SET で TRAP するイベントを指定する必要があります。

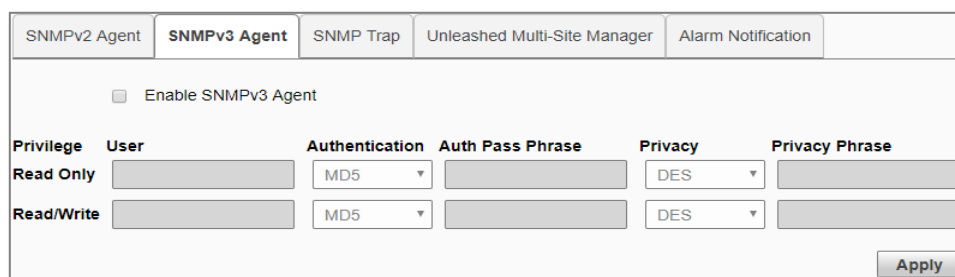
Administer > Network Management > [SNMPv2 Agent]



The screenshot shows the 'SNMPv2 Agent' configuration page. At the top, there are tabs: 'SNMPv2 Agent' (selected), 'SNMPv3 Agent', 'SNMP Trap', 'Unleashed Multi-Site Manager', and 'Alarm Notification'. Below the tabs, the page title is 'SNMPv2 Agent'. The main content area contains the following text: 'SNMPv2 Agent' with a checkbox 'Enable SNMP Agent' which is checked. Below this, there are four fields: 'System Contact*' with the value 'support@ruckuswireless.com', 'System Location*' with the value '880 West Maude Avenue, Suite 101,', 'SNMP RO community*' with the value 'public', and 'SNMP RW community*' with the value 'private'. At the bottom right, there is an 'Apply' button.

SNMP v2 設定画面

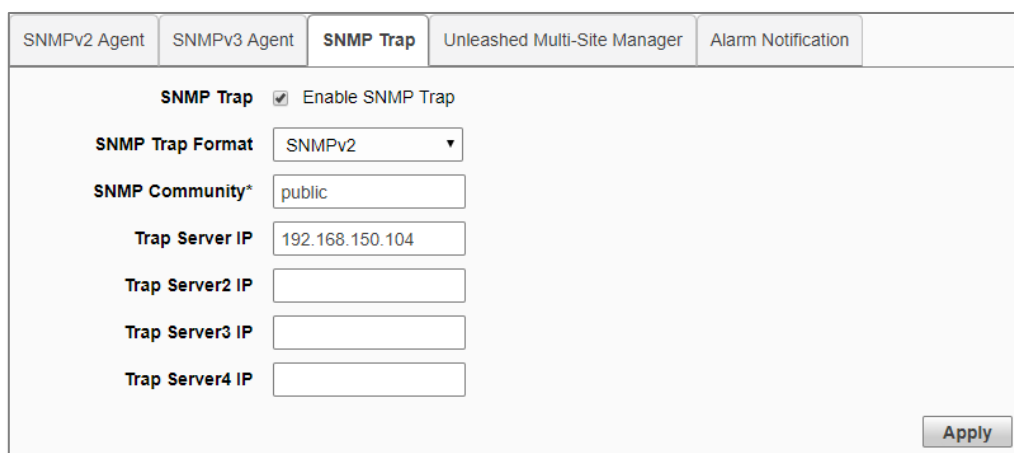
Administer > Network Management > [SNMPv3 Agent]



The screenshot shows the 'SNMPv3 Agent' configuration page. At the top, there are tabs for 'SNMPv2 Agent', 'SNMPv3 Agent' (selected), 'SNMP Trap', 'Unleashed Multi-Site Manager', and 'Alarm Notification'. Below the tabs, there is a checkbox labeled 'Enable SNMPv3 Agent'. Underneath, there are two rows of configuration fields. The first row is for 'Read Only' privileges, and the second row is for 'Read/Write' privileges. Each row has fields for 'User', 'Authentication' (with a dropdown menu showing 'MD5'), 'Auth Pass Phrase', 'Privacy' (with a dropdown menu showing 'DES'), and 'Privacy Phrase'. An 'Apply' button is located at the bottom right.

SNMP v3 設定画面

Administer > Network Management > [SNMP Trap]

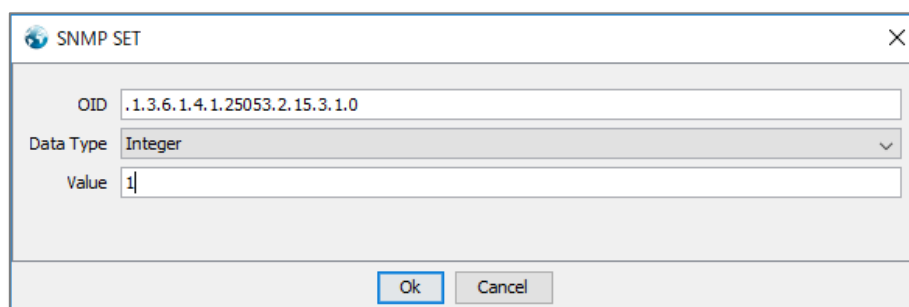


The screenshot shows the 'SNMP Trap' configuration page. At the top, there are tabs for 'SNMPv2 Agent', 'SNMPv3 Agent', 'SNMP Trap' (selected), 'Unleashed Multi-Site Manager', and 'Alarm Notification'. Below the tabs, there is a checkbox labeled 'Enable SNMP Trap' which is checked. Underneath, there are several configuration fields: 'SNMP Trap Format' (dropdown menu showing 'SNMPv2'), 'SNMP Community*' (text field with 'public'), 'Trap Server IP' (text field with '192.168.150.104'), 'Trap Server2 IP' (text field), 'Trap Server3 IP' (text field), and 'Trap Server4 IP' (text field). An 'Apply' button is located at the bottom right.

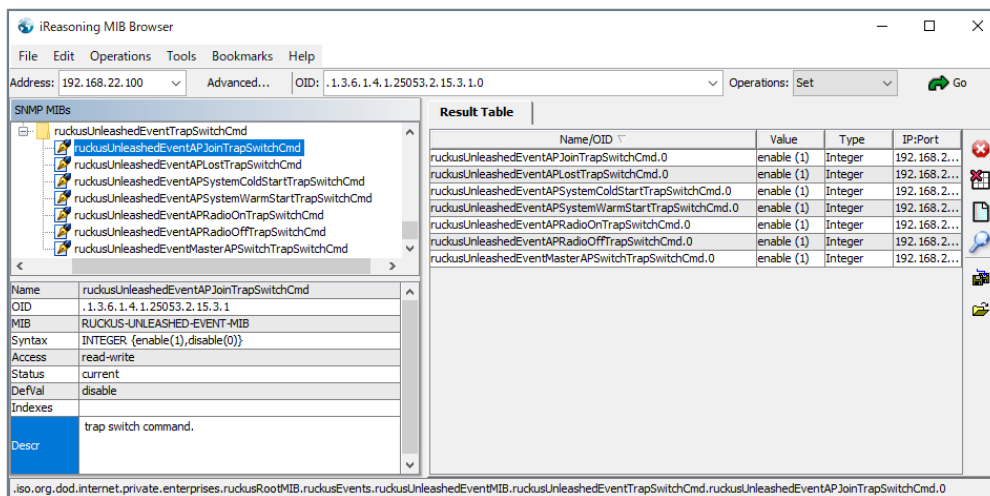
SNMP Trap 設定画面

また、以下は MIB ツールを使って SNMP SET を行った例です。

SNMP Trap 指定



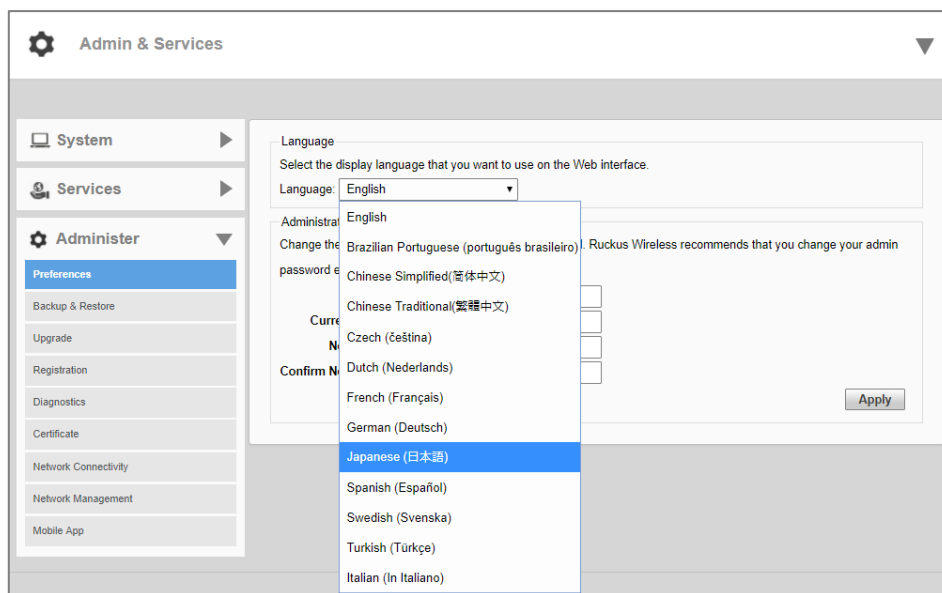
The screenshot shows a dialog box titled 'SNMP SET'. It has a close button (X) in the top right corner. Inside the dialog, there are three fields: 'OID' (text field with '.1.3.6.1.4.1.25053.2.15.3.1.0'), 'Data Type' (dropdown menu showing 'Integer'), and 'Value' (text field with '1'). At the bottom, there are 'Ok' and 'Cancel' buttons.



4.6 マルチ言語のサポート

Unleashed システムの WebUI は、複数言語のサポートを行っており、日本語による管理を行うことが可能です。設定は WebUI から容易に可能です。

Admin & Services > Administer > Preferences



WebUI 言語指定

5 WLAN サンプルコンフィグ

Unleashed でよく利用されている WLAN の設定例を紹介します。

5.1 Open PSK

最もシンプルな設定で、セットアップウィザードでも作成することができます。以下の WebUI から設定することができます。

WiFi ネットワーク > 作成 又は 編集

WLAN の編集

* 名前: unleashed.40

使用タイプ: ☒ 標準 大部分の通常のワイヤレスネットワークで使用
☐ ゲスト アクセス ゲスト アクセス ポリシーおよびアクセス制御が適用されます
☐ ホットスポット サービス WISPr として知られる
☐ ソーシャル メディア ソーシャル メディア ネットワークから認証します

認証方法: ☒ オープン ☐ 802.1X EAP ☐ MAC アドレス

暗号化方法: ☒ WPA2 ☐ None

パスワード: ruckus123 [パスワードを非表示](#)

アカウント サーバー: 無効 [新規作成](#)

仮更新を次の間隔で送信: 分

詳細オプションを表示 ▶

OK

キャンセル

詳細オプションを非表示 ▼

Zero-IT & DPSK

優先度

アクセス制御

無線制御

その他

優先度: ☒ 高 ☐ 低

SSID を非表示: ☐ ビーコンのブロードキャストで SSID を非表示にします (クローズ システム)

アクセス VLAN: 1 ☐ 動的 VLAN を有効にする

クライアントの最大数: 最大許可数 100 アクセス ポイントごとのクライアント数

サービス スケジュール: ☒ 常時オン ☐ 常時オフ ☐ 特定

OK

キャンセル

WLAN PSK 設定

5.2 WPA2-PSK-AES と MAC アドレス認証

小規模ネットワークにおいて、WPA2-PSK で MAC アドレス認証を行いたいというエンドユーザ様は数多くいらっしゃると思います。Unleashed 内部ユーザデータベース (Local Database) 又は外部 RADIUS サーバーと連携して MAC アドレス認証を行う WLAN を構築します。以下の WebUI から設定することができます。

WiFi ネットワーク > 作成 又は 編集



WLAN MAC アドレス認証 設定

Local Database へのユーザ登録は以下 WebUI の「新規作成」より行います。MAC アドレスの登録フォーマットは、「aabbccddeeff」です。

管理 & サービス > システム > ユーザ



ユーザー名	姓名	役割	操作
新規作成			

検索用語: ☒ すべての用語を含む ☐ これらの用語のいずれかを含む

内部データベースの登録

* ユーザー名
 姓 名
 * パスワード
 * パスワードの確認
 役割

システム

システム情報

IP 設定

システム時刻

国コード

役割

ユーザー

メッシュ

サービス

管理者

内部ユーザー データベース (Unleashed)

この表には、現在のすべてのユーザー アカウントと基本情報の一覧が表示されます。ユーザー アカウントは追加、編集、削除できます。また、[印刷] ボタンをクリックして、ユーザー向けの『ワイヤレス ネットワークに初めて接続する場合のガイド』を印刷することもできます。

作成

編集

複製

削除

印刷

ユーザー名	姓 名	役割
2c200bf39b08		Default

1 件中 1-1 件を表示

外部 RADIUS サーバーと連携する場合には、以下 WebUI の設定画面より RADIUS サーバーの登録を行い、認証サーバーを選択します。

管理 & サービス > サービス > AAA サーバー

新規作成

名前

タイプ ☐ Active Directory ☒ RADIUS ☐ RADIUS 会計

暗号化 ☐ TLS

認証方法 ☒ PAP ☐ CHAP

バックアップ RADIUS ☐ バックアップ RADIUS のサポートを有効にする

IP アドレス*

ポート*

共有シークレット*

シークレットの確認*

再試行ポリシー

リクエストタイムアウト* 秒間

再試行の最大数* 回

5.3 802.1X EAP

Unleashed 内部ユーザデータベース (Local Database) 又は外部 RADIUS サーバーと連携して 802.1X 認証によるセキュアな WLAN を構築します。以下の WebUI から設定することができます。

WiFi ネットワーク > 作成 又は 編集



名前: unleashed.40.eap

使用タイプ: ☒ 標準 大部分の通常のワイヤレスネットワークで使用
☐ ゲスト アクセス ゲスト アクセス ポリシーおよびアクセス制御が適用されます
☐ ホットスポット サービス WISPr として知られる

認証方法: ☐ オープン ☒ 802.1X EAP ☐ MAC アドレス

認証サーバー: Local Database ▼ +

WLAN サバイバビリティ: 無効 ▼

キャッシュ時間: [] 時間

アカウントサーバー: 無効 ▼ +

仮更新を次の間隔で送信: 10 分

WLAN 802.1X EAP 設定

Local Database へのユーザ登録は以下 WebUI の「新規作成」より行います。

管理 & サービス > システム > ユーザ



管理 & サービス

システム ▼

- システム情報
- IP 設定
- システム時刻
- 国コード
- 役割
- ユーザー**
- メッシュ

サービス ▶

管理者 ▶

内部ユーザー データベース (Unleashed)

この表には、現在のすべてのユーザー アカウントと基本情報の一覧が表示されます。ユーザー アカウントは追加、編集、削除できます。また、[印刷] ボタンをクリックして、ユーザー向けの『ワイヤレス ネットワークに初めて接続する場合のガイド』を印刷することもできます。

ユーザー名	姓名	役割	操作
			新規作成
			削除 0-0 (0)

検索用語: [] ☒ すべての用語を含む ☐ これらの用語のいずれかを含む

内部データベースの登録

新規作成

ユーザー名*

姓

パスワード*

パスワードの確認*

役割

内部ユーザー データベース (Unleashed)

この表には、現在のすべてのユーザー アカウントと基本情報の一覧が表示されます。ユーザー アカウントは追加、編集、削除できます。また、[印刷] ボタンをクリックして、ユーザー向けの『ワイヤレス ネットワークに初めて接続する場合のガイド』を印刷することもできます。

☐	ユーザー名	姓	役割	操作
☐	localuser1		Default	編集 複製 印刷
☐	localuser2		Default	編集 複製 印刷
☐	localuser3		Default	編集 複製 印刷
☐	localuser4		Default	編集 複製 印刷
☐	localuser5		Default	編集 複製 印刷

[新規作成](#)

[削除](#) 1-5 (5)

検索用語 ☒ すべての用語を含む ☐ これらの用語のいずれかを含む

外部 RADIUS サーバーと連携する場合には、以下 WebUI の設定画面より RADIUS サーバーの登録を行い、認証サーバーを選択します。

管理 & サービス > サービス > AAA サーバー

新規作成

名前

タイプ ☐ Active Directory ☒ RADIUS ☐ RADIUS 会計

暗号化 ☐ TLS

認証方法 ☒ PAP ☐ CHAP

バックアップ RADIUS ☐ バックアップ RADIUS のサポートを有効にする

IP アドレス*

ポート*

共有シークレット*

シークレットの確認*

再試行ポリシー

リクエストタイムアウト* 秒間

再試行の最大数* 回

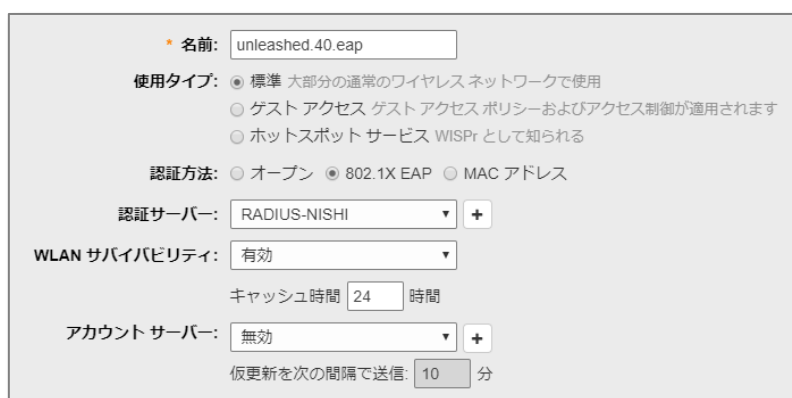
認証サーバーの作成

5.3.1 WLAN サバイバビリティ

Unleashed 200.7 より、802.1x EAP 認証で接続したクライアント情報を特定時間キャッシュし、遠隔地に存在する RADIUS サーバーとの接続性を失っても、接続性を維持し、ローミングや再接続を可能にします。システムでキャッシュできるクライアント数は、最大 800 とし、キャッシュ時間は 1~168 時間とします。

以下の WebUI より、WLAN 設定の「WLAN サバイバビリティ」を有効化し、キャッシュ時間を指定してください。

WiFi ネットワーク > 作成 又は 編集



* 名前: unleashed.40.eap

使用タイプ: ☒ 標準 大部分の通常のワイヤレスネットワークで使用
☐ ゲスト アクセス ゲスト アクセス ポリシーおよびアクセス制御が適用されます
☐ ホットスポット サービス WISPr として知られる

認証方法: ☐ オープン ☒ 802.1X EAP ☐ MAC アドレス

認証サーバー: RADIUS-NISHI +

WLAN サバイバビリティ: 有効

キャッシュ時間 24 時間

アカウント サーバー: 無効 +

仮更新を次の間隔で送信: 10 分

WLAN サバイバビリティ 設定

5.4 AP 設定

システム内の AP をグループ化し、AP グループごとに WLAN の割り当てが可能です。
システムで割り当てできる AP グループは最大 4 グループです。

WebUI の アクセスポイント 画面にて、下図のように AP 表示又はグループ表示 ボタンにて表示の切り替えが可能です。

新たに AP グループを作成する場合には、グループ表示に切り替え、「作成」ボタンをクリックし、3つのステップを経て作成します。

アクセスポイント >

AP 表示

グループ表示



ステップ 1: アクセスポイントの割り当て

AP グループ名を入力し、アクセスポイントの選択を行います。作成したグループに追加する AP を、画面左欄の「System Default」又は既存の AP グループから選択し、矢印ボタンにて「このグループ用に選択されたアクセスポイント」へ移動し、「次へ」をクリックしてください。



ステップ 2: WLAN の割り当て

作成したグループに追加する WLAN を、画面左欄の「利用可能な WLAN」から選択し、矢印ボタンにて「選択されている WLAN」へ移動し、「次へ」をクリックしてください。



ステップ 3: 無線設定

必要に応じて、このグループのアクセス ポイントの無線設定を編集し、「終了」をクリックしてください。

Radio B/G/N(2.4G)	Radio A/N/AC(5G)	Other
無線 B/G/N (2.4GHz) ☒ 1 ☒ 2 ☒ 3 ☒ 4 ☒ 5 ☒ 6 ☒ 7 ☒ 8 ☒ 9 ☒ 10 ☒ 11 ☒ 12 ☒ 13		
チャネル化	自動 ▼	
チャンネル	自動 ▼	
送信電力	Auto ▼	
11n のみのモード	自動 ▼	
コールドミッション制御	Off ▼	
WLAN サービス	Enable ▼	
保護モード	RTS/CTS ▼	

なお、5GHz のチャネル化は最大チャネルを自動設定するため、AP が 5 台以上になるネットワークにおいては、40MHz, 又は 20MHz とすることを推奨いたします。

Radio (2.4G)	Radio (5G)	Other
無線5GHz屋内 ☒ 36 ☒ 40 ☒ 44 ☒ 48 ☒ 52 ☒ 56 ☒ 60 ☒ 64 ☒ 100 ☒ 104 ☒ 108 ☒ 112 ☒ 116 ☒ 120 ☒ 124 ☒ 128 ☒ 132 ☒ 136		
無線5GHz屋外 ☒ 100 ☒ 104 ☒ 108 ☒ 112 ☒ 116 ☒ 120 ☒ 124 ☒ 128 ☒ 132 ☒ 136		
チャネル化	40 ▼	
チャンネル	屋内 Auto ▼	屋外 Auto ▼
送信電力	Auto ▼	
11n/ac のみのモード	Auto ▼	
コールドミッション制御	Off ▼	
WLAN サービス	Enable ▼	

5.5 WLAN のチューニング

5.5.1 Master AP のクライアント接続制限

Master AP に最大クライアント接続数を制限したい場合に設定してください。工場出荷時は、100 台に制限されています。通常は変更する必要はないと思いますが、変更する場合には十分な事前検証を実施してください。

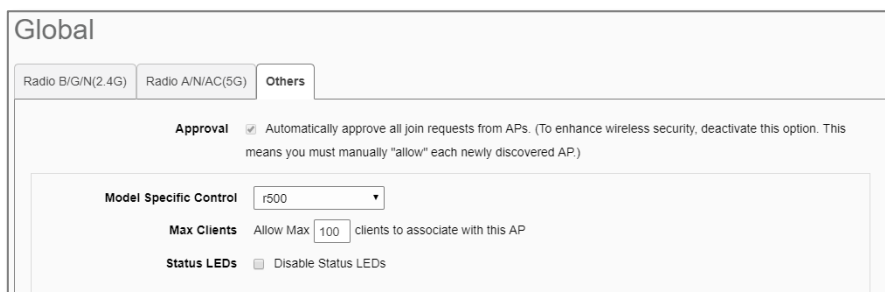
SSH でログインし、CLI で設定します。

```
ruckus# config
You have all rights in this mode.
ruckus(config)# system
ruckus(config-sys)# master-protect
ruckus(config-sys-master-protect)# master-max-sta 50
The master AP protection settings have been updated.
ruckus(config-sys-master-protect)# exit
The master AP protection settings have been updated.
Your changes have been saved.
ruckus(config-sys)# master-protect
ruckus(config-sys-master-protect)# show
Master AP Protection:
  Master max STA= 50
```

5.5.2 Member AP のクライアント接続制限

Member AP にクライアント接続数を AP モデル毎に制限したい場合に設定してください。工場出荷時は 100 台に制限されています。通常は変更する必要はないと思いますが、変更する場合には十分な事前検証を実施してください。

Access Points > Summary > Edit > Global > [Other]



Global

Radio B/G/N(2.4G) Radio A/N/AC(5G) Others

Approval ☒ Automatically approve all join requests from APs. (To enhance wireless security, deactivate this option. This means you must manually "allow" each newly discovered AP.)

Model Specific Control r500

Max Clients Allow Max 100 clients to associate with this AP

Status LEDs ☐ Disable Status LEDs

Max Clients 設定

5.5.3 OFDM Only

昨今では、802.11n や 802.11ac が主流となり、802.11b デバイスは、ほとんど見かけることがありません。しかし AP は 802.11b の後方互換性を確保するため、Beacon を含むマネージメントフレームを CCK の転送レートを用いて送信します。

この低レートのマネージメントフレームは、高密度環境において全体パフォーマンスを下げ、不要にセルが広くなり、スティッキー端末を発生させる要因となる場合があります。OFDM Only を有効とすることで、低レートのマネージメントフレームがなくなり、全体的なパフォーマンスが向上し、また、セルが小さくなることでスティッキー端末への対策となります。ただし、802.11b デバイスの接続ができなくなるのでご注意ください。

CCK/OFDM Rates

CCK Rates (802.11b)		OFDM Rates (802.11g/a/n)	
転送レート (Mbps)	受信感度 (dBm)	転送レート (Mbps)	受信感度 (dBm)
11	-82	54	-68
5.5	-85	48	-68
2	-86	36	-75
1	-89	24	-79
		18	-82
		9	-87
		6	-88

設定は CLI より、WLAN 毎に行うことが可能です。この ofdm-only 設定は 2.4GHz に対する設定で、5GHz への効果はありません。

```
ruckus(config)# wlan unleashed.200.5
The WLAN service 'unleashed.200.5' has been loaded. To save the WLAN service, type 'end' or 'exit'.

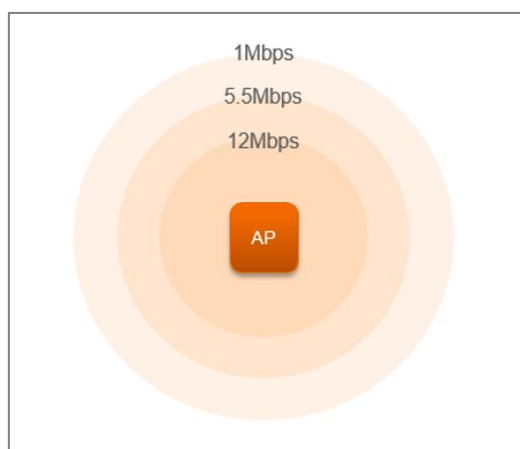
ruckus(config-wlan)# ofdm-only
The mgmt-tx-rate will be set to 6Mbps due to ofdm-only enable.
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

5.5.4 bss-minrate

前項では 2.4GHz 帯における転送レートの改善と、セルサイズの調整について述べましたが、この bss-minrate は 2.4GHz/5GHz 双方に対するもので、Beacon 内の最低サポートレートの調整を行います。

期待できる効果としては、高密度環境などにおける全体のパフォーマンス向上、スティッキー端末の回避策となり、セルサイズは縮小します。

Rate とセルサイズ



設定は CLI より、WLAN 毎に行うことが可能です。2.4GHz 及び 5GHz 同時に設定が反映されます。

```
ruckus(config)# wlan unleashed.200.5
The WLAN service 'unleashed.200.5' has been loaded. To save the WLAN service, type 'end' or 'exit'.
ruckus(config-wlan)# bss-minrate 12
The mgmt-tx-rate will be set to the same value as bss-minrate.
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

5.5.5 パフォーマンス、スティッキー端末の改善設定の例

以下の例は、システム内に 802.11b デバイスは存在しないものとし、一般的なオフィス環境におけるパフォーマンス改善の例で、 ofdm-only と bss-minrate を 12 Mbps としています。

```
ruckus(config)# wlan unleashed.200.5
The WLAN service 'unleashed.200.5' has been loaded. To save the WLAN service, type 'end' or 'exit'.

ruckus(config-wlan)# ofdm-only
The mgmt-tx-rate will be set to 6Mbps due to ofdm-only enable.
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)# bss-minrate 12
The mgmt-tx-rate will be set to the same value as bss-minrate.
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)# exit
The WLAN service 'unleashed.200.5' has been updated and saved.
Your changes have been saved.
ruckus(config)# show wlan
WLAN Service:
  ID:
    1:
      NAME = unleashed.200.5
      Tx. Rate of Management Frame(2.4GHz) = 12.0Mbps
      Tx. Rate of Management Frame(5GHz)  = 12.0Mbps
      Beacon Interval = 100ms
      SSID = unleashed.200.5

---- 途中省略 ----

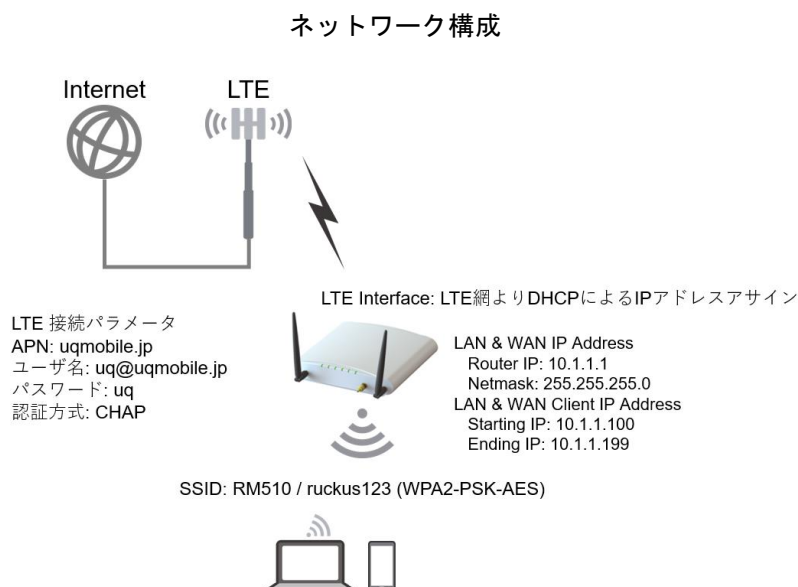
Https Redirection = Disabled
OFDM-Only State = Enabled
Multicast Filter State = Disabled
802.11d State = Disabled
Force DHCP State = Disabled
Force DHCP Timeout = 0
DHCP Option82:
  Status = Disabled
  Option82 sub-Option1 = Disabled
  Option82 sub-Option2 = Disabled
  Option82 sub-Option150 = Disabled
  Option82 sub-Option151 = Disabled
Ignore unauthorized client statistic = Disabled
STA Info Extraction State = Enabled
BSS Minrate = 12.0 Mbps
Call Admission Control State = Disabled
PMK Cache Timeout= 720 minutes
PMK Cache for Reconnect= Enabled
```

6 Unleashed M510 LTE バックホール セットアップ

この章では、LTE バックホールを用いて Wi-Fi インターネットアクセスサービスを提供する M510 Unleashed AP の設定について解説します。

LTE バックホールを介し、帰属デバイスにインターネット接続を提供するには、M510 は Gateway モードとして設定する必要があります。Gateway モードとなることで、自身が DHCP サーバーとなり Wi-Fi デバイスへ IP アドレスをアサインし、ユーザトラフィックを NAT して LTE バックホールへフォワードします。

この章では、以下の構成を元にシステム設定の解説を行います。



M510 Unleashed Firmware: 200.7.10.102.64

なお、LTE SIM サービス提供会社と契約を行った際、**APN、ユーザ名、パスワード、認証タイプ**が提供されるので、**設定前に必ずご確認ください**。なお、このスマートガイドでは、UQ mobile を例に記載いたします。

UQ mobile ネットワーク設定の際に入力する情報

APN	uqmobile.jp
ユーザ名	uq@uqmobile.jp
パスワード	uq
認証タイプ	CHAP

6.1 M510 各部の説明

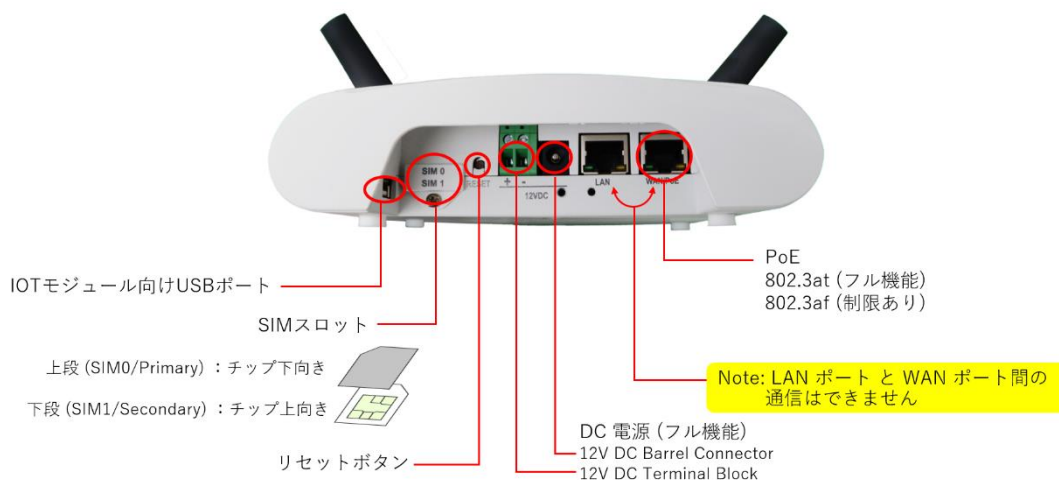
6.1.1 各種アンテナの接続

M510 本体両端にあるアンテナ端子は、3G/4G アンテナ接続用で、同梱の 3G/4G アンテナを取り付けてください。また、GPS アンテナが同梱されていますので、GPS アンテナコネクタに取り付けてご利用ください。



6.1.2 SIM の挿入

M510 の SIM スロットは、Micro SIM タイプです。SIM スロットには、トルクスネジ(T8)で留められたカバーが付いています。SIM 挿入の際は、トルクスネジを緩め、カバーをスライドさせて挿入してください。SIM が浮き出ることがありますので、SIM 挿入後はカバーを戻し、浮き出しを防止して、M510 が正常に SIM を読み込めるようにしてください。



6.1.3 電源供給

M510 は、PoE、又は DC 12V による給電がサポートされています。

PoE による給電では、802.1at、又は 802.af によって動作しますが、802.af では 2.4GHz 及び 5GHz 帯の出力が低下するほか、USB、GPS、LAN ポートの利用ができません。

802.3at 又は DC による電源供給のご利用をお勧めいたします。

6.2 Unleashed M510 セットアップ

6.2.1 設定 PC を Unleashed AP へ接続

以下の手順で、設置 PC を Unleashed AP へ接続します。

- ① 3G/4G アンテナ、GPS アンテナを接続し、SIM カードを SIM0 (primary) へ挿入します。
- ② 工場出荷時の Unleashed AP を、AC アダプタ、又は PoE インジェクタ経由で起動します。
- ③ 暗号化されていない一時的な SSID 「Configure.Me-XXXXXX」 が立ち上がります。
XXXXXX は、AP の背面に記載されている MAC の下 6 桁です。
- ④ 設定用 PC の Wi-Fi 設定にて、「Configure.Me-XXXXXX」を選択して帰属します。

設定用 PC の Wi-Fi 設定 (Windows 10)



- ⑤ 設定用 PC の Wi-Fi 設定にて、「Configure.Me-XXXXXX」を選択して帰属します。
- ⑥ Web ブラウザを起動し、以下の URL を入力します。
unleashed.ruckuswireless.com
- ⑦ セットアップウィザードにリダイレクトされます。

6.2.2 セットアップウィザードの実行

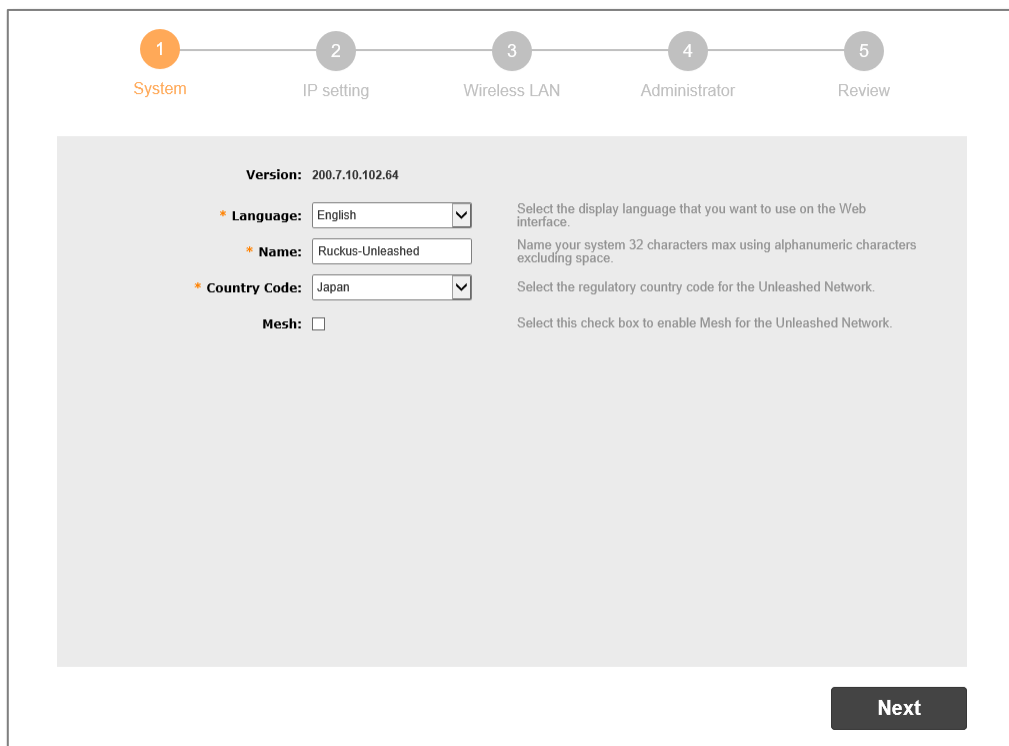
① 初めに「System」設定です。

この例では Language、System Name はデフォルトのままとしますが、必要であれば設定してください。

Country Code は、日本国内で使用する場合には、必ず **Japan** に設定します。他国を選択した場合には電波法違反となる場合がありますのでご注意ください。

「Next」をクリックして次の画面へ進みます。

セットアップウィザード : System



1 System 2 IP setting 3 Wireless LAN 4 Administrator 5 Review

Version: 200.7.10.102.64

* Language: English

* Name: Ruckus-Unleashed

* Country Code: Japan

Mesh: ☐

Select the display language that you want to use on the Web interface.

Name your system 32 characters max using alphanumeric characters excluding space.

Select the regulatory country code for the Unleashed Network.

Select this check box to enable Mesh for the Unleashed Network.

Next

② 「IP Setting」 設定へ移動します。

Gateway Mode にチェックし、AP をゲートウェイモードとします。

WAN Selection の WAN connection 設定では、「Ethernet (primary) with cellular failover」と「Cellular only」の何れかをプルダウンメニューより選択します。

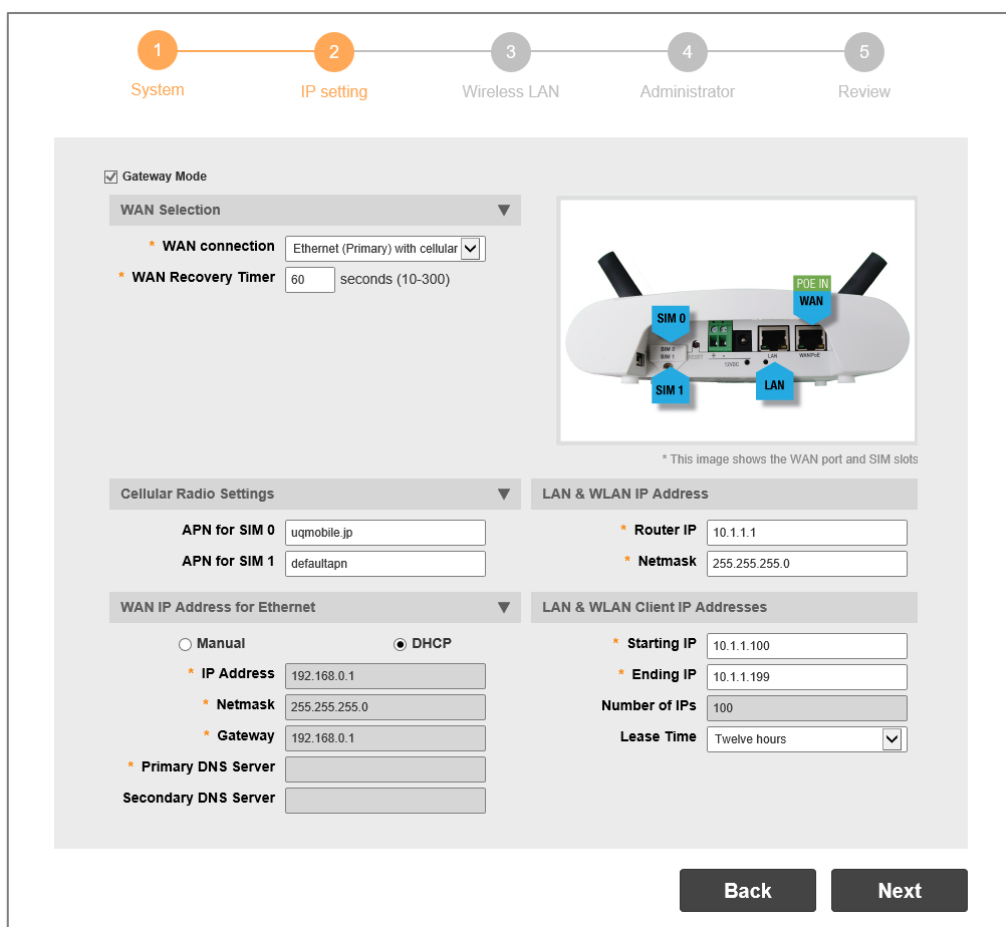
Cellular Radio Settings の APN for SIM X には、SIM スロットに挿入した SIM カードの **APN** を入力します。この例では、SIM Slot 1 に UQ Mobile の SIM カードを挿入しているので、uqmobile.jp と入力しました。

LAN & WAN IP Address には、この AP が NAT ルータとして動作するための IP インターフェイスを入力します。この例では、**Router IP: 10.1.1.1**、**Netmask: 255.255.255.0** を入力します。

LAN & WAN Client IP Address には、この AP が DHCP サーバーとして動作する条件を設定します。この例では、**Starting IP: 10.1.1.100**、**Ending IP: 10.1.1.199** を入力します。

「Next」 をクリックして次の画面へ進みます。

セットアップウィザード : IP setting



1 System 2 IP setting 3 Wireless LAN 4 Administrator 5 Review

☒ Gateway Mode

WAN Selection

* WAN connection Ethernet (Primary) with cellular

* WAN Recovery Timer 60 seconds (10-300)

Cellular Radio Settings

APN for SIM 0 uqmobile.jp

APN for SIM 1 defaultapn

WAN IP Address for Ethernet

☐ Manual ☒ DHCP

* IP Address 192.168.0.1

* Netmask 255.255.255.0

* Gateway 192.168.0.1

* Primary DNS Server

Secondary DNS Server

LAN & WLAN IP Address

* Router IP 10.1.1.1

* Netmask 255.255.255.0

LAN & WLAN Client IP Addresses

* Starting IP 10.1.1.100

* Ending IP 10.1.1.199

Number of IPs 100

Lease Time Twelve hours

Back Next

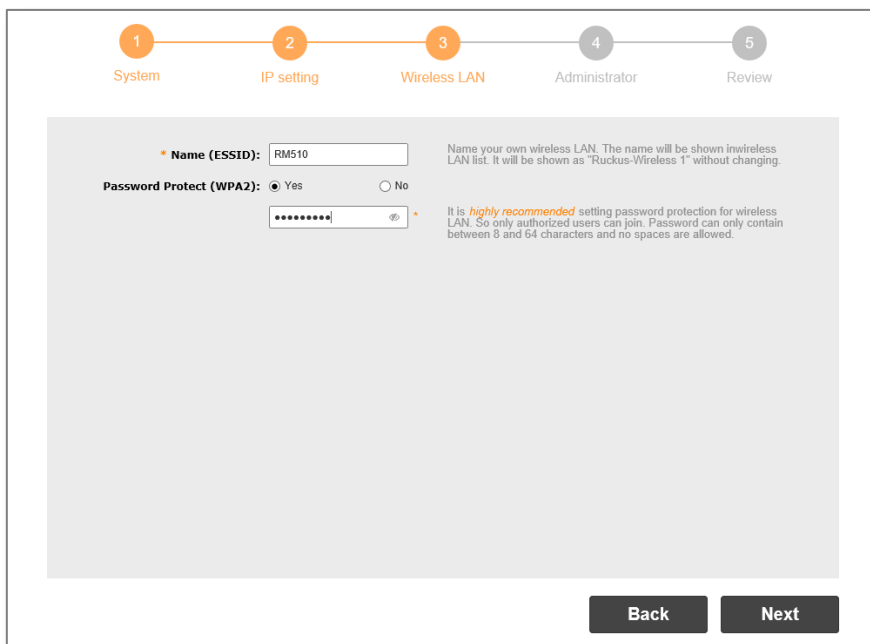
③ 「IP Wireless LAN」へ移動します。

ここでは、WPA2-PSK の WLAN 設定を行います。実際に使用しない場合でも作成する必要があり、不要な場合にはセットアップウィザード終了後に削除してください。

SSID と パスフレーズを設定します。この例では、**Name (ESSID): RM510**、**Password Protect (WPA2) : ruckus123** を入力します。

「Next」をクリックして次の画面へ進みます。

セットアップウィザード : IP Wireless LAN



1 System 2 IP setting 3 Wireless LAN 4 Administrator 5 Review

Name (ESSID): RM510

Name your own wireless LAN. The name will be shown in wireless LAN list. It will be shown as "Ruckus-Wireless 1" without changing.

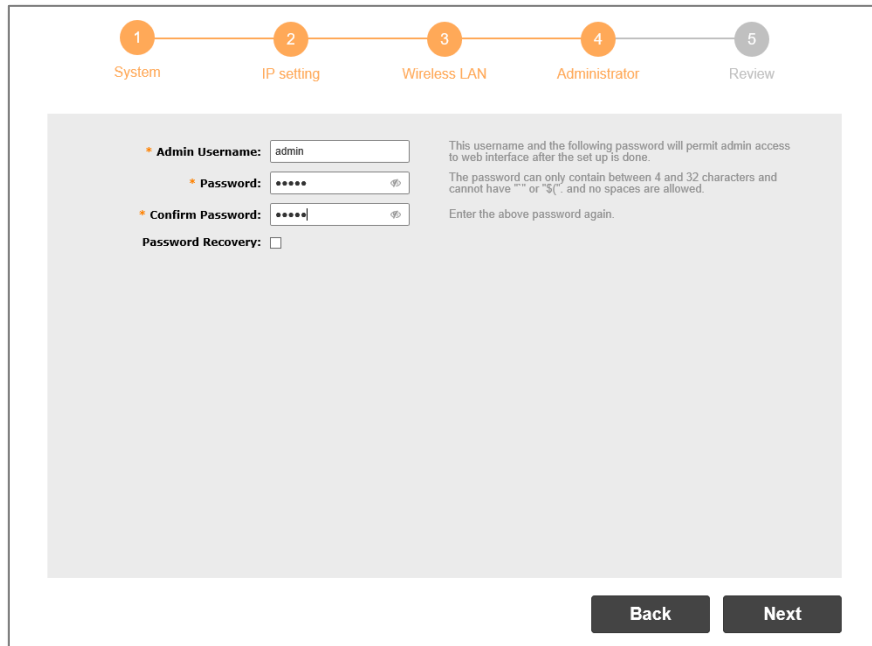
Password Protect (WPA2): ☒ Yes ☐ No

It is *highly recommended* setting password protection for wireless LAN. So only authorized users can join. Password can only contain between 8 and 64 characters and no spaces are allowed.

Back Next

④「Administrator」ではシステムの管理者アカウントとパスワードを設定します。アカウント名とパスワードを入力し、「Next」をクリックして次の画面へ進みます。

セットアップウィザード : Administrator



1 System 2 IP setting 3 Wireless LAN 4 Administrator 5 Review

* Admin Username:

* Password:

* Confirm Password:

Password Recovery: ☐

This username and the following password will permit admin access to web interface after the set up is done.

The password can only contain between 4 and 32 characters and cannot have " " or \$ () and no spaces are allowed.

Enter the above password again.

Back Next

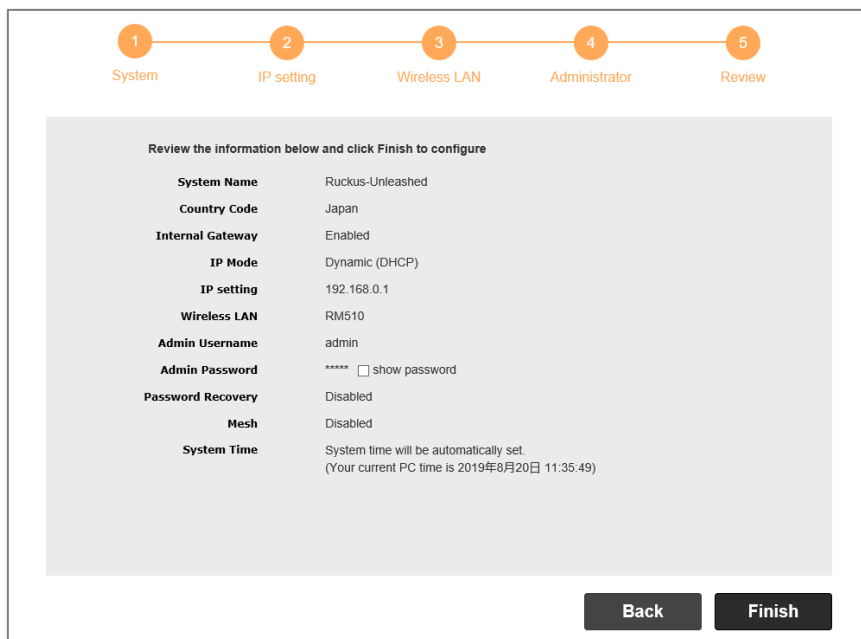
⑤ セットアップウィザードで設定した内容が表示されます。

内容を確認し、「Finish」をクリックするとシステムが再起動されます。

再起動後、セットアップ完了画面が表示されるので、「Finish」をクリックして下さい。

設定が完了したら、ネットワークに接続して動作確認を実施します。

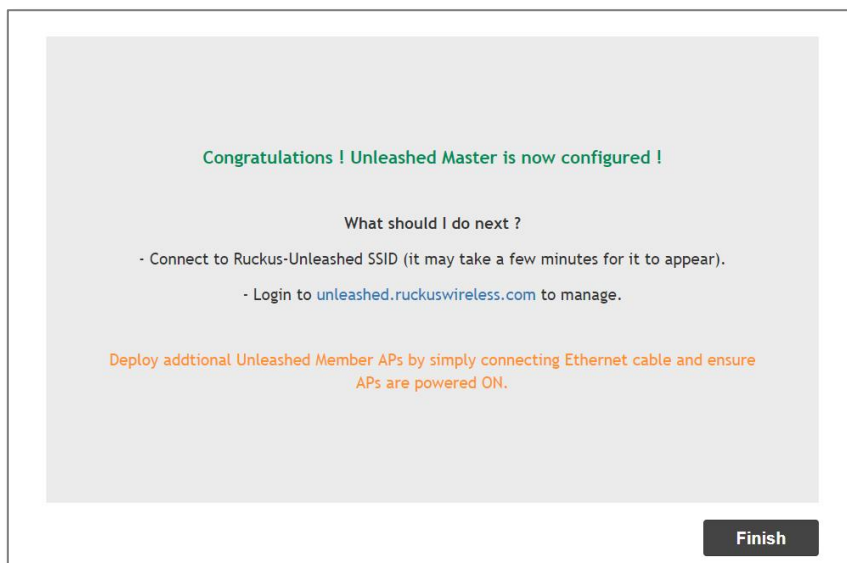
セットアップウィザード : Review



Review the information below and click Finish to configure	
System Name	Ruckus-Unleashed
Country Code	Japan
Internal Gateway	Enabled
IP Mode	Dynamic (DHCP)
IP setting	192.168.0.1
Wireless LAN	RM510
Admin Username	admin
Admin Password	***** ☐ show password
Password Recovery	Disabled
Mesh	Disabled
System Time	System time will be automatically set. (Your current PC time is 2019年0月20日 11:35:49)

Back Finish

セットアップ完了



Congratulations ! Unleashed Master is now configured !

What should I do next ?

- Connect to Ruckus-Unleashed SSID (it may take a few minutes for it to appear).
- Login to unleashed.ruckuswireless.com to manage.

Deploy additional Unleashed Member APs by simply connecting Ethernet cable and ensure APs are powered ON.

Finish

6.3 その他の LTE 設定

Unleashed OS 200.7 の WebUI が提供する LTE 設定は APN 情報のみで、その他の LTE パラメータを設定するには、SSH 経由による CLI から設定することができます。

WLAN または、LAN ポートに接続した設定用 P から SSH 経由でアクセスし、GUI と同じユーザ名、パスワードでログインしてください。

```
Please login: admin
Password : admin # 表示されません
Welcome to Ruckus Unleashed Network Command Line Interface
ruckus> enable
ruckus# ap-mode
You have all rights in this mode.
ruckus(ap-mode)#
```

6.3.1 LTE パラメータ入力

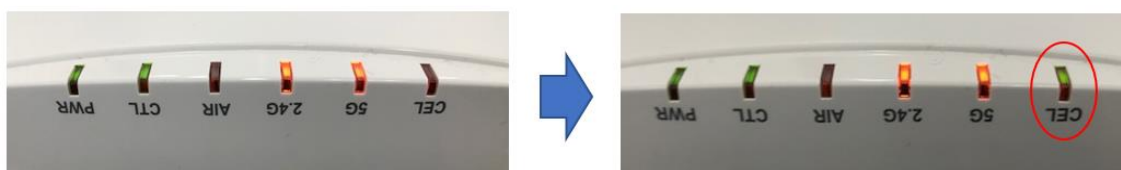
LTE 網へ接続するために必要なパラメータを set コマンドを用いて入力します。
以下は LTE 網へ接続するための主なコマンドです。

- set lte-sim-apn {primary|secondary} {APN name}
primary: SIM0 スロット (上側)
secondary: SIM1 スロット (下側)
※ set lte-sim-apn は、先に説明した WebUI で設定可能です
- set lte-sim-username {primary|secondary} {User name}
- set lte-sim-password [primary|secondary] {password}
- set lte-sim-authentication {primary|secondary} {0|1|2|3}
(0=NONE, 1=PAP, 2=CHAP, 3=PAP/CHAP)

UQ mobile 接続 設定例

```
ruckus (ap-mode) # set lte-sim-apn primary uqmobile.jp
OK
ruckus (ap-mode) # set lte-sim-username primary uq@uqmobile.jp
OK
ruckus (ap-mode) # set lte-sim-password primary uq
OK
ruckus (ap-mode) # set lte-sim-authentication primary 2
OK
```

設定が反映され、LTE 接続が完了すると、以下の様に「CEL」LED の状態が、消灯から緑点灯へ変化します。



設定内容と LTE 接続状態は、以下の get コマンドで確認することができます。

- get lte-statistics

```
ruckus (ap-mode) # get lte-statistics
LTE CHIP                = EC25-J
LTE FW VERSION          = EC25JFAR06A05M4G_01.005.01.005 - SubEdition: V04
TIME OF DAY             = 19/08/20, 05:49:11+36
GPS STATUS              = enabled
IMEI NUMBER             = 865036040453068
SIM SELECTION           = auto
```

[次ページへ続く](#)

SIM 0	= present (active)
SIM 0 MCC	= 440
SIM 0 MNC	= 51
SIM 0 APN	= uqmobile.jp
SIM 0 IMSI	= 440513007509587
SIM 0 ICCID	= 8981300058125095875F
SIM 0 ROAMING	= enabled
SIM 0 USERNAME	= uq@uqmobile.jp
SIM 0 PASSWORD	= uq
SIM 0 AUTHENTICATION	= CHAP
SIM 0 PINCODE	= -
SIM 0 TX	= 30.85 MB
SIM 0 RX	= 6.57 MB
SIM 0 NW REG	= registered, home network
SIM 0 RSSI	= -51 dBm (excellent)
SIM 0 GW	= 10.11.53.217
SIM 0 DNS	= 27.80.249.62 106.187.11.189
SIM 0 IP	= 10.11.53.216
SIM 0 MASK	= 255.255.255.240
SIM 0 OPERATOR	= KDDI KDDI
SIM 0 MODE	= 4G
SIM 0 NW TYPE	= FDD LTE
SIM 0 BAND	= LTE BAND 18
SIM 0 CHANNEL	= 5900
SIM 1	= present (inactive)
SIM 1 MCC	= 440
SIM 1 MNC	= 10
SIM 1 APN	= uqmobile.jp
SIM 1 IMSI	= NA
SIM 1 ICCID	= NA
SIM 1 ROAMING	= enabled
SIM 1 USERNAME	= -
SIM 1 PASSWORD	= -

[次ページへ続く](#)

```
SIM 1 AUTHENTICATION      = NONE
SIM 1 PINCODE             = -
SIM 1 TX                  = 0.00 bytes
SIM 1 RX                  = 0.00 bytes
SIM 0 switch count        = 0
SIM 0 nw lost count       = 0
SIM 0 card removal count  = 0
SIM 0 dhcp timeout count  = 0
SIM 0 transmit            = 30.85 MB
SIM 0 receive             = 6.57 MB
SIM 1 switch count        = 0
SIM 1 nw lost count       = 0
SIM 1 card removal count  = 0
SIM 1 dhcp timeout count  = 0
SIM 1 transmit            = 0.00 bytes
SIM 1 receive             = 0.00 bytes
OK
ruckus (ap-mode) #
```

LTE の接続性が悪くなり、M510 をリブートしても改善しない場合、以下のコマンドにて M510 に搭載されている LTE モジュールのリセットができます。

- set lte-state disable
- set lte-reset

```
ruckus(ap-mode)# set lte-state disable          # リセットを実行する前に LTE モジュールを停止
+ /etc/init.d/nat delete_nat_rules br0
Disabling NAT... wan:br0 lan:
LTE state changed successfully
+ /etc/init.d/nat enable br0
Loading NAT/Firewall modules...
Enabling NAT...exec _add_nat for br0
Chain IPFORWARD_FIREWALL (1 references)
target      prot opt source          destination
Chain IPFORWARD_LIST (0 references)
target      prot opt source          destination
Chain REMOTE_MANAGEMENT_CHAIN2 (1 references)
target      prot opt source          destination
ACCEPT      tcp  --  0.0.0.0/0         0.0.0.0/0         multiport dports 443,80
ACCEPT      all  --  0.0.0.0/0         0.0.0.0/0         state RELATED,ESTABLISHED
ACCEPT      udp  --  0.0.0.0/0         0.0.0.0/0         udp dpt:161
DROP        all  --  0.0.0.0/0         0.0.0.0/0
OK
ruckus(ap-mode)# set lte-reset                  # リセットを実行
Initiating LTE Chip reset., might take ~40s      # 完了まで 40 秒程度要する
LTE Chip reset done, Bringing up LTE interface...
LTE reset succeeded..
OK
ruckus(ap-mode)# get lte-state                  # 終了後 状態確認
-----

LTE Status:
以下省略
```

7 その他

7.1 ファームウェア アップグレード

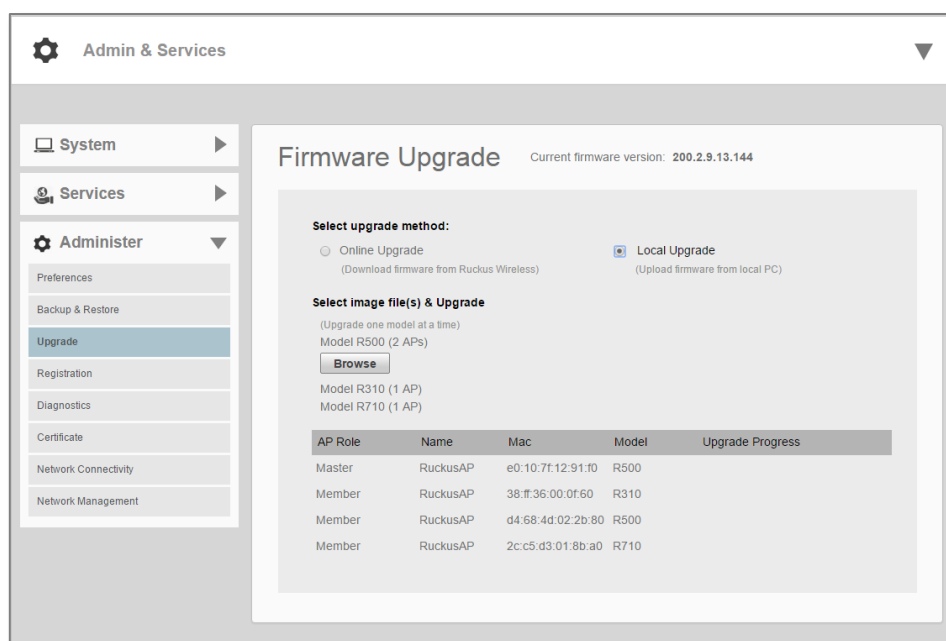
インターネットが接続されている環境では、自動的にアップグレード可能なバージョンをロードできるため、管理者は Online Upgrade を選択し、Upgrade するだけです。

インターネットが接続されていない環境では、Local Upgrade を選択し、作業 PC 内に保存しているファームウェアへアップグレードすることができます。

アップグレードパスは、Release Notes の Upgrade Information をご確認ください。

Admin & Service > Administration > Upgrade

Firmware Upgrade



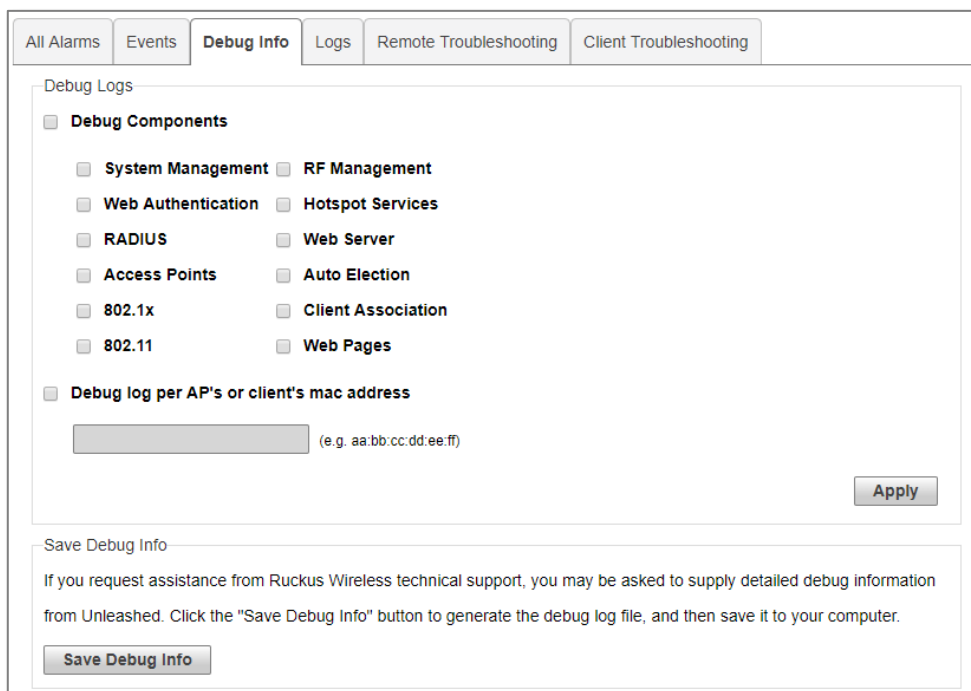
AP Role	Name	Mac	Model	Upgrade Progress
Master	RuckusAP	e0:10:7f:12:91:f0	R500	
Member	RuckusAP	38:f1:36:00:0f:60	R310	
Member	RuckusAP	d4:68:4d:02:2b:80	R500	
Member	RuckusAP	2c:c5:d3:01:8b:a0	R710	

7.2 デバッグ情報の取得

障害対応などで Ruckus Support から依頼があった際に取得をお願いします。デバッグログファイルに含めるデバッグコンポーネントを指定し、必要なデバッグ情報だけを取得、又はデバッグログボックスに AP 又はクライアント MAC アドレスを登録し、その登録された MAC アドレスのデバッグだけを取得することができます。

Admin & Service > Administration > Diagnostics > Debug Info タブ

デバッグ情報の取得



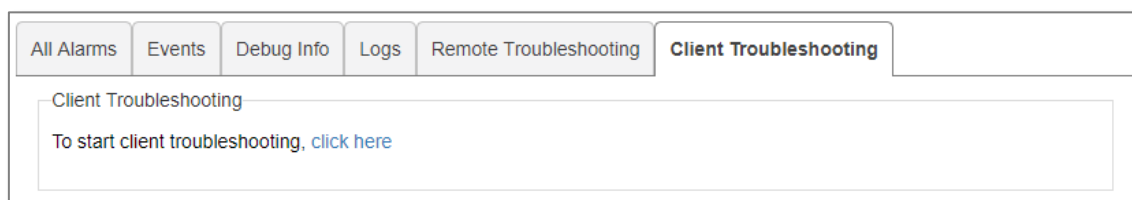
7.3 クライアント・トラブルシューティング ツール

クライアントの接続シーケンスをグラフィカルに表示します。

ツールを利用するには、WebUI より、Client Troubleshooting を起動します、以下の画面より、「click here」をクリックします。

Admin & Service > Administration > Diagnostics > Client Troubleshooting タブ

Client Troubleshooting タブ



ツールが起動したら、接続性を調査するクライアントの MAC アドレスを入力し、「Start」ボタンをクリックし、トレースを開始します。

Troubleshooting

*Client MAC Address:

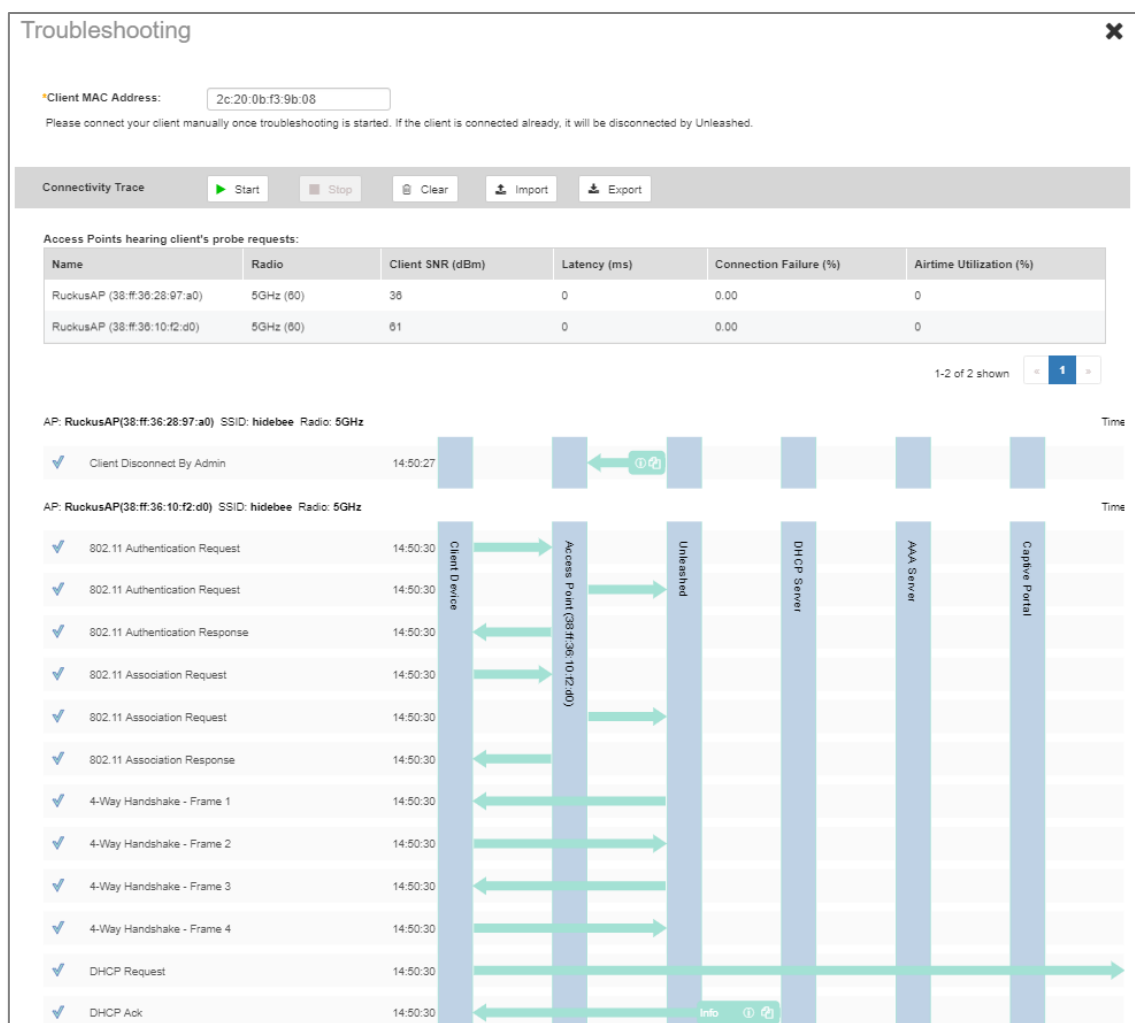
Please connect your client manually once troubleshooting is started. If the client is connected already, it will be disconnected by Unleashed.

Connectivity Trace ▶ Start ■ Stop 🗑 Clear 📄 Import 📄 Export

Access Points hearing client's probe requests:

Name	Radio	Client SNR (dBm)	Latency (ms)	Connection Failure (%)	Airtime Utilization (%)
No data available.					

クライアントが AP に帰属すると、以下の様に接続シーケンスが表示されます。「Stop」ボタンでトレースを停止します。





以上