a Hewlett Packard Enterprise company

Aruba ClearPass 基本設定ガイド v1.0

Hewlett Packard Enterprise

日本ヒューレット・パッカード株式会社
Aruba 事業統括本部

目次

第 1章 はじめに

1.1 本資料について

本資料は Aruba ClearPass の初期セットアップ、基本設定について紹介しています。

1.2 注意事項

本資料は記載の内容は、お使いの製品、バージョンによっては異なる場合がございます。またコマンドの説明など簡略化して記載しておりますので、最新の情報や詳細につきましてはマニュアルをご参照ください。

1.3 本資料で説明している ClearPass バージョン及び機器のバージョン

本資料が対象としている ClearPass のバージョンは 6.8.0.109592 となります。Aruba Mobility Controller 及び Aruba IAP は 8.5.0.2、ArubaOS Switch は 16.09.0003 で確認を行なっています。

1.4 改版履歴

Version	Change history	Author
1.0	1st release	Shingo Namitoko

第 2章 ClearPass 製品構成

2.1 ClearPass の提供形態

ClaerPass はバーチャルアプライアンス、ハードウェアアプライアンスで提供されます。

- バーチャルアプライアンスの種類
  - CLABV : 検証用途のみ
  - C1000 Virtual Appliance : 小規模(1,000 ユーザー以下)
  - C2000 Virtual Appliance : 中規模(10,000 ユーザー以下)
  - C3000 Virtual Appliance : 大規模(50,000 ユーザー以下)
- ハードウェアアプライアンスの種類
  - C1000 Hardware Appliance : 小規模(1,000 ユーザー以下)
  - C2000 Hardware Appliance : 中規模(10,000 ユーザー以下)
  - C3000 Hardware Appliance : 大規模(50,000 ユーザー以下)

2.2 ClearPass のライセンス

2.2.1 Platform ライセンス

ClearPass プラットフォームを有効化するためのライセンスとなり、初回ログオン時にインストールします。各アプライアンス共通のライセンス(1 種類)となっており、ハードウェアアプライアンスには同梱されています。

2.2.2 Access ライセンス

Access ライセンスは下記の機能を有効化するためのライセンスで、100, 500, 1K, 2500, 5K, 10K の 6 種類があります。

- 802.1X 認証
- MAC 認証
- Guest サービスの提供、Guest 認証
- TACACS+
- OnConnect
- Endpoint Profiling
- Security Exchange

同時セッション数(ClearPass によって認証及び認可されたアクティブなクライアント数)に応じてライセンスが消費されます。セッションの情報が利用できない(RADIUS Accounting が利用できない)場合は、認証時にライセンスを消費し 24 時間でクリアされます。

2.2.3 Onboard ライセンス

Onboard ライセンスは証明書を発行したユーザー数(認証時の Username)によって消費され、100, 500, 1K, 2500, 5K, 10K の 6 種類があります。

2.2.4 Onguard ライセンス

Onguard ライセンスは端末数によってライセンスを消費します。複数の NIC を持つ端末は 1 端末としてカウントします。100, 500, 1K, 2500, 5K, 10K の 6 種類があります。

第 3章 ClearPass Virtual Appliance のセットアップ

3.1 動作に必要な仮想環境

ClearPass は下記のハイパーバイザーでの動作をサポートしています。(本資料では ESXi 環境を前提に説明しています)

- VMware vSphere Hypervisor (ESXi) 5.5, 6.0, 6.5, 6.5 U1, 6.5 U2, 6.7
- Microsoft Hyper-V Server 2012 R2, Microsoft Hyper-V Server 2016, Windows Server 2012 R2 with Hyper-V, Windows Server 2016 with Hyper-V
- KVM on CentOS 7.5

3.2 ClearPass Virtual Appliance の動作に必要なリソース

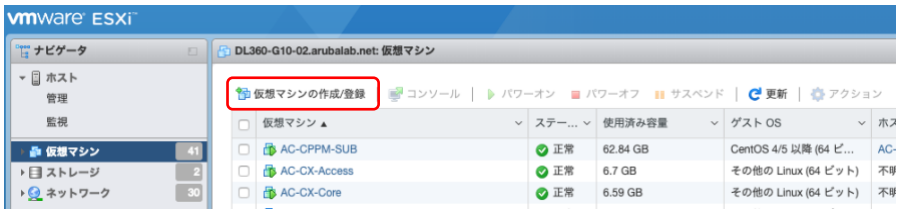
動作に必要なハイパーバイザーのリソースは下記の通りです。

	CLABV(検証用)	C1000	C2000	C3000
CPU	2 Virtual CPU	8 Virtual CPU	8 Virtual CPU	24 Virtual CPU
Memory	6GB	8GB	8GB (16GB Recommended)	64GB
Hard Drive Storage	80GB	1000GB	1000GB	1800GB
Network Interface	2 Gigabit virtual switched ports	2 Gigabit virtual switched ports	2 Gigabit virtual switched ports	2 Gigabit virtual switched ports
Functional IOP rating (40-60 read/write profile for 4K random read/write)	-	75	105	350

3.3 ClearPass Virtual Appliance のデプロイ/初期設定

本手順ではバーチャルアプライアンスを CLABV(検証用)でセットアップを行なっています。C1000, C2000, C3000 でセットアップする場合も手順は同じとなります。

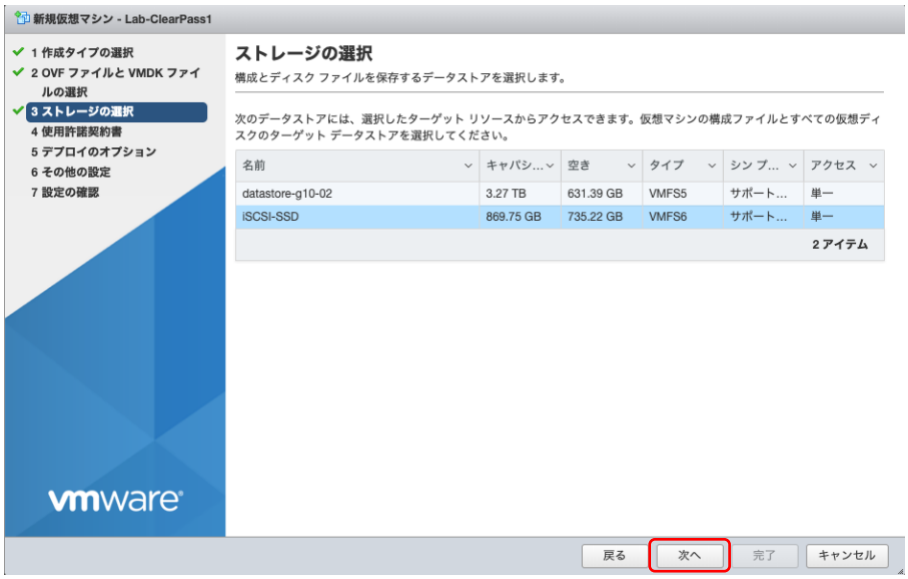
1) ESXi にログインし、「仮想マシン」>「仮想マシンの作成登録」をクリックします。



2) 「OVF ファイルまたは OVA ファイルから仮想マシンをデプロイ」を選択して、「次へ」をクリックします。

3) 任意の仮想マシン名を入力し、入手した ClearPass のファイルをドラッグして、「次へ」をクリックします。

4) ストレージを選択して「次へ」をクリックします。



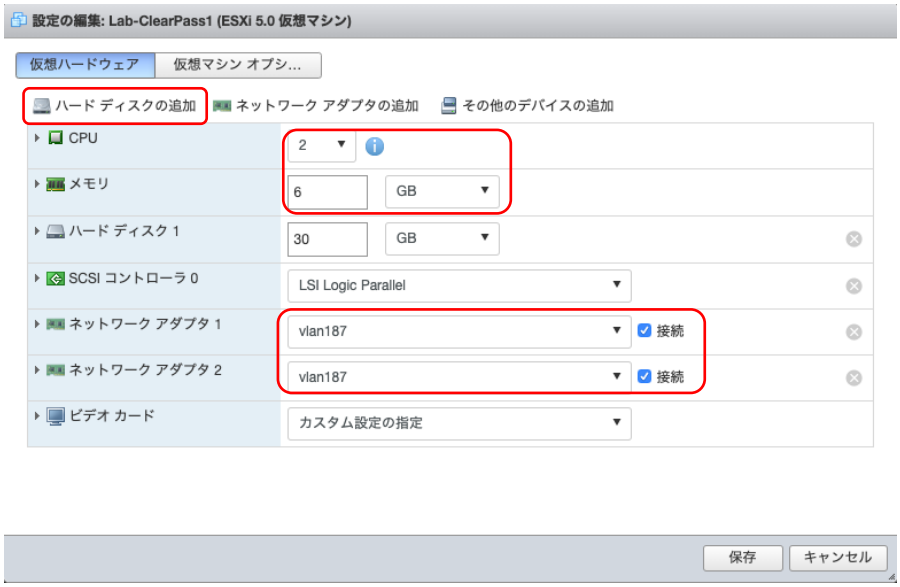
5) ソフトウェアの使用許諾契約書が表示されますので、「同意します」>「次へ」とクリックします。

6) ネットワークのマッピングは導入環境に合わせて設定を行ってください。ディスクプロビジョニングはどちらでも動作は可能ですが、実導入の場合はシックを推奨します。自動的にパワーオンのチェックは外しておき、設定を行なったら「次へ」をクリックします。

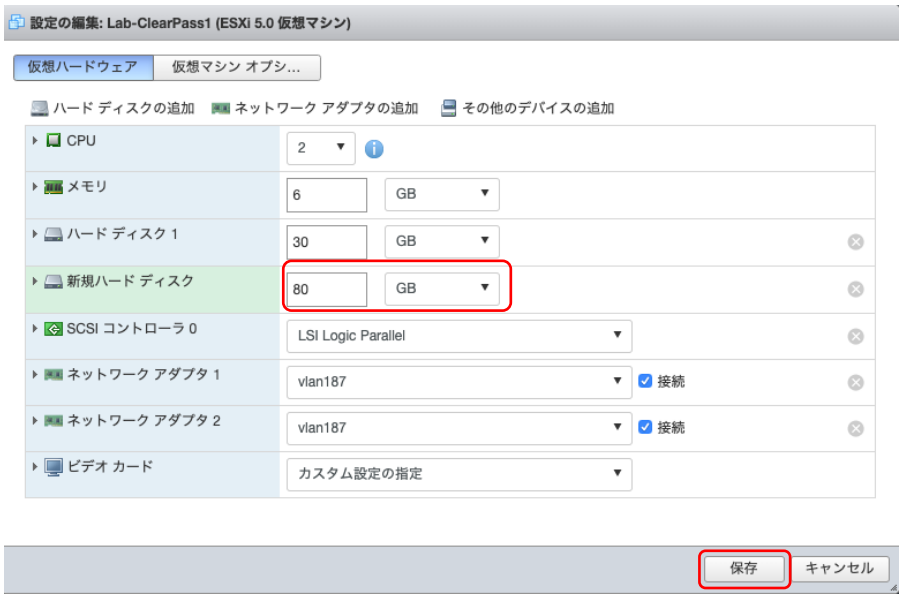
7) 設定の確認を行い「完了」をクリックするとデプロイが開始されますので、完了するまで待ちます。

8) デプロイした仮想マシンを選択し、「編集」をクリックします。

9) 動作させるバーチャルアプライアンスに必要な CPU, メモリを割り当てます。ネットワークアダプタ 1,2 にチェックがついていることを確認します。設定ができたら、「ハードディスクの追加」>「新規ハードディスク」をクリックします。

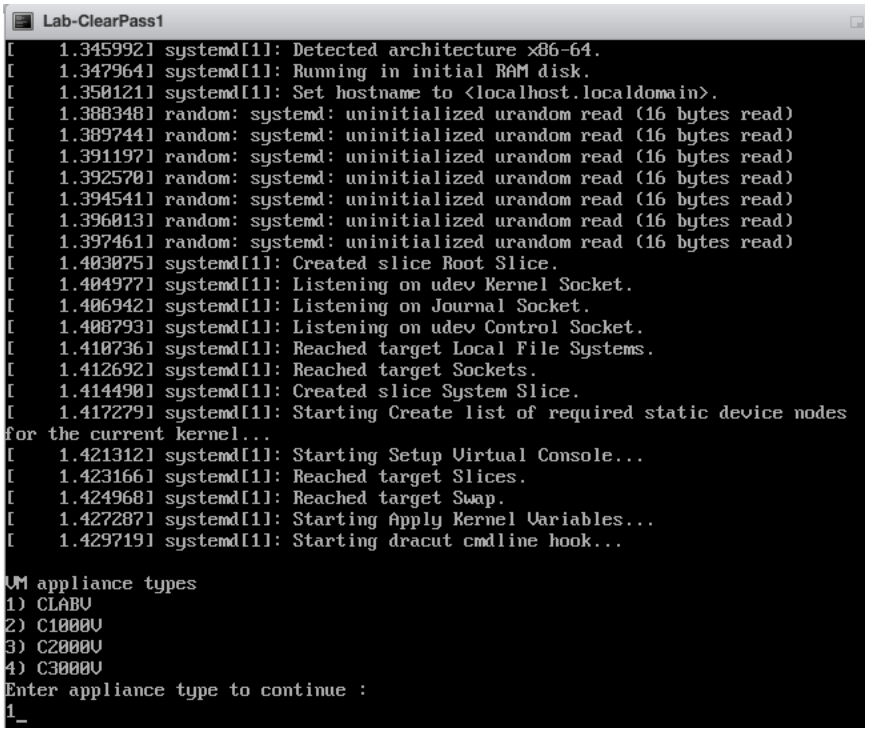


10) 動作させるバーチャルアプライアンスに必要なディスクサイズを設定して「保存」をクリックします。

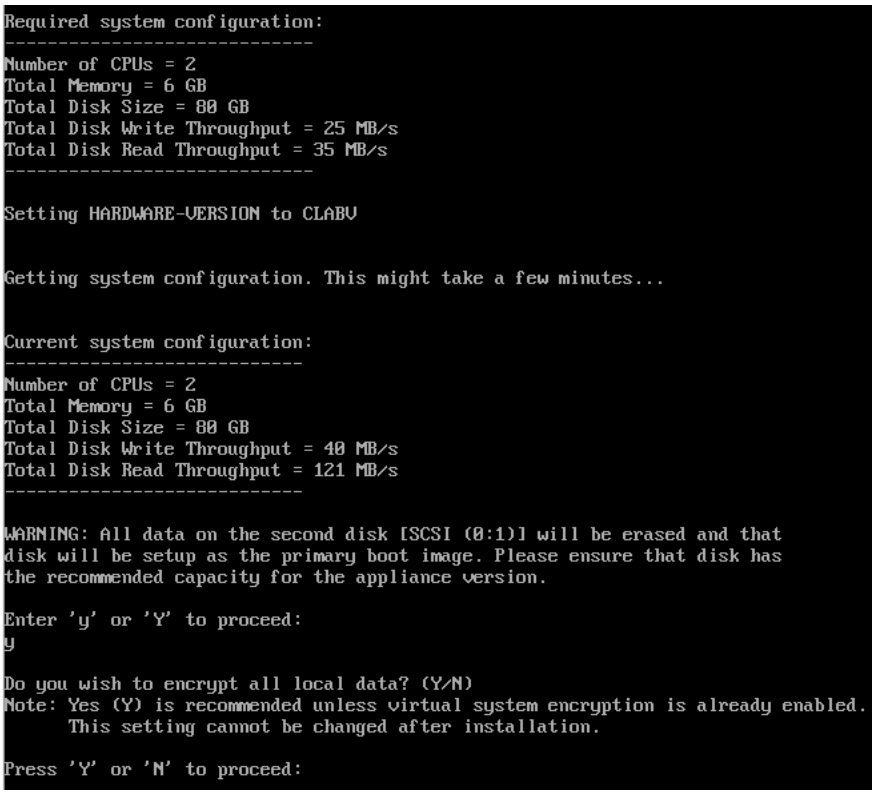


11) 仮想マシンを起動します。

12) 最初にバーチャルアプライアンスの選択となりますので、セットアップするアプライアンスの番号を入力し、Enter キーを押します。



13) 選択したバーチャルアプライアンスで要求されるスペックが表示され、実環境の情報が表示されます。また、セットアップ先のディスクの中身を削除するための確認が表示されますので、”Y”を入力します。その後、ClaerPass のローカルデータの暗号化を行うか確認が表示されますので、”Y”を入力します。

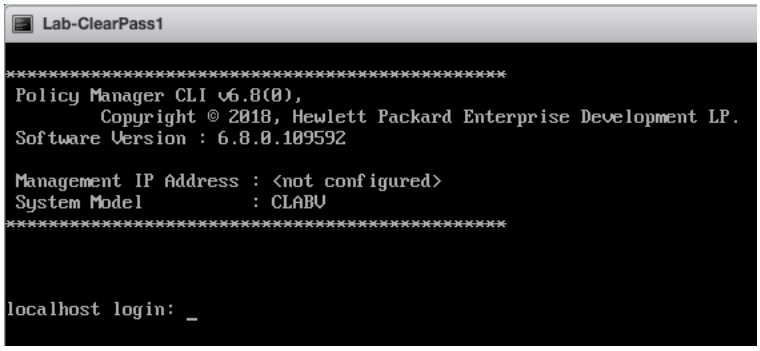


14) しばらくするとログインプロンプトが表示されますので、

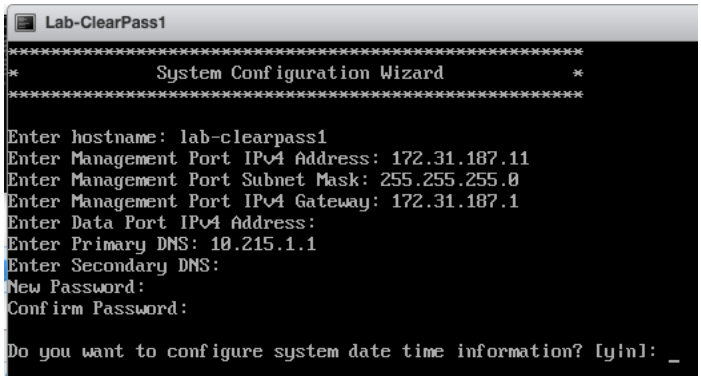
ID : appadmin

Pass : eTIPS123

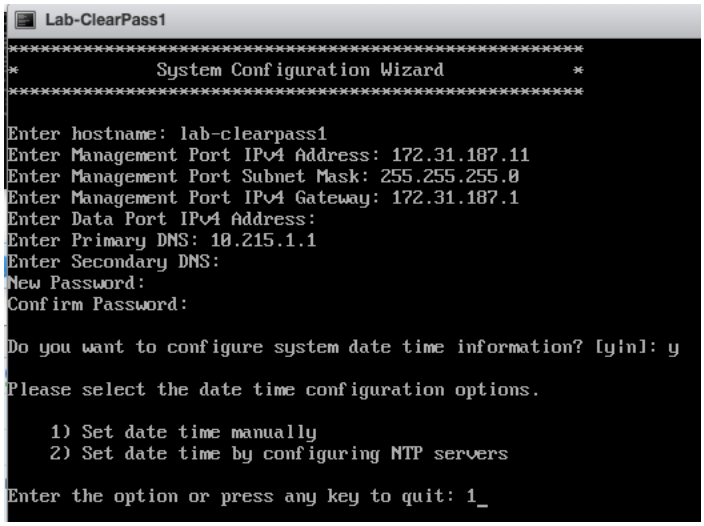
でログインします。



15) ホスト名や IP アドレスなどネットワークの設定を行います。Data Port(認証トラフィックなどの管理用以外のトラフィックを受信するポート)の設定を空欄で Enter キーを押すと、Management Port が Data Port も兼用となります。システム時刻のセットを行うかを聞かれますので、”Y”を入力して Enter キーを押します。



16) インストール完了時の時刻がずれると証明書に影響があるため時計設定を行いますが、NTP の場合再起動後に時刻同期となるため、ここでは Manual で設定を行います。”1”を入力し Enter キーを押します。



17) 指定されたフォーマットで日付、時刻を入力します。設定後、タイムゾーンの指定を行うか聞かれますので、”Y”を入力し Enter キーを押します。”5” (Asia)を入力して Enter キーを押し、”19” (Japan)を入力して Enter キーを押します。

```
Enter the system date in 'yyyy-mm-dd' format: 2019-08-14
Enter the system time in 'HH:MM:SS' format: 11:58:00

Do you want to configure the timezone? [y|n]: y

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa                              7) Australia
2) Americas                            8) Europe
3) Antarctica                          9) Indian Ocean
4) Arctic Ocean                       10) Pacific Ocean
5) Asia                               11) quit
6) Atlantic Ocean
#? 5
Please select a country.
 1) Afghanistan          18) Israel              35) Palestine
 2) Armenia              19) Japan               36) Philippines
 3) Azerbaijan           20) Jordan              37) Qatar
 4) Bahrain              21) Kazakhstan          38) Russia
 5) Bangladesh           22) Korea (North)       39) Saudi Arabia
 6) Bhutan               23) Korea (South)       40) Singapore
 7) Brunei               24) Kuwait              41) Sri Lanka
 8) Cambodia             25) Kyrgyzstan          42) Syria
 9) China                26) Laos                43) Taiwan
10) Cyprus               27) Lebanon             44) Tajikistan
11) East Timor           28) Macau               45) Thailand
12) Georgia              29) Malaysia            46) Turkmenistan
13) Hong Kong            30) Mongolia            47) United Arab Emirates
14) India                31) Myanmar (Burma)     48) Uzbekistan
15) Indonesia            32) Nepal               49) Vietnam
16) Iran                 33) Oman                50) Yemen
17) Iraq                 34) Pakistan
#? 19_
```

18) 設定した情報が合っているか確認されますので、”1”を入力して Enter キーを押します。

```
The following information has been given:

        Japan

Therefore TimeZone='Asia/Tokyo' will be used.
Local time is now:      Wed Aug 14 11:58:37 JST 2019.
Universal Time is now:  Wed Aug 14 02:58:37 UTC 2019.

Is the above information OK?
1) Yes
2) No
#? 1_
```

19) FIPS モードを有効にするか聞かれますが、日本で FIPS モードは関係がないため、”n”を入力し Enter キーを押します。

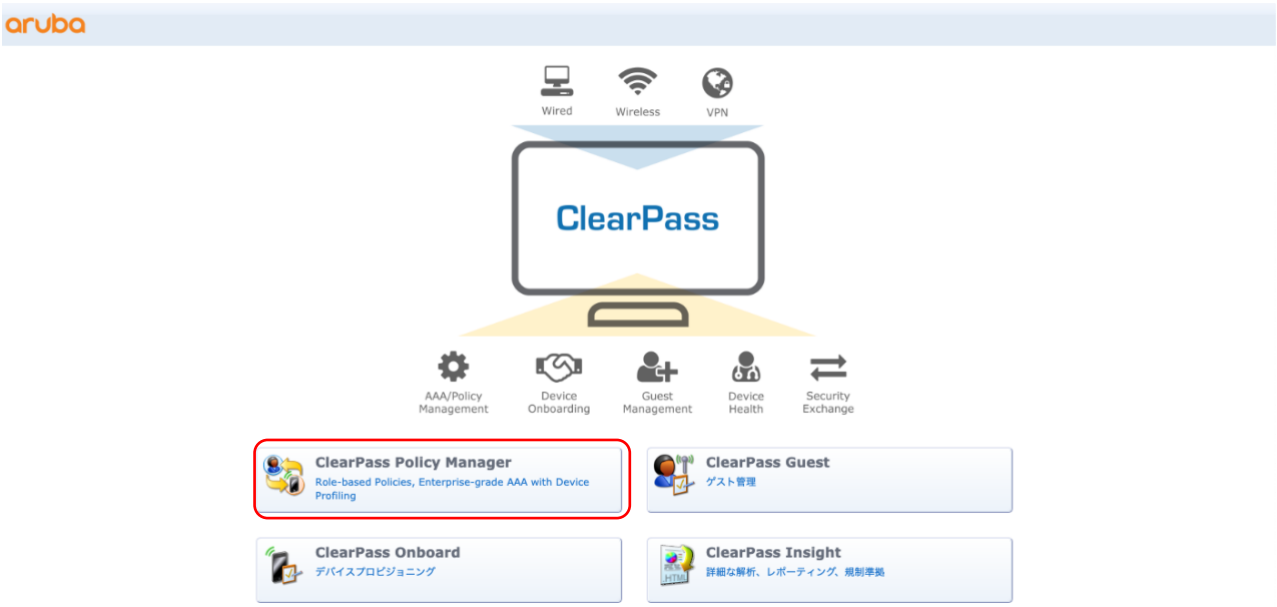
```
Do you want to enable FIPS Mode? [y|n]: n
```

20) 最後に設定の確認が表示されますので、問題なければ”Y”を入力して Enter キーを押します。

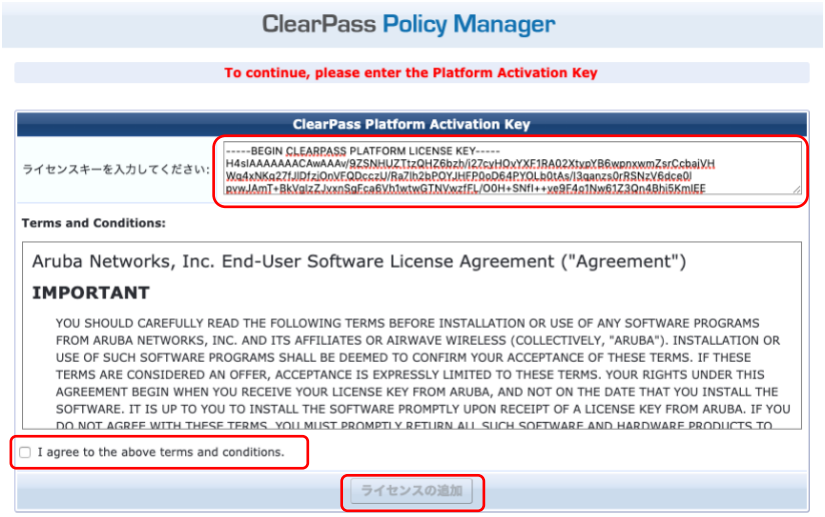
```
================================================
              Configuration Summary
================================================
Hostname                    :  lab-clearpass1
Management Port IP Address  :  172.31.187.11
Management Port Subnet Mask :  255.255.255.0
Management Port Gateway     :  172.31.187.1
Data Port IP Address        :  <not configured>
Data Port Subnet Mask       :  <not configured>
Data Port Gateway           :  <not configured>
Primary DNS                 :  10.215.1.1
Secondary DNS               :  <not configured>
System Date                 :  2019-08-14
System Time                 :  11:58:00
Timezone                    :  'Asia/Tokyo'
FIPS Mode                   :  False

================================================

Proceed with the configuration [y[Y]/n[N]/q[Q]]
                y[Y] to continue
                n[N] to start over again
                q[Q] to quit

Enter the choice: y
```

3.4 Platform License Key のインストール

1) セットアップ時に設定した IP アドレスへブラウザからアクセスすると、ClearPass の Web GUI が表示されますので、「ClearPass Policy Manager」をクリックします。



2) プラットフォームアクティベーションキーの入力を求められますので、ClearPass Platform License Key を貼り付けます。(貼り付ける場合は” -----BEGIN CLEARPASS PLATFORM LICENSE KEY-----”の行から” -----END CLEARPASS PLATFORM LICENSE KEY-----”の行までを選択してください) ”I agree to the above terms and conditions.”にチェックを入れ、「ライセンスの追加」をクリックします。

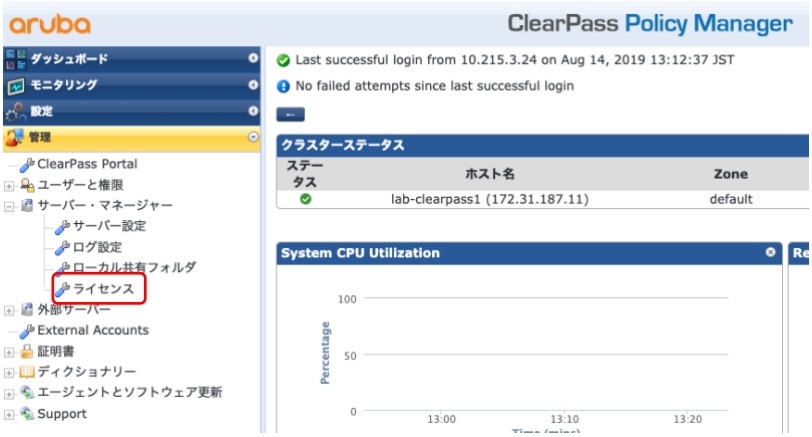


3) ログイン画面が表示されますので、ユーザー名”admin”、パスワードはセットアップ時に設定したパスワードを入力して「ログイン」をクリックするとログインできます。購入したライセンスの場合、アクティベーションが必要ですので、アクティベーションを行う場合は「直ちにアクティベーション」をクリックしてください。(検証目的の場合はアクティベーション不要ですのでスキップしてください)

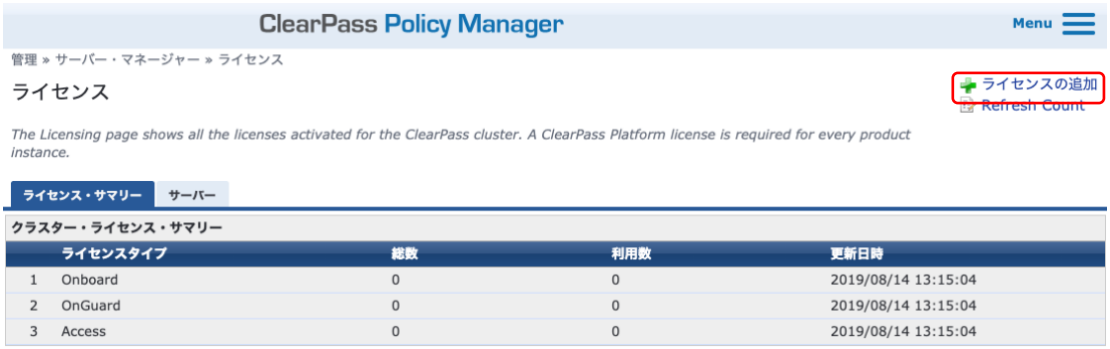
4) アクティベーションを行う場合、ClearPass がインターネットに直接接続されている場合はオンラインアクティベーションが利用可能です。「直ちにアクティベート」をクリックして下さい。ClearPass がインターネットに接続されていない場合は、画面の手順に従ってアクティベーションキーを入手して下さい。

3.5 ライセンスの追加

1) ClearPass Policy Manager へログインし、「管理」>「サーバー・マネージャー」>「ライセンス」を選択します。



2) 「ライセンスの追加」をクリックします。



3) インストールするライセンス製品を選択して、ライセンスキーを貼り付け(” -----BEGIN CLEARPASS PLATFORM LICENSE KEY-----”の行から” -----END CLEARPASS PLATFORM LICENSE KEY-----”の行までを選択してください)、 ”I agree to the above terms and conditions.”にチェックを入れ、「追加 License」をクリックします。インストールするライセンス分、繰り返し行います。

4) ライセンスが追加されていることを確認します。

5) 購入したライセンスの場合はライセンスのアクティベーションを行います。「アプリケーション」タブをクリックし、アクティベーションするライセンスの「Click to Activate」をクリックします。

6) ClearPass がインターネットに直接接続されている場合はオンラインアクティベーションが利用可能です。「直ちにアクティベート」をクリックして下さい。ClearPass がインターネットに接続されていない場合は、画面の手順に従ってアクティベーションキーを入手して下さい。

3.6 ClearPass のオンラインアップデート

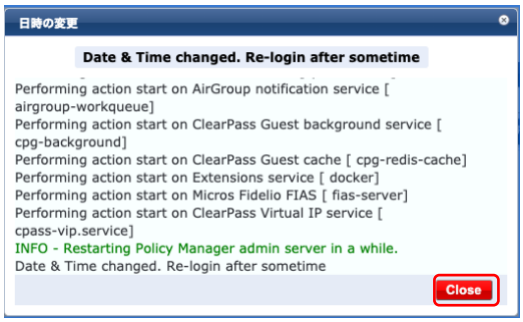
「管理」>「エージェントとソフトウェア更新」とクリックし、ClearPass ソフトウェアを入手する時に利用した HPE Passport アカウントを入力し「保存」をクリックすると、ClearPass がインターネットと通信できる場合、ファームウェア・パッチのダウンロードが可能になります。

3.7 NTP の設定

1) 「管理」>「サーバー・マネージャー」を開き、「日時の設定」をクリックします。

2) 「時刻を NTP サーバーと同期させる」にチェックを入れると、NTP サーバーの設定ができるようになりますので、NTP サーバーの設定を行い「Save」をクリックします。

3) 時刻の同期と ClearPass Policy Manager の再起動が行われ、完了したら「Close」をクリックします。

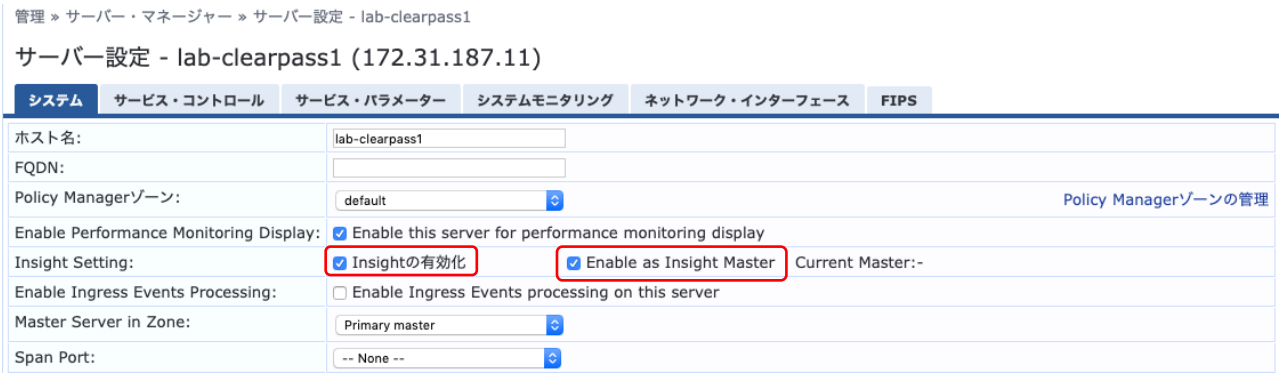


4) 画面をリロードするとログイン画面が表示されるので、再度ログインして画面下の時刻が正しいことを確認します。

3.8 ClearPass Insight の有効化

1) 「管理」>「サーバーマネージャー」>「サーバー設置」を開き、ClearPass サーバーをクリックします。

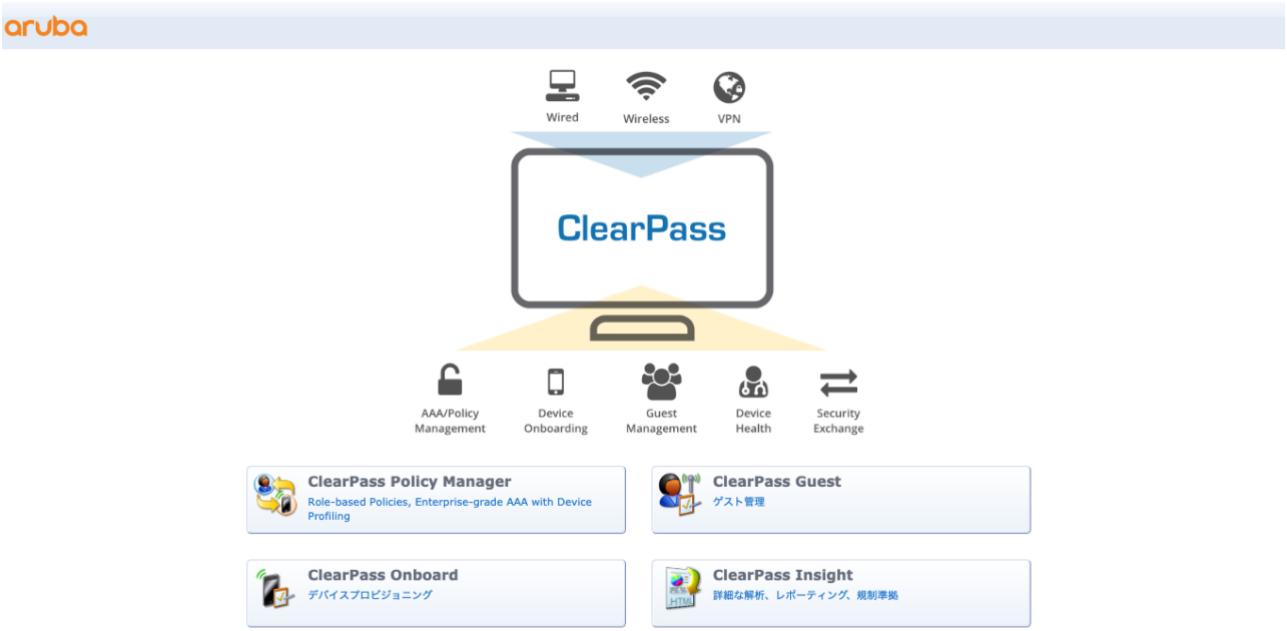
2) 「Insight の有効化」にチェックを入れます。操作している ClearPass が単独で動作、もしくはクラスタ構成の Master として動作している場合は、「Enable as Insight Master」にもチェックを入れ、右下の「保存」をクリックします。



第 4章 ClearPass の基本操作・管理

4.1 ClearPass へのアクセス

ClearPass の IP アドレスへアクセスすると下記のような 4 つのボタンが表示されます。



- ClearPass Policy Manager : 認証の設定、ロールベースのポリシー管理など基本的な設定を行う機能となります。
- ClearPass Guest : ClearPass を使ったゲストアクセス向けの設定を行う機能です。
- ClearPass Onboard : 認証局の設定や、証明書・ネットワーク設定をプッシュで配信する機能です。
- ClearPass Insight : 解析やレポートなどを提供する機能です。

4.2 ClearPass Policy Manager の構成

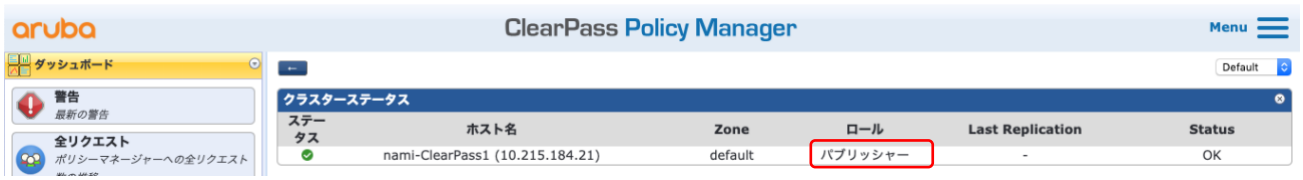
ClearPass Policy Manager にログインすると下記のような画面が表示されます。

4.3 ClearPass のクラスタ構成

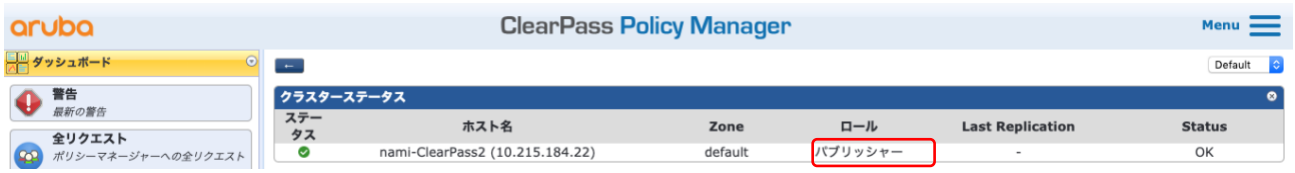
ClearPass はクラスタ構成を組むことで冗長構成にすることができます。本章では 2 台の ClearPass Virtual Appliance でクラスタ構成を組む手順について説明しています。

1) 各 ClearPass へログインし、それぞれがパブリッシャーになっていることを確認します。

a) パブリッシャーになる ClearPass



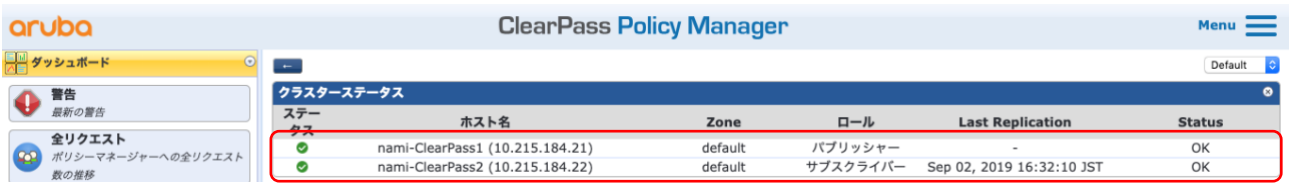
b) サブスクライバーになる ClearPass



2) サブスクライバーにする ClearPass で、「管理」>「サーバー・マネージャー」>「サーバー設定」と開き、「サブスクライバーの作成」をクリック。

3) パブリッシャーIP アドレス(この場合は lab-clearpass1 のアドレス)、パブリッシャー・パスワードを入力して「Save」をクリックします。

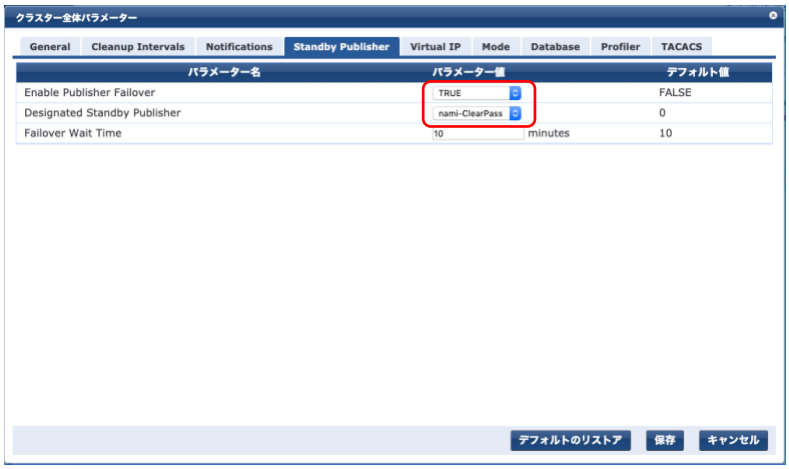
4) しばらく待つとパブリッシャーにサブスクライバーが追加されます。ダッシュボードで下記のようにパブリッシャーとサブスクライバーが一緒に表示され、Status が”OK”になっていることを確認します。



なお、サブスクライバー側はログインページにパブリッシャーへログインする旨のメッセージが表示されます。

5) 「管理」「サーバー・マネージャー」「サーバー設定」と開き、「クラスター全体パラメーター」をクリックします。

6) 「Standby Publisher」タブをクリックし、Enable Publisher Failover を”TRUE”にして、Designated Standby Publisher としてサブスクライバーのサーバーを選択し、「保存」をクリックします。



7) サブスクライバーで Insight を有効にしていなければ有効にします。「管理」「サーバー・マネージャー」「サーバー設定」と開き、サブスクライバーのサーバーをクリックします。

8) Insight の有効化にチェックを入れ、「保存」をクリックします。

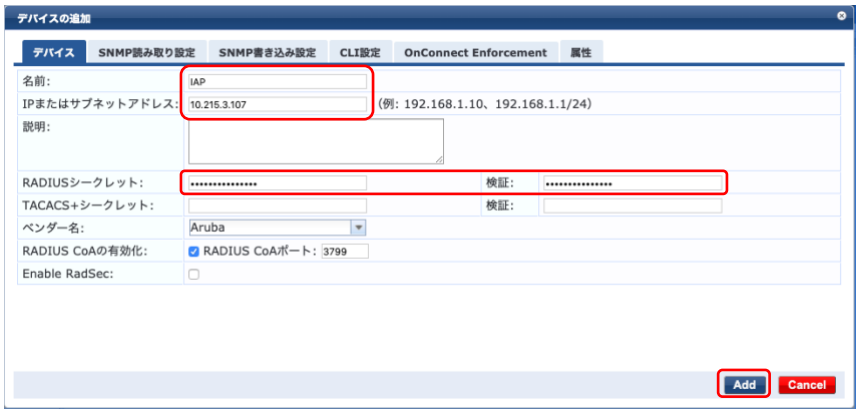
第 5章 基本的なネットワーク認証の設定

5.1 RADIUS クライアントの登録

1) 「設定」>「ネットワーク」>「デバイス」を開き、「デバイスの追加」をクリックします。

2) 任意の名前、デバイスの IP アドレス、RADIUS シークレットキーを設定して「Add」をクリックします。

- Aruba 無線 LAN コントローラー及び IAP の場合
  ※IAP では Dynamic RADIUS Proxy を有効にしていれば VC の IP アドレスを登録、無効(デフォルト)の場合は全ての AP の IP アドレスを登録して下さい。



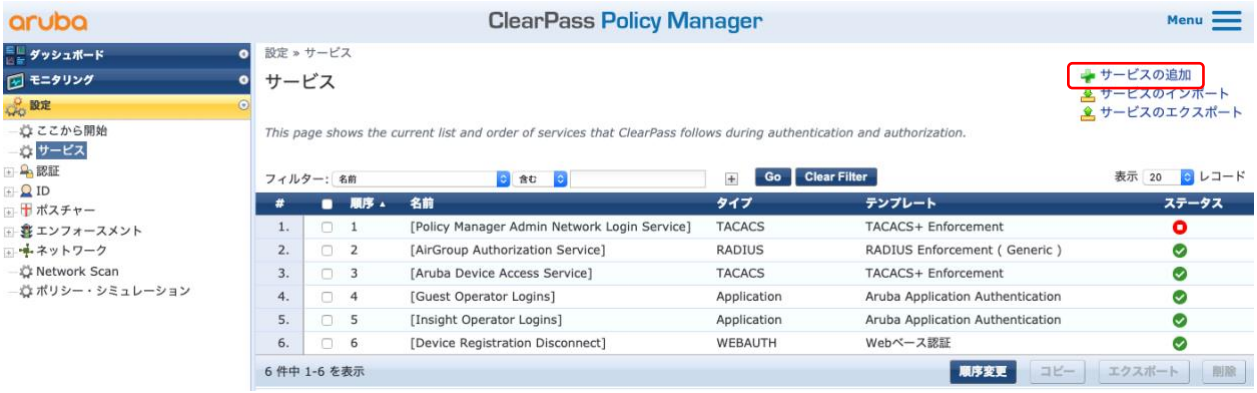
- ArubaOS スイッチの場合
  ※ArubaOS スイッチの場合ベンダー名を「Hewlett-Packard-Enterprise」にします。

5.2 無線 LAN&有線 LAN の MAC 認証

本セクションでは無線 LAN 及び有線 LAN での ClearPass を認証サーバーとした MAC 認証の設定について設定例を説明しています。無線 LAN については PSK + MAC 認証の例としています。

5.2.1 ClearPass のサービス設定

1) 「設定」>「サービス」を開き、「サービスの追加」をクリックします。



2) サービスのタイプで「MAC 認証のバイパス」を選択し、任意の名前を入力して右下の「Next」 をクリックします。

3) 認証ソースにて「Select to Add」をクリックし、「Local User Repository」をクリックして追加し、右下の「Next」をクリック

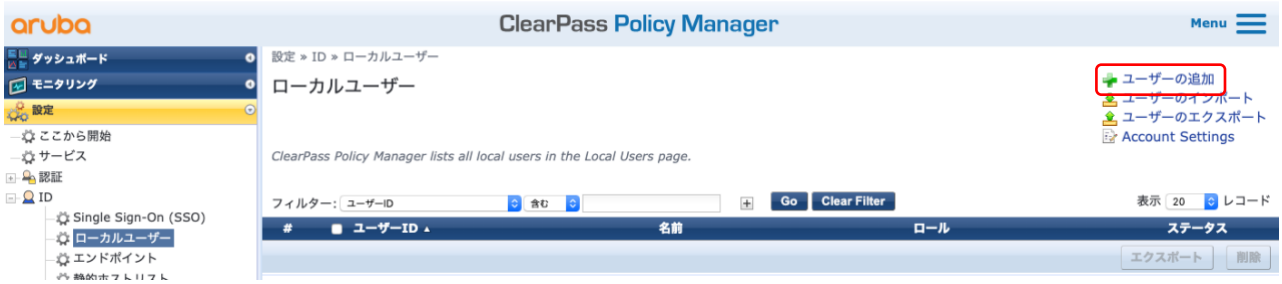
4) ロールマッピングポリシーは特に選択せず、そのまま右下の「Next」をクリックします。

5) エンフォースメントポリシーはデフォルトの「Sample Allow Access Policy」が選択されていることを確認して右下の「Next」をクリックします。

6) 設定した内容のサマリーが表示されるので確認して右下の「保存」をクリックします。

5.2.2 ClearPass へ MAC アドレス追加設定

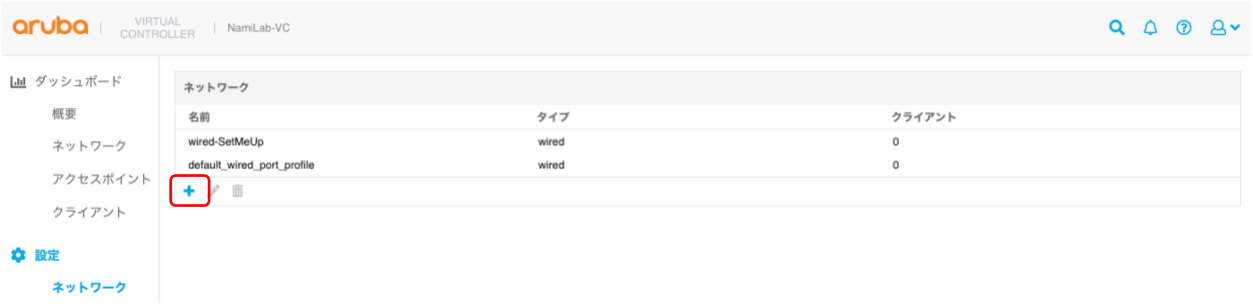
1) 「設定」>「ID」>「ローカルユーザー」と開き、「ユーザーの追加」をクリックします。



2) ユーザーID とパスワードに MAC アドレス、名前は任意の名前を入力し、ロールは[Employee]を選択して「追加」をクリックします。(MAC アドレスの記述方法はネットワーク機器側に依存します。Aruba 無線機器、スイッチ製品のデフォルトは区切り文字なし英数字小文字となります)

5.2.3 Aruba IAP の設定

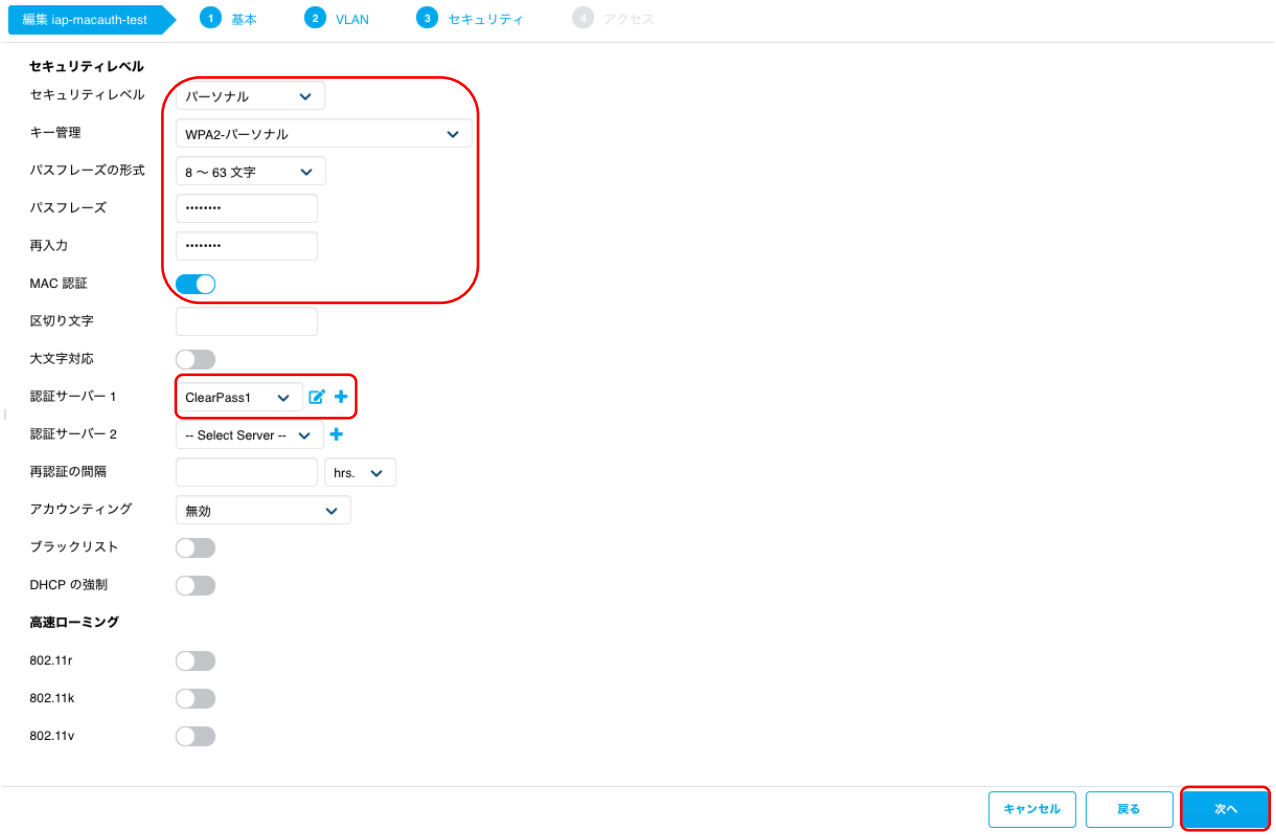
1) 「設定」>「ネットワーク」を開き、「+」をクリックします。



2) 名前を入力し「次へ」をクリックします。

3) クライアント IP と VLAN の割り当てはデフォルトのまま、「次へ」をクリックします。

4) ここでは PSK+MAC 認証の設定を行います。セキュリティレベルを「パーソナル」にしてパスフレーズの設定を行い、「MAC 認証」をオンにすると認証サーバーの項目が表示されますので、「+」をクリックして、RADIUS サーバーとして ClearPass を登録して、認証サーバー1 で選択を行い「次へ」をクリックします。



認証サーバー追加の設定を行います。任意の名前、IP アドレス、ClearPass 側と同じシークレットキーの設定を行い、「OK」をクリックします。

5) アクセスルールはデフォルトのまま「終了」をクリックします。

5.2.4 Aruba IAP での MAC 認証動作確認

1) クライアントを SSID に接続します。

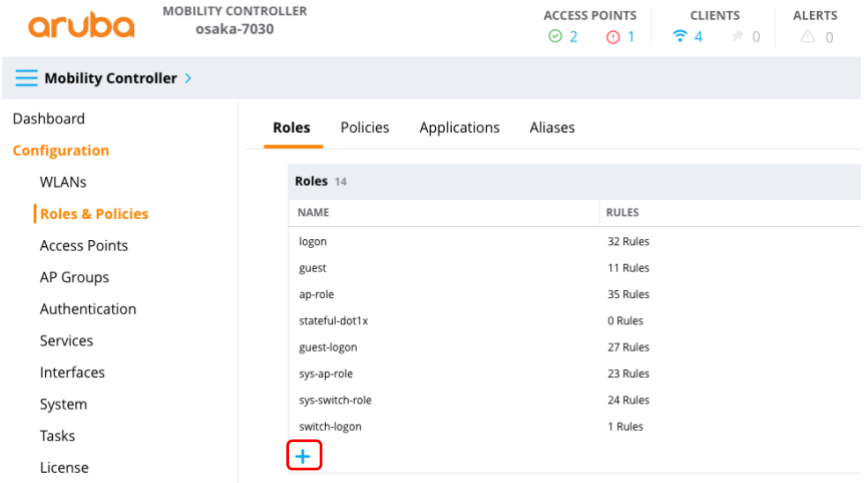
2) 接続ができたら ClearPass の「モニタリング」>「Live Monitoring」>「アクセス・トラッカー」を開くと、IAP からの認証履歴が表示されていますので、クリックすると詳細を確認することができます。

3) IAP の「ダッシュボード」>「クライアント」でも接続されていることが確認できます。

5.2.5 Aruba Mobility Controller の設定

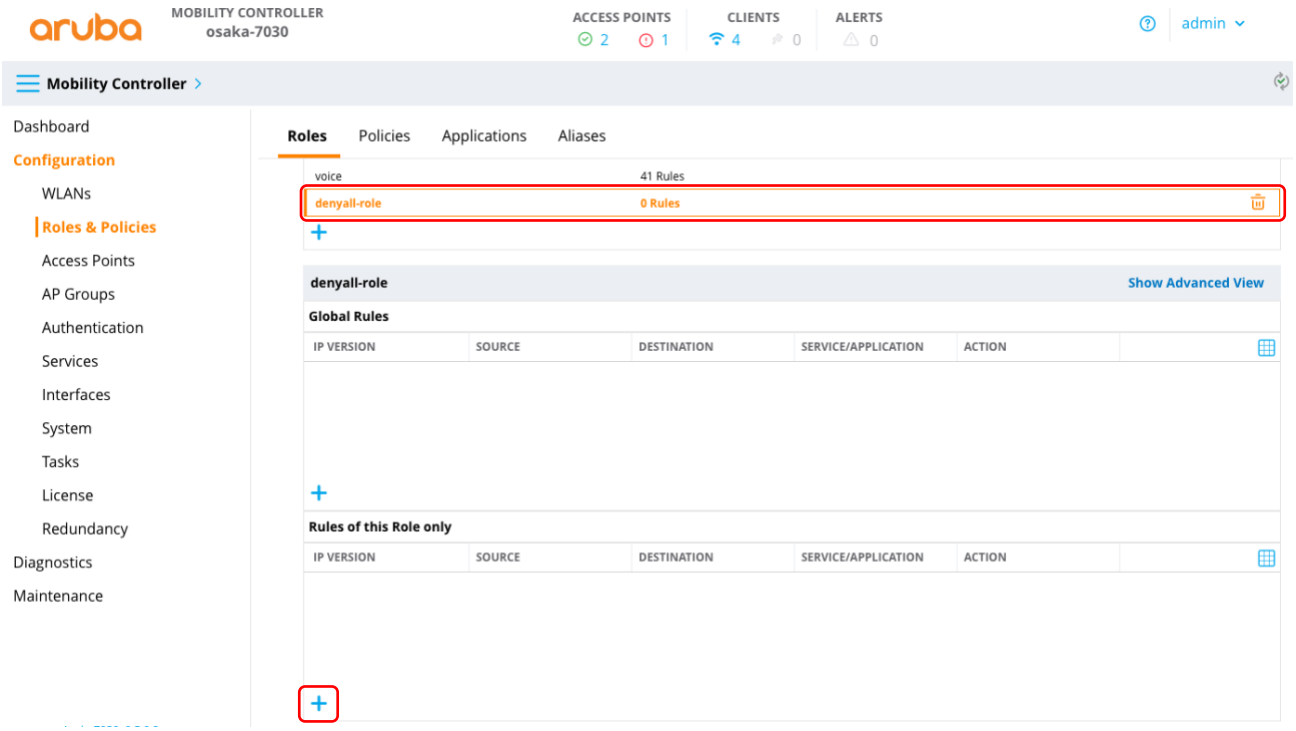
※本説明は AOS8 Standalone MC で行なっております。

1) まず、MAC 認証失敗時にどこにも通信ができない Role を作成します。「Mobility Controller」>「Configuration」>「Roles & Policies」と開き、Roles タブの「+」をクリックします。

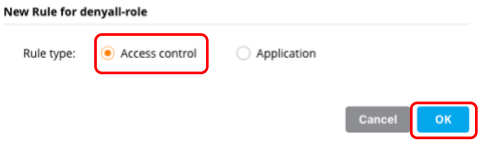


2) Name に任意のロール名(ここでは denyall-role)を入力して「Submit」をクリックします。クリックしたら右上の「Pending Changes」>「Deploy Changes」とクリックして設定を反映します。

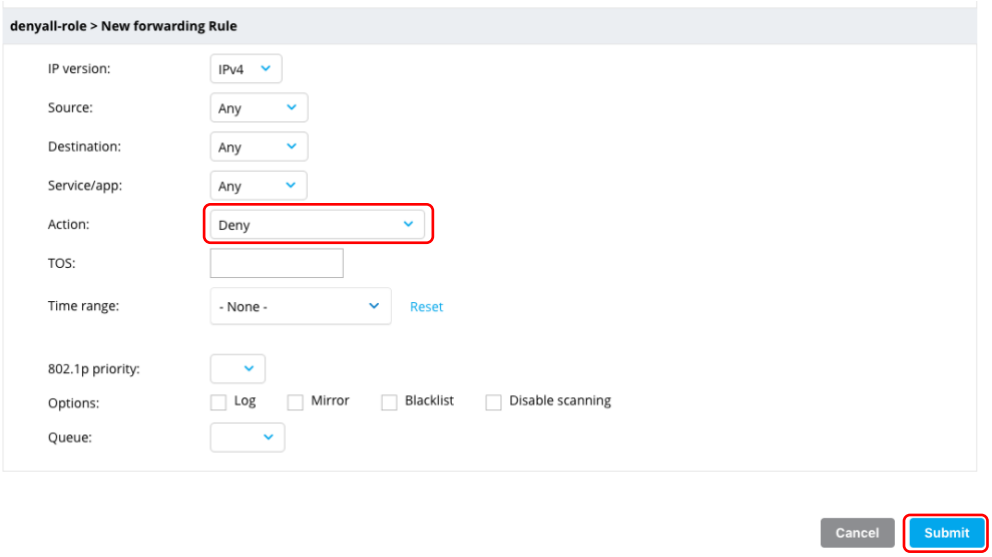
3) Roles の一覧に作成したロールが表示されているので選択し、Roles of this Role only の「+」をクリックします。



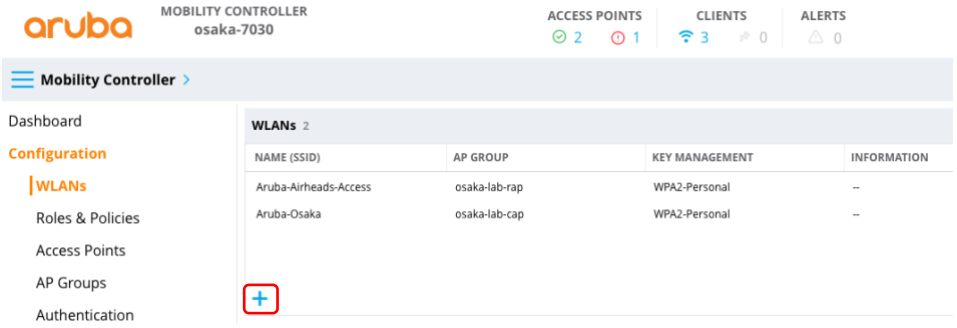
4) Rule type で「Access control」が選択されていることを確認して「OK」をクリックします。



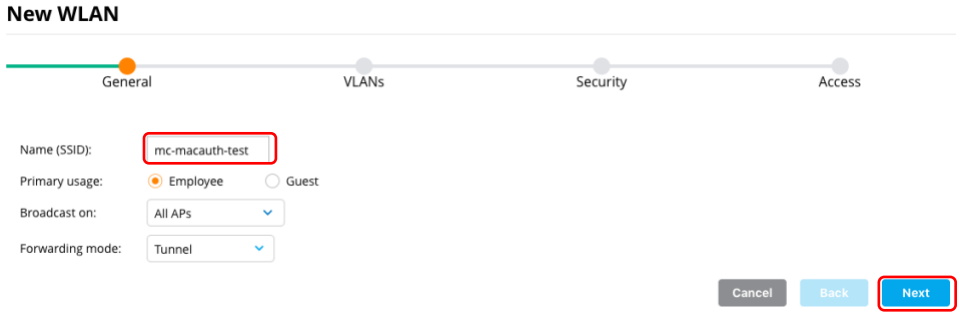
5) ルールの設定となりますので、Action を「Deny」に設定して「Submit」をクリックします。クリックしたら右上の「Pending Changes」>「Deploy Changes」とクリックして設定を反映します。



6) 次に SSID の作成を行います。「Mobility Controller」>「Configuration」>「WLANs」と開き、「+」をクリックします。

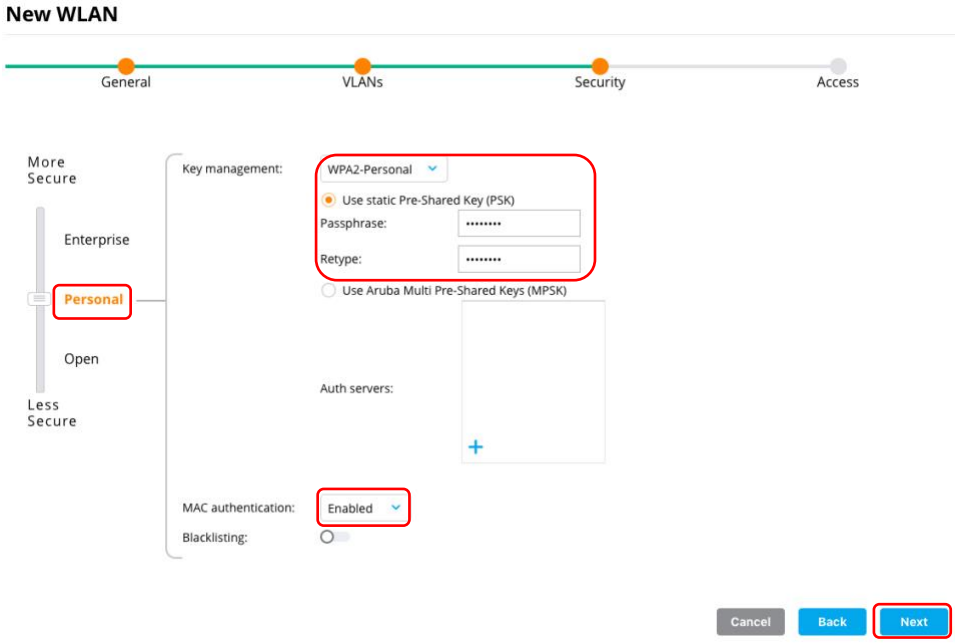


7) SSID の名前を入力して、「Next」をクリックします。

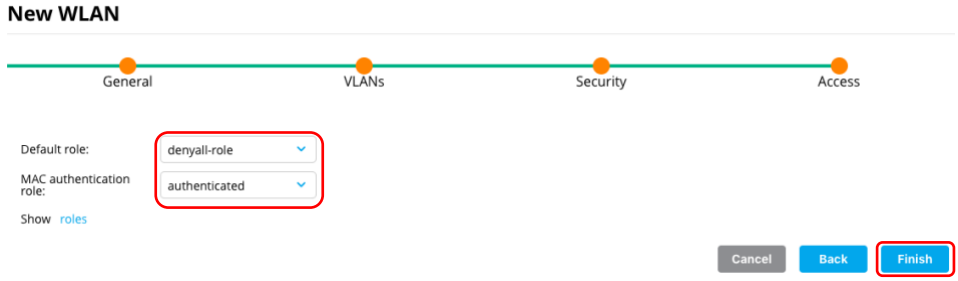


8) VLAN は特に指定がなければそのまま「Next」をクリックします。

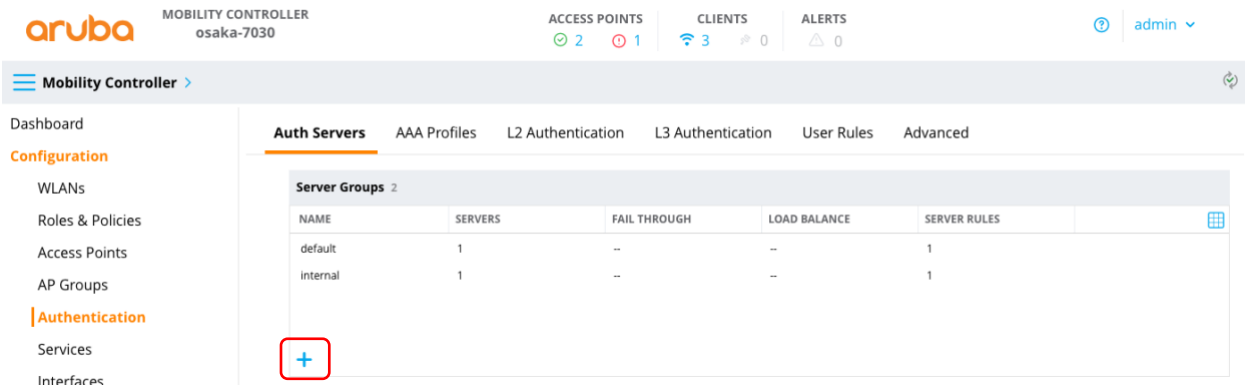
9) ここでは PSK+MAC 認証の設定を行います。左の選択肢より「Personal」を選択し、Key management を「WPA2-Personal」に設定して、PSK の Passphrase を設定します。MAC authentication を「Enabled」にして、「Next」をクリックします。



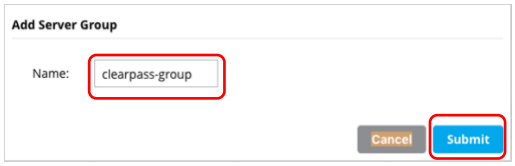
10) Default role を「denyall-role」、MAC authentication role を「authenticated」にして「Finish」をクリックします。クリックしたら右上の「Pending Changes」>「Deploy Changes」とクリックして設定を反映します。



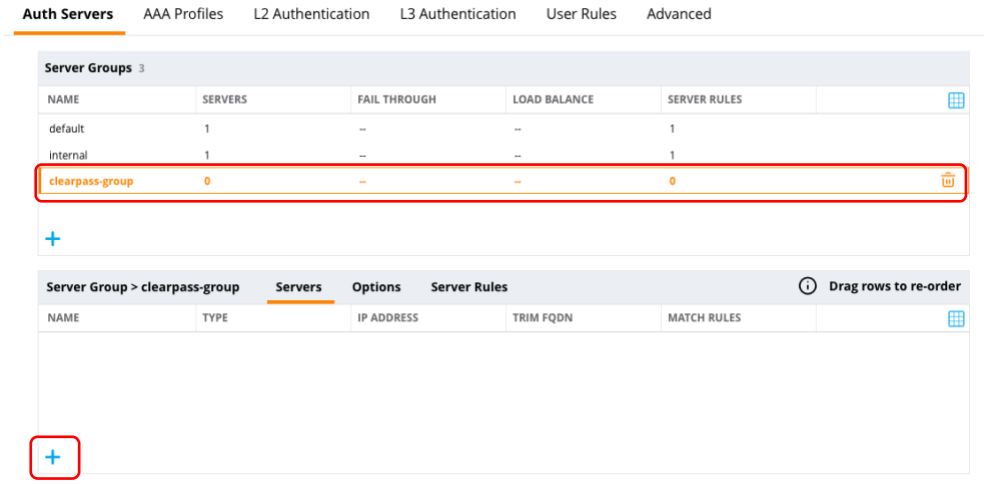
11) SSID 作成の手順において MAC 認証を有効にしましたが、外部 RADIUS サーバーの指定がなかったため、ClearPass を RADIUS サーバーとして追加して、MAC 認証用として指定します。「Mobility Controller」>「Configuration」>「Authentication」と開き、Auth Servers の Server Groups にある「+」をクリックします。



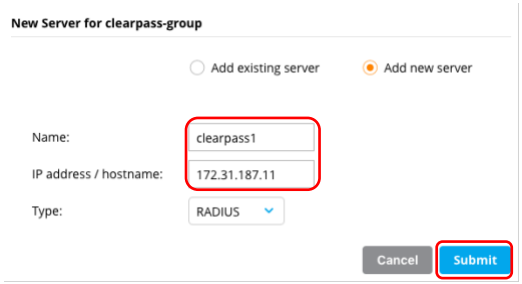
12) 任意の名前を入れて「Submit」をクリックします。クリックしたら右上の「Pending Changes」>「Deploy Changes」とクリックして設定を反映します。



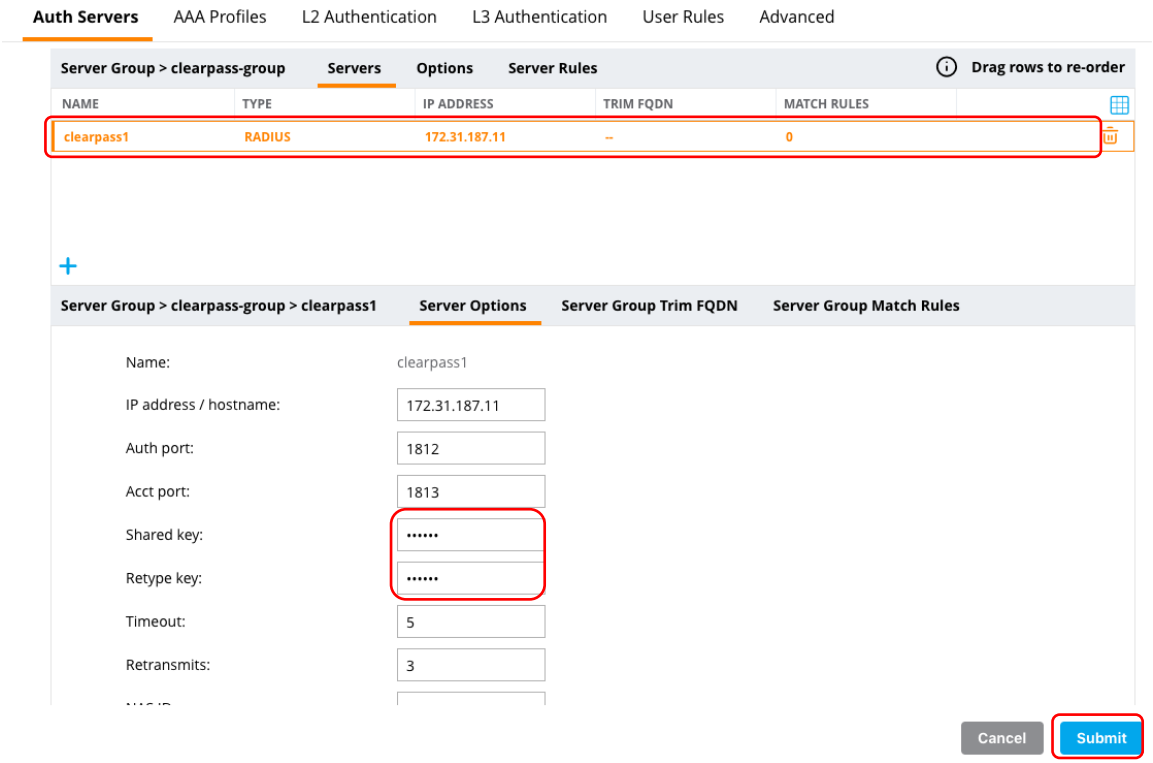
13) グループをクリックして、下段の Servers の「+」をクリックします。



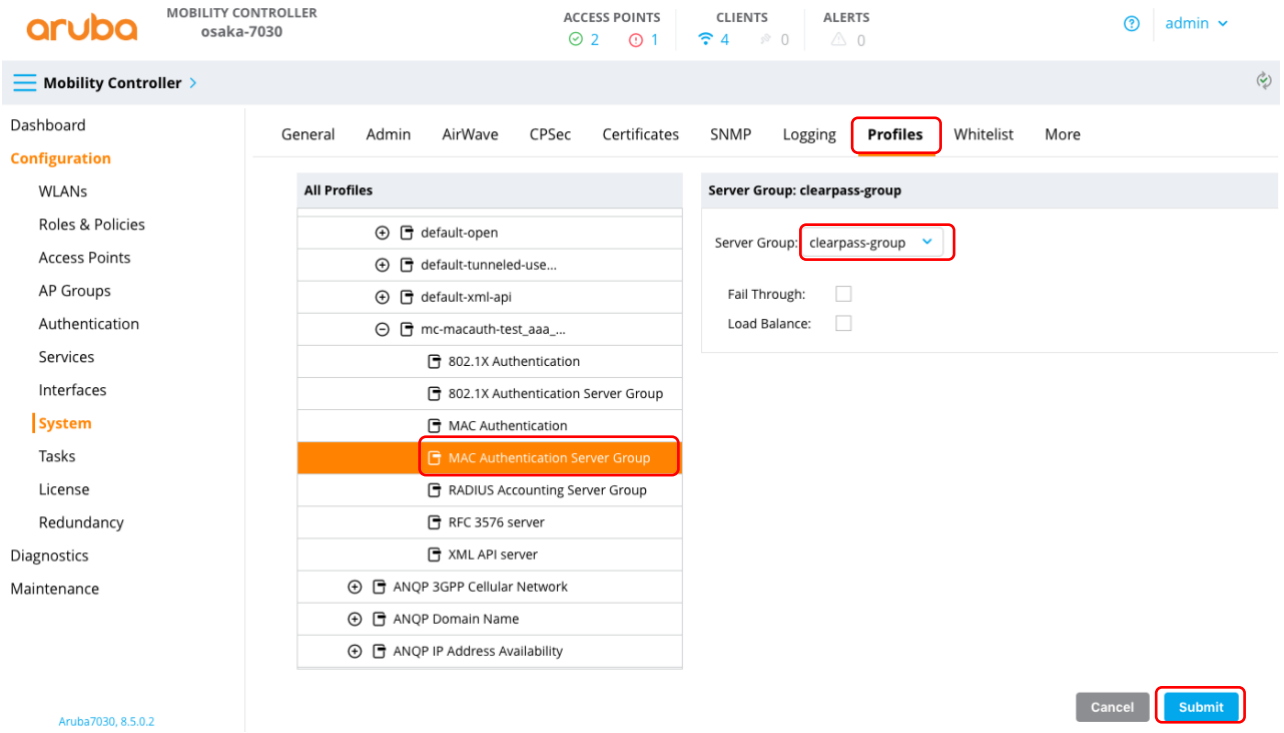
14) 「Add new server」をクリックして、任意の名前と ClearPass の IP アドレスを入力して「Submit」をクリックします。クリックしたら右上の「Pending Changes」>「Deploy Changes」とクリックして設定を反映します。



15) All Servers に ClearPass が追加されていますので、クリックしてシークレットキーを ClearPass で設定したものと同じにし、「Submit」をクリックします。クリックしたら右上の「Pending Changes」>「Deploy Changes」とクリックして設定を反映します。



16) 「Mobility Controller」>「Configuration」>「System」と開き、「Profiles」タブをクリックし、「Wireless LAN」>「AAA」>「(作成した SSID 名)_aaa_prof」>「MAC Authentication Server Group」を開きます。Server Group を先程作成したグループに変更し「Submit」をクリックします。クリックしたら右上の「Pending Changes」>「Deploy Changes」とクリックして設定を反映します。

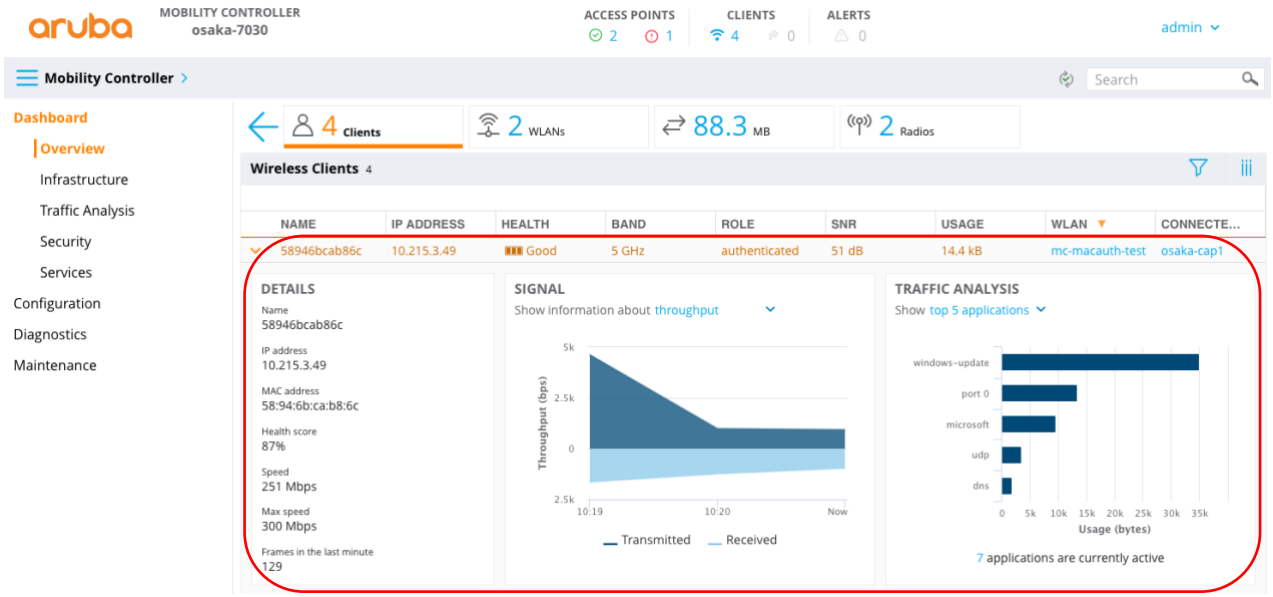


5.2.6 Aruba Mobility Controller での MAC 認証動作確認

1) クライアントを SSID に接続します。

2) 接続ができたら ClearPass の「モニタリング」>「Live Monitoring」>「アクセス・トラッカー」を開くと、コントローラーからの認証履歴が表示されていますので、クリックすると詳細を確認することができます。

3) コントローラーの「Dashboard」>「Overview」>「Clients」でも接続されていることが確認できます。



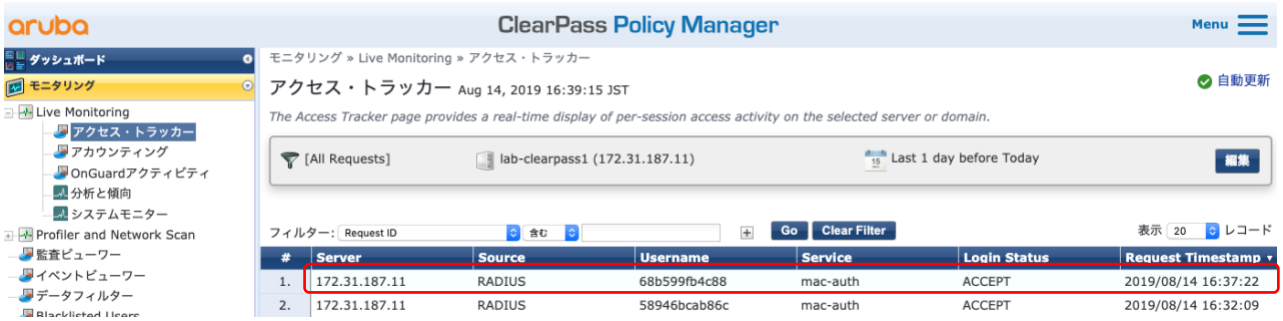
5.2.7 ArubaOS Switch の設定

```
Aruba# configure terminal

VLAN に IP アドレスを設定する
Aruba(config)# vlan 1 ip address 10.215.3.122 255.255.255.0

RADIUS サーバに ClearPass を設定する
Aruba(config)# radius-server host 172.31.187.11 key secret

1 番ポートで MAC 認証を有効化する
Aruba(config)#  aaa port-access mac-based 1

1 番ポートにおいて MAC 認証の最大クライアント数を指定する
Aruba(config)# aaa port-access mac-based 1 addr-limit 256

認証端末の IP アドレス情報も表示できるようにする(必須ではありません)
Aruba(config)# ip client-tracker
```

5.2.8 ArubaOS Switch での MAC 認証動作確認

1) クライアントをスイッチの認証ポートに接続します。

2) 接続ができたら ClearPass の「モニタリング」>「Live Monitoring」>「アクセス・トラッカー」を開くと、スイッチからの認証履歴が表示されていますので、クリックすると詳細を確認することができます。



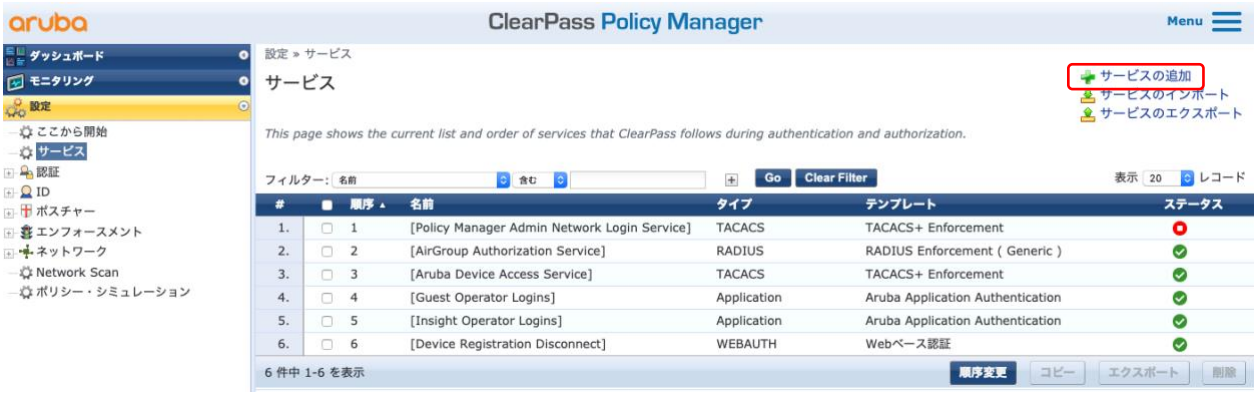
3) スイッチの方でも認証できていることが確認できます。

```
Aruba (config)# show port-access clients

 Port Access Client Status
  Port  Client Name   MAC Address       IP Address      User Role         Type  VLAN
  ----- ------------- ----------------- --------------- ----------------- ----- ---
  1     68b599fb4c88  68b599-fb4c88     10.215.3.227                      MAC   1

Aruba (config)# show port-access mac-based clients

 Port Access MAC-Based Client Status

  Port  MAC Address       IP Address                      Mode Client Status
  ----- ----------------- ------------------------------- ---- -----------------
  1     68b599-fb4c88     10.215.3.227                    User authenticated
```

5.3 無線 LAN の 802.1X 認証(EAP-PEAP)

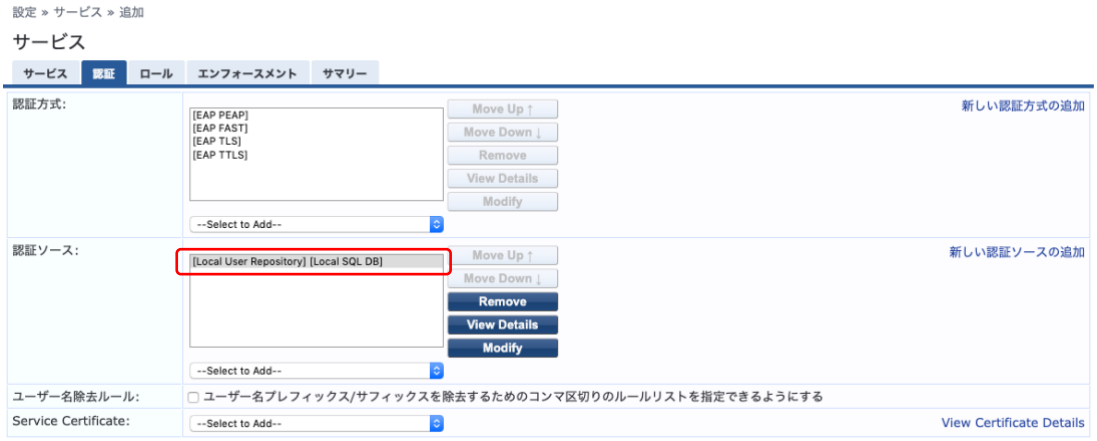
5.3.1 ClearPass のサービス設定

1) 設定」>「サービス」を開き、「サービスの追加」をクリックします。



2) サービスのタイプで「802.1X Wireless – Identity Only」を選択し、任意の名前を入力して右下の「Next」 をクリックします。

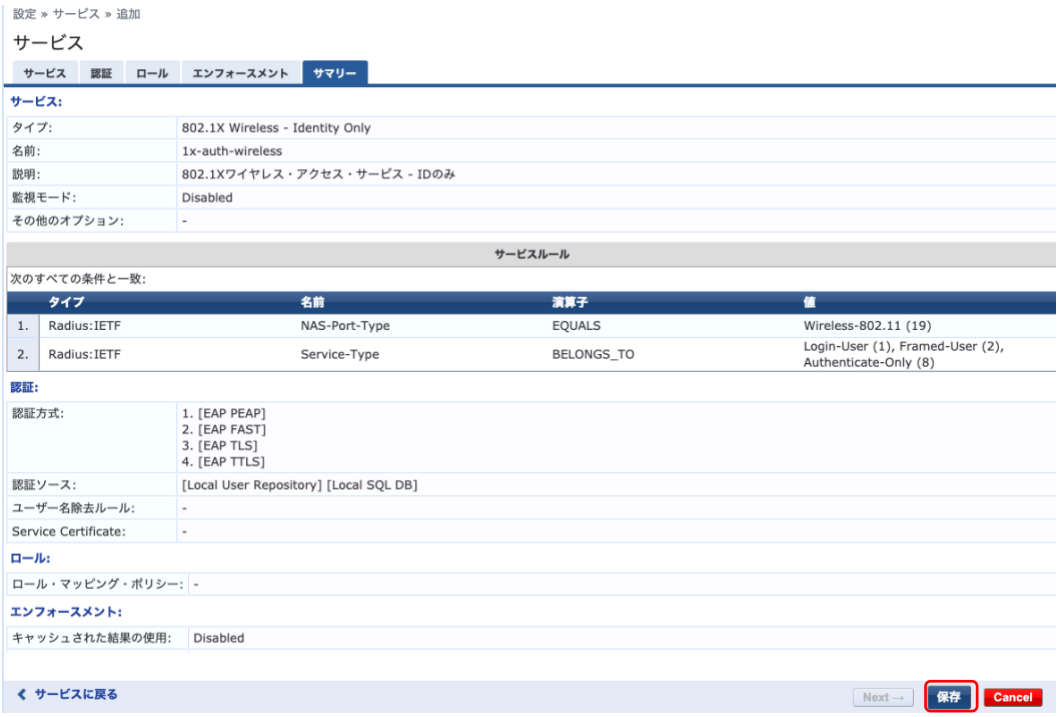
3) 認証ソースにて「Select to Add」をクリックし、「Local User Repository」をクリックして追加し、右下の「Next」をクリック



4) ロールマッピングポリシーは特に選択せず、そのまま右下の「Next」をクリックします。

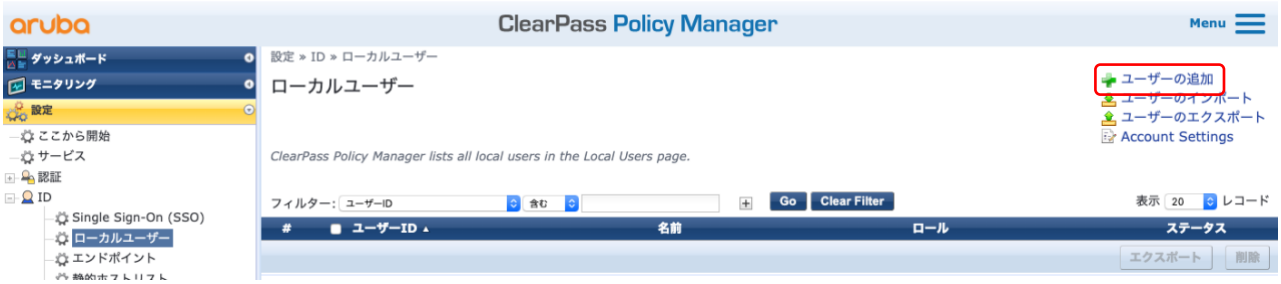
5) エンフォースメントポリシーはデフォルトの「Sample Allow Access Policy」が選択されていることを確認して右下の「Next」をクリックします。

6) 設定した内容のサマリーが表示されるので確認して右下の「保存」をクリックします。

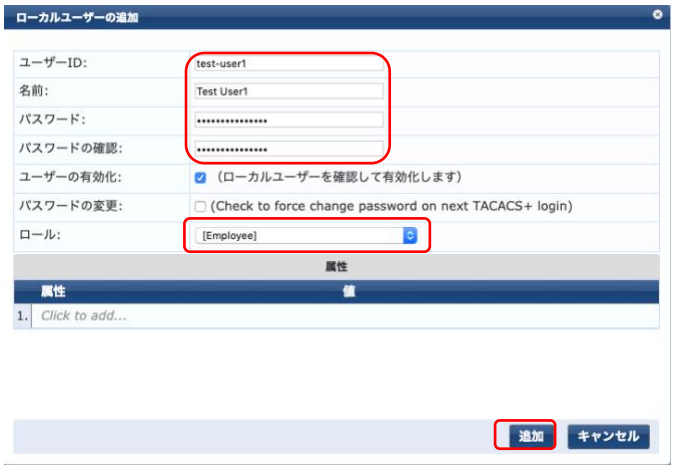


5.3.2 ClearPass へユーザー追加設定

1) 「設定」>「ID」>「ローカルユーザー」と開き、「ユーザーの追加」をクリックします。

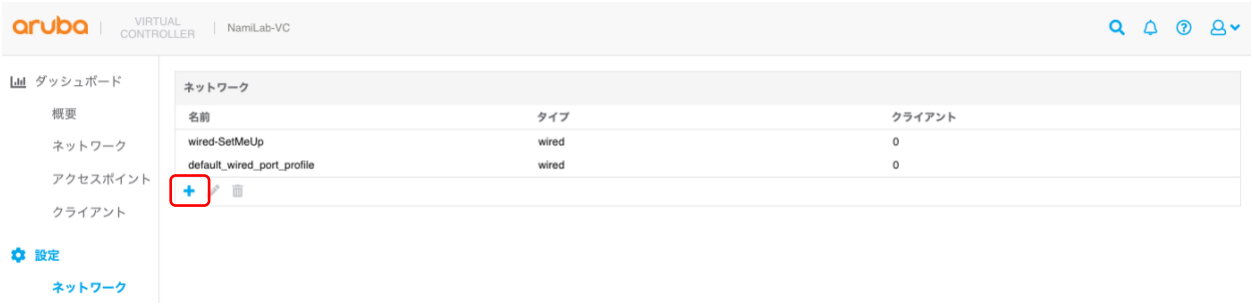


2) ユーザーID、名前、パスワードに任意の値を入力し、ロールは[Employee]を選択して「追加」をクリックします。



5.3.3 Aruba IAP の設定

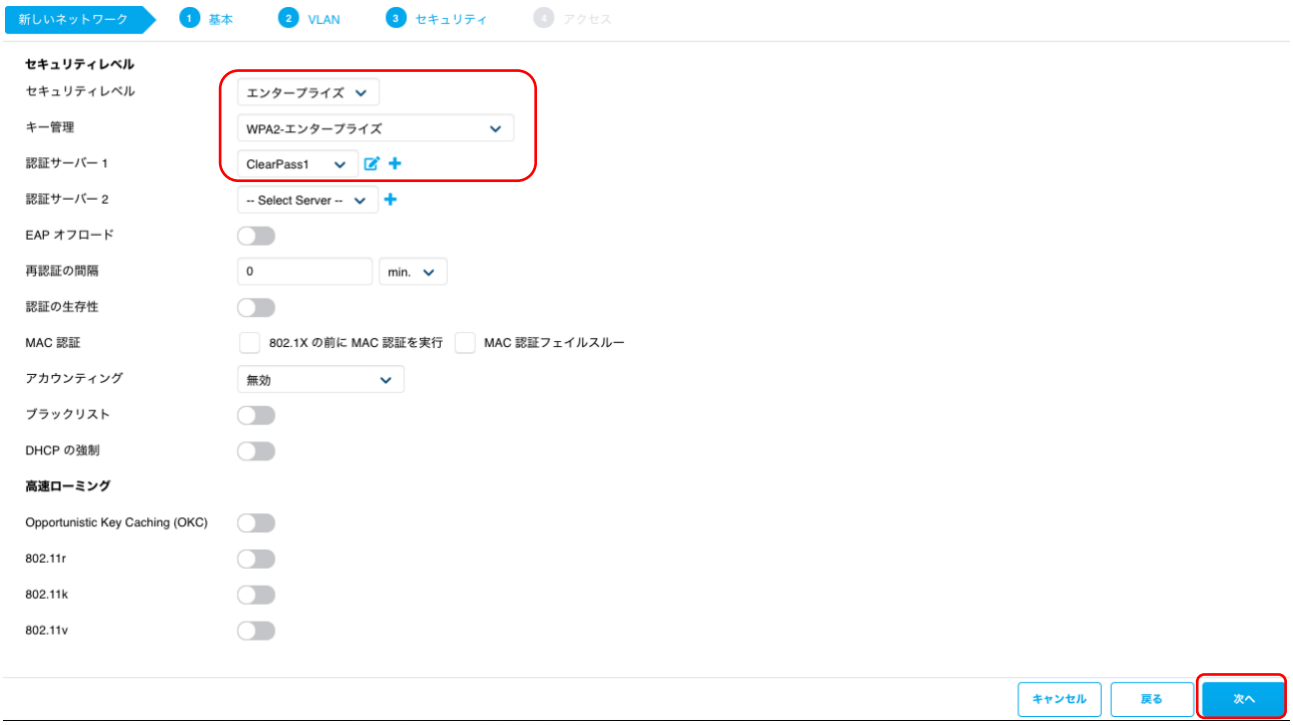
1) 「設定」>「ネットワーク」を開き、「+」をクリックします。



2) 名前を入力し「次へ」をクリックします。

3) クライアント IP と VLAN の割り当てはデフォルトのまま、「次へ」をクリックします。

4) セキュリティレベルを「エンタープライズ」にして、キー管理に「WPA2-エンタープライズ」を選択します。認証サーバー1 の「+」をクリックして、RADIUS サーバーとして ClearPass を登録して、「次へ」をクリックします。



認証サーバー追加の設定を行います。任意の名前、IP アドレス、ClearPass 側と同じシークレットキーの設定を行い、「OK」をクリックします。

5) アクセスルールはデフォルトのまま「終了」をクリックします。

5.3.4 Aruba IAP での 802.1X 認証(EAP-PEAP)動作確認

(1) Windows10 クライアントの設定

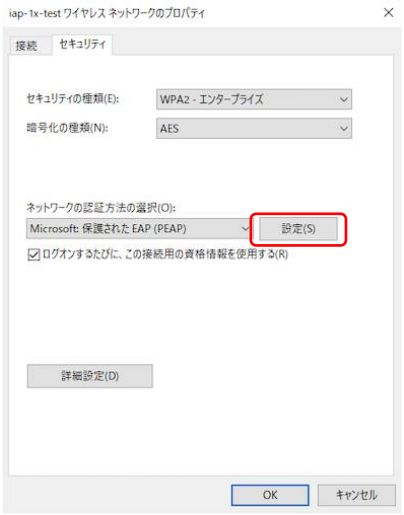
1) 「コントロールパネル」>「ネットワークとインターネット」>「ネットワークと共有センター」を開き、「新しい接続またはネットワークのセットアップ」をクリックします。

2) 「ワイヤレスネットワークに手動で接続します」を選択して「次へ」をクリックします。

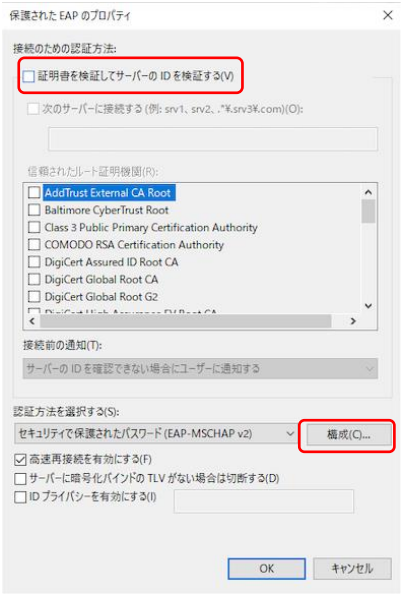
3) ネットワーク名に作成した SSID 名を入力し、セキュリティの種類で「WPA2-エンタープライズ」を選択して「次へ」をクリックします。

4) 「接続の設定を変更します」をクリックします。

5) ワイヤレスネットワークのプロパティが表示されますので、ネットワーク認証方法の選択の「設定」をクリックします。

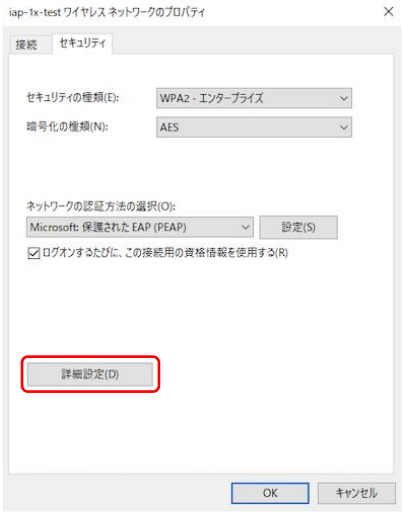


6) 保護された EAP のプロパティが表示されますので、「証明書を検証してサーバーの ID を検証する」のチェックを外し、認証方法を選択するの「構成」をクリックします。

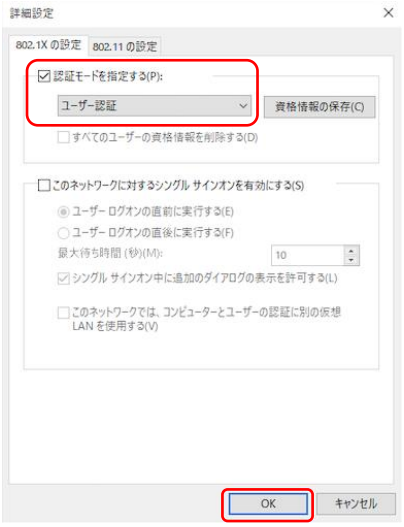


7) チェックを外して「OK」をクリックします。保護された EAP のプロパティに戻りますので、「OK」をクリックします。

8) ワイヤレスネットワークのプロパティに戻るので、「詳細設定」をクリックします。



9) 「認証モードを指定する」にチェックを入れ、「ユーザー認証」を選択して「OK」をクリックします。ワイヤレスネットワークのプロパティに戻るので「OK」をクリックして閉じます。



(2) 動作確認

1) クライアントを SSID に接続します。

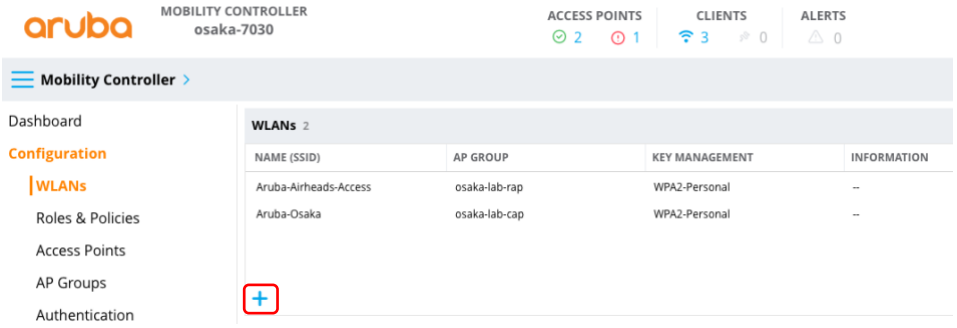
2) 接続ができたら ClearPass の「モニタリング」>「Live Monitoring」>「アクセス・トラッカー」を開くと、IAP からの認証履歴が表示されていますので、クリックすると詳細を確認することができます。

3) IAP の「ダッシュボード」>「クライアント」でも接続されていることが確認できます。

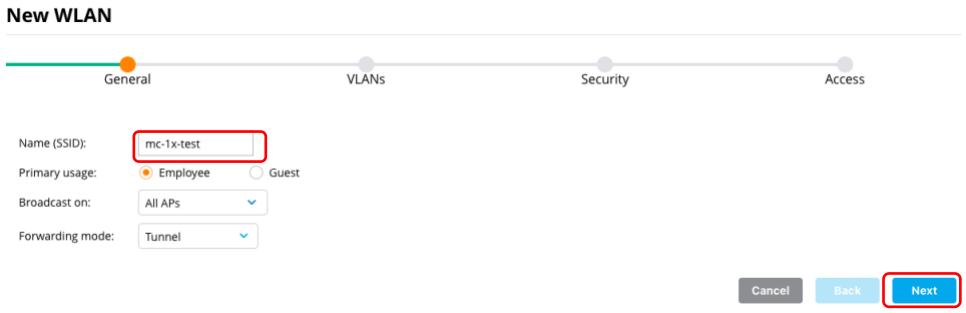
5.3.5 Aruba Mobility Controller の設定

※本説明は AOS8 Standalone MC で行なっております。

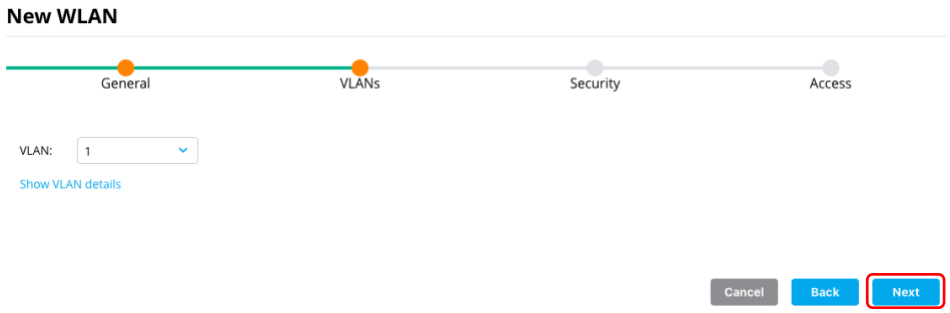
1) SSID の作成を行います。「Mobility Controller」>「Configuration」>「WLANs」と開き、「+」をクリックします。



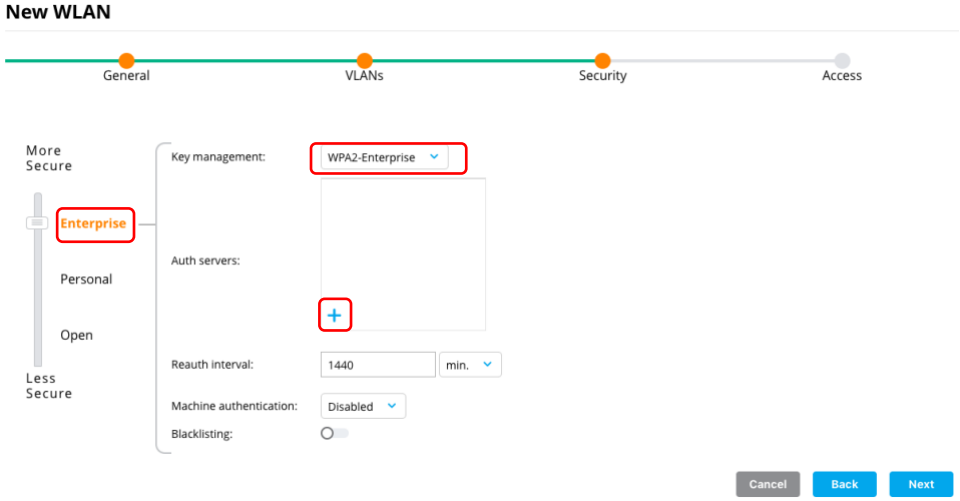
2) SSID の名前を入力して、「Next」をクリックします。



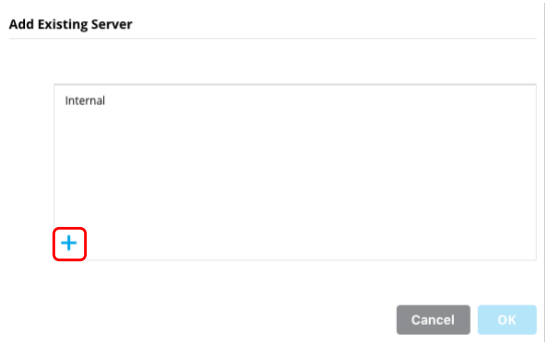
3) VLAN は特に指定がなければそのまま「Next」をクリックします。



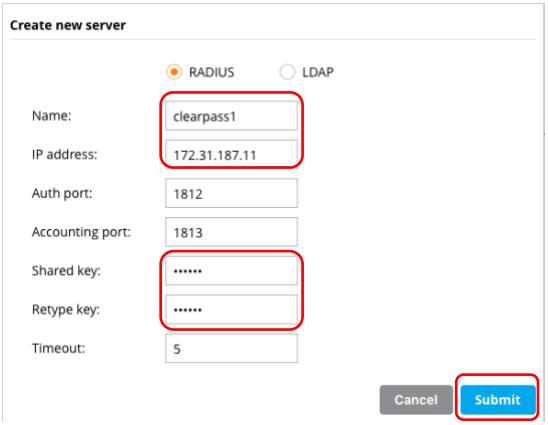
4) 左の選択肢より「Enterprise」を選択し、Key management を「WPA2-Enterprise」に設定して、Auth Servers の「+」をクリックします。PSK の Passphrase を設定します。



5) 「+」をクリックします。



6) 認証サーバー追加の設定を行います。任意の名前、IP アドレス、ClearPass 側と同じシークレットキーを入力したら「Submit」をクリックします。セキュリティ設定に戻りますので、「Next」をクリックします。



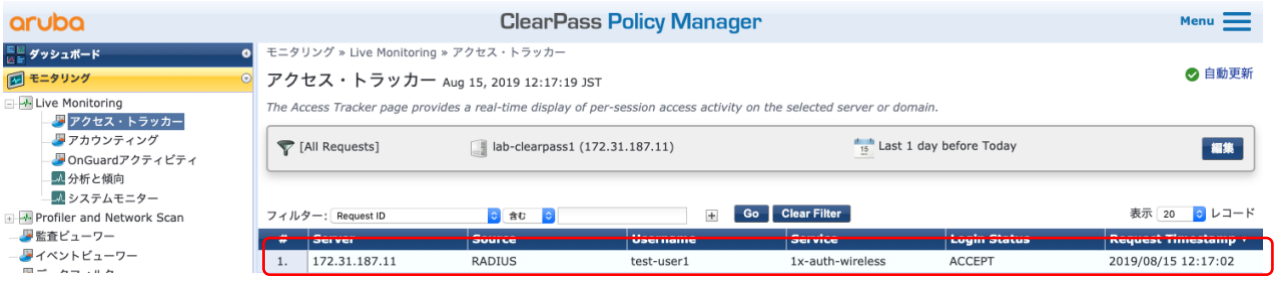
7) Default role を「authenticated」にして「Finish」をクリックします。クリックしたら右上の「Pending Changes」>「Deploy Changes」とクリックして設定を反映します。

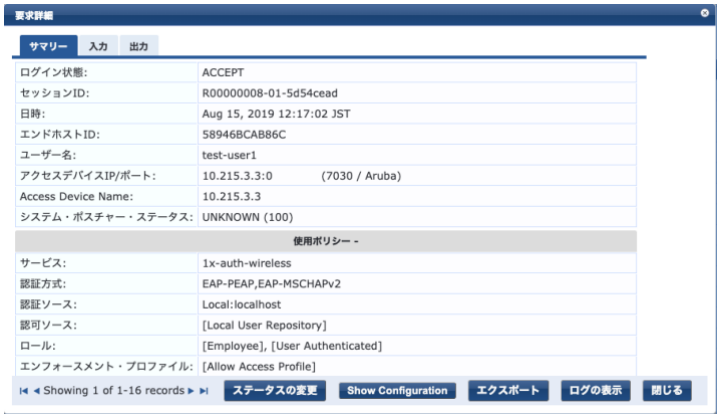
5.3.6 Aruba Mobility Controller での 802.1X 認証(EAP-PEAP)動作確認

※Windows10 クライアントの設定については「無線 LAN の 802.1X 認証(EAP-PEAP)」の「Windows10 クライアントの設定」と同様ですので、そちらを参照して下さい。

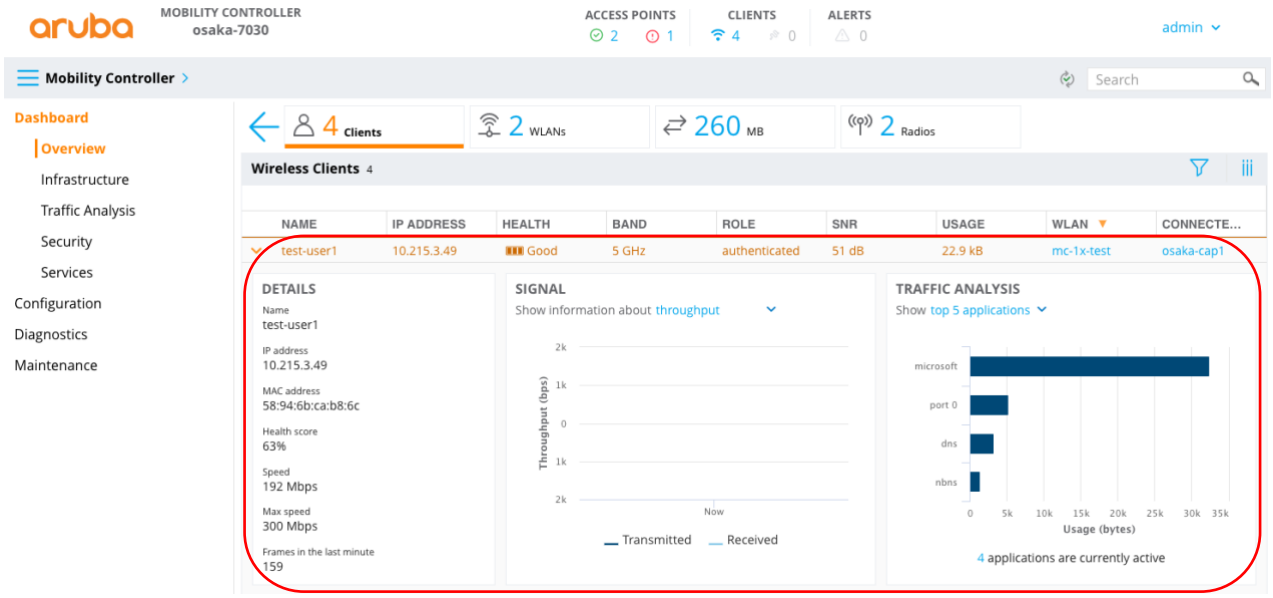
1) クライアントを SSID に接続します。

2) 接続ができたら ClearPass の「モニタリング」>「Live Monitoring」>「アクセス・トラッカー」を開くと、コントローラーからの認証履歴が表示されていますので、クリックすると詳細を確認することができます。





3) コントローラーの「Dashboard」>「Overview」>「Clients」でも接続されていることが確認できます。



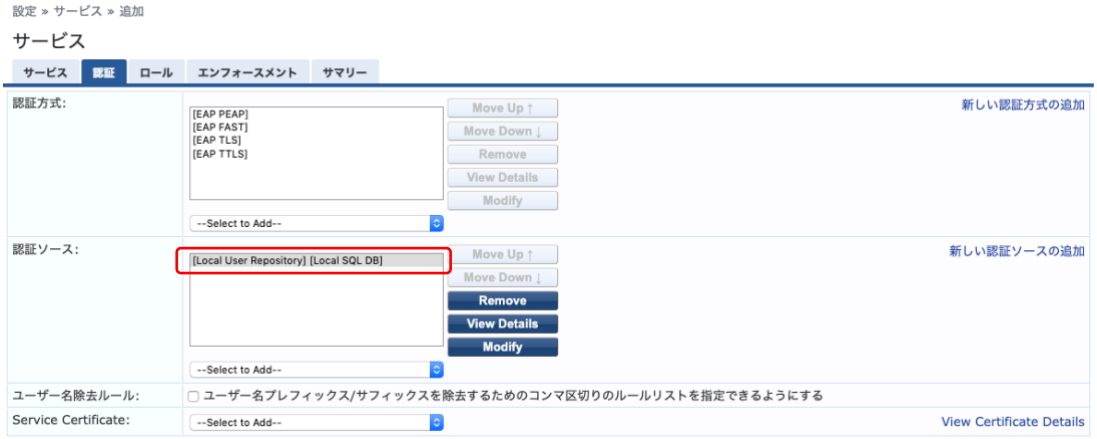
5.4 有線 LAN の 802.1X 認証(EAP-PEAP)

5.4.1 ClearPass の設定

1) 設定」>「サービス」を開き、「サービスの追加」をクリックします。

2) サービスのタイプで「802.1X Wired – Identity Only」を選択し、任意の名前を入力して右下の「Next」 をクリックします。

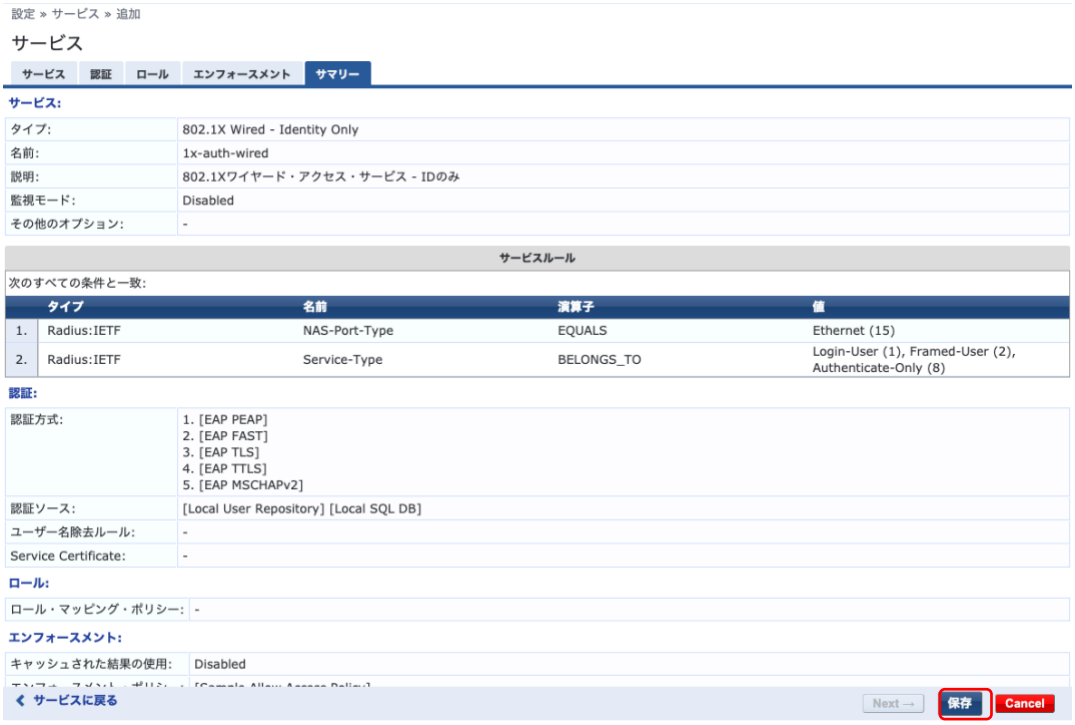
3) 認証ソースにて「Select to Add」をクリックし、「Local User Repository」をクリックして追加し、右下の「Next」をクリック



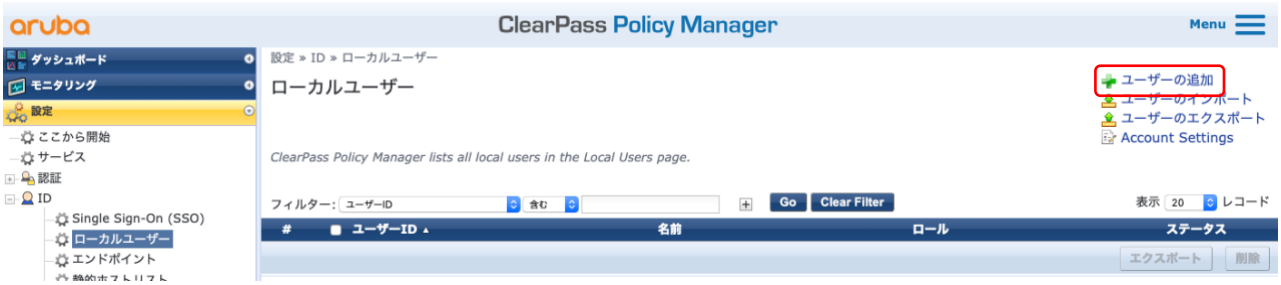
4) ロールマッピングポリシーは特に選択せず、そのまま右下の「Next」をクリックします。

5) エンフォースメントポリシーはデフォルトの「Sample Allow Access Policy」が選択されていることを確認して右下の「Next」をクリックします。

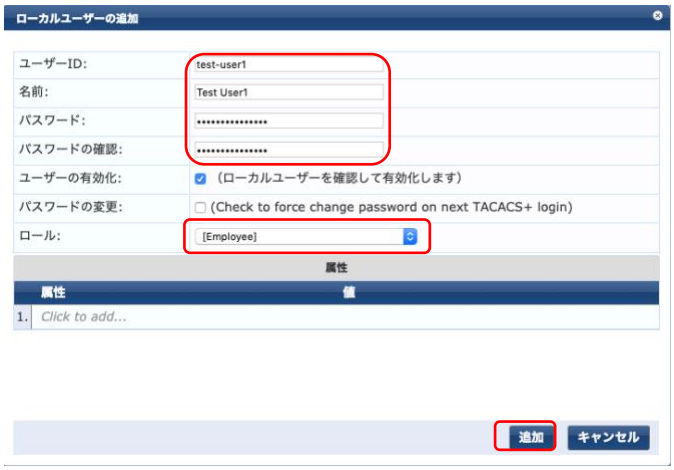
6) 設定した内容のサマリーが表示されるので確認して右下の「保存」をクリックします。



7) 「設定」>「ID」>「ローカルユーザー」と開き、「ユーザーの追加」をクリックします。



8) ユーザーID、名前、パスワードに任意の値を入力し、ロールは[Employee]を選択して「追加」をクリックします。



5.4.2 ArubaOS Switch の設定

Aruba# configure terminal

VLAN に IP アドレスを設定する
Aruba(config)# vlan 1 ip address 10.215.3.122 255.255.255.0

RADIUS サーバに ClearPass を設定する
Aruba(config)# radius-server host 172.31.187.11 key secret

802.1X 認証の認証方式を EAP RADIUS に設定する
Aruba(config)# aaa authentication port-access eap-radius

1 番ポートで 802.1X 認証を有効化する
Aruba(config)# aaa port-access authenticator 1

1 番ポートにおいて 802.1X 認証の最大クライアント数を指定する
Aruba(config)# aaa port-access authenticator 1 client-limit 32

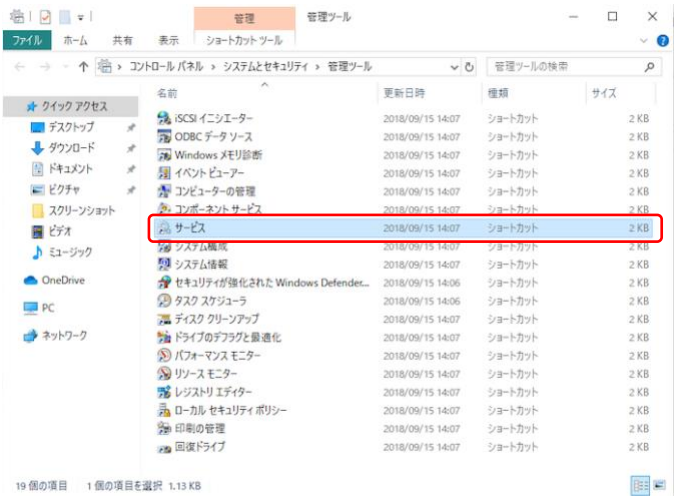
802.1X 認証を有効にする
Aruba(config)# aaa port-access authenticator active

認証端末の IP アドレス情報も表示できるようにする(必須ではありません)
Aruba(config)# ip client-tracker

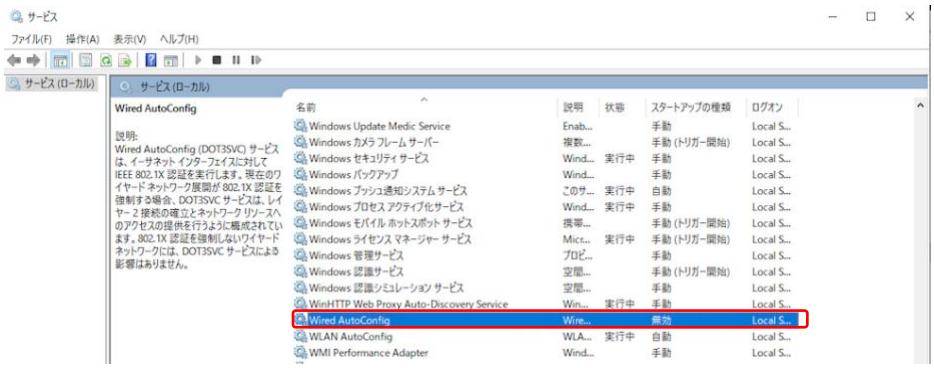
5.4.3 ArubaOS Switch での 802.1X 認証(EAP-EPAP)動作確認

(1) Windows10 クライアントの設定

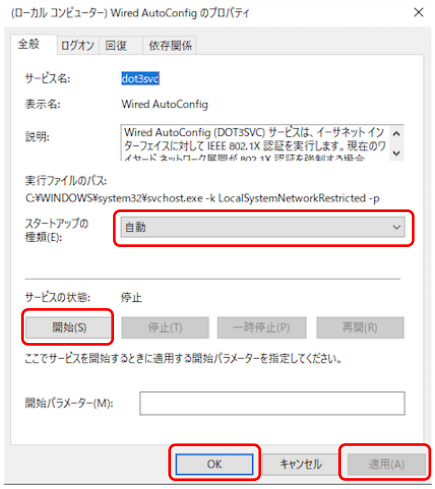
1) 「コントロールパネル」>「システムとセキュリティ」>「管理ツール」を開き、「サービス」をダブルクリックします。



2) 「Wired AutoConfig」をダブルクリックします。



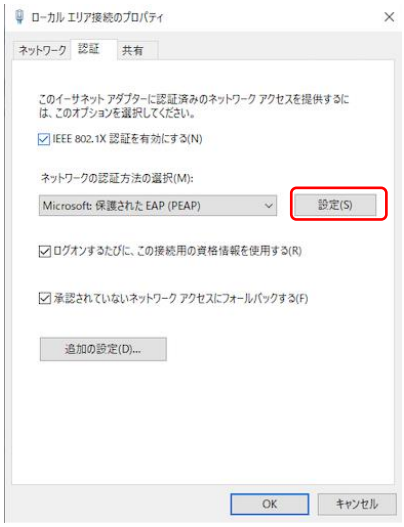
3) スタートアップの種類を「自動」にして「適用」をクリックし、その後「開始」をクリックします。サービスの状態が実行中になったら、「OK」をクリックします。



4) 「コントロールパネル」>「ネットワークとインターネット」>「ネットワークと共有センター」を開き、「アダプターの設定の変更」をクリックします。

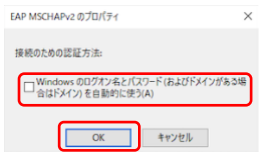
5) 「ローカルエリア接続」を右クリックしプロパティを表示します。

6) ローカルエリア接続のプロパティが表示されますので、ネットワーク認証方法の選択の「設定」をクリックします。

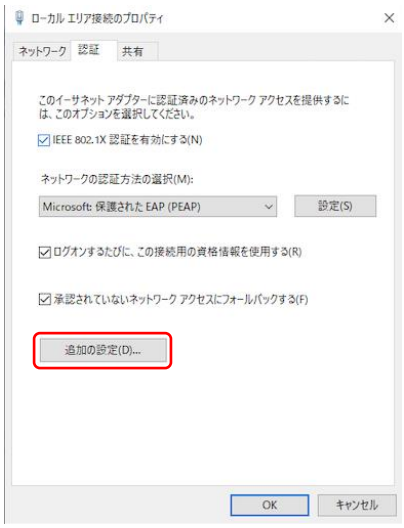


7) 保護された EAP のプロパティが表示されますので、「証明書を検証してサーバーの ID を検証する」のチェックを外し、認証方法を選択するの「構成」をクリックします。

8) チェックを外して「OK」をクリックします。保護された EAP のプロパティに戻りますので、「OK」をクリックします。



9) ローカルエリア接続のプロパティに戻るので、「追加の設定」をクリックします。

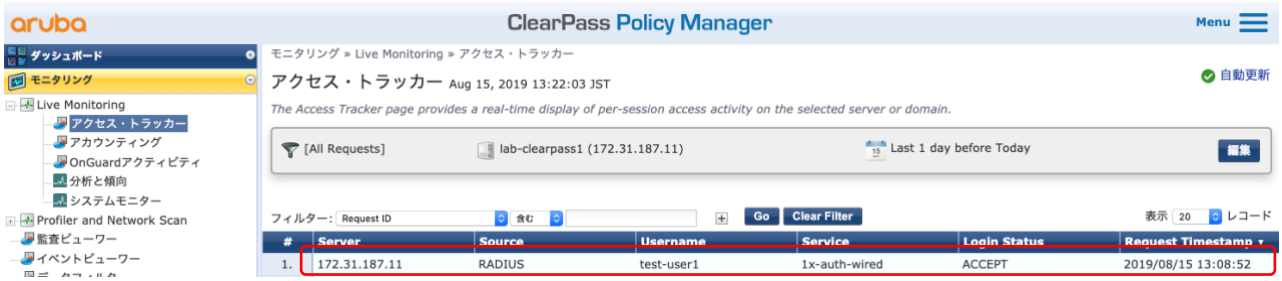


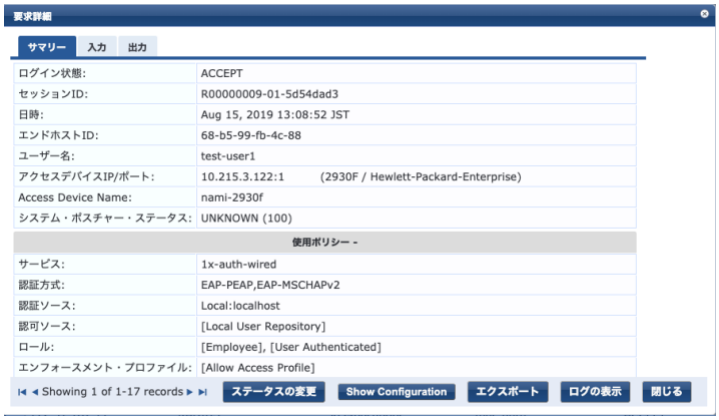
10) 「認証モードを指定する」にチェックを入れ、「ユーザー認証」を選択して「OK」をクリックします。ローカルエリア接続のプロパティに戻るので「OK」をクリックして閉じます。

(2) 動作確認

1) クライアントをスイッチの認証ポートに接続します。

2) 接続ができたら ClearPass の「モニタリング」>「Live Monitoring」>「アクセス・トラッカー」を開くと、スイッチからの認証履歴が表示されていますので、クリックすると詳細を確認することができます。





3) スイッチの方でも認証できていることが確認できます。

```
Aruba (config)# show port-access clients

 Port Access Client Status
  Port  Client Name   MAC Address       IP Address      User Role         Type  VLAN
  ----- ------------- ----------------- --------------- ----------------- ----- ---
  1     test-user1    68b599-fb4c88     10.215.3.227                      8021X 1

Aruba (config)# show port-access authenticator clients
 Port Access Authenticator Client Status

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No
  Use LLDP data to authenticate [No] : No
  Dot1X EAP Identifier Compliance [Disabled] : Disabled

  Port  Client Name           MAC Address       IP Address      Client Status
  ----- --------------------- ----------------- --------------- --------------------
  1     test-user1            68b599-fb4c88     10.215.3.227    Authenticated
```

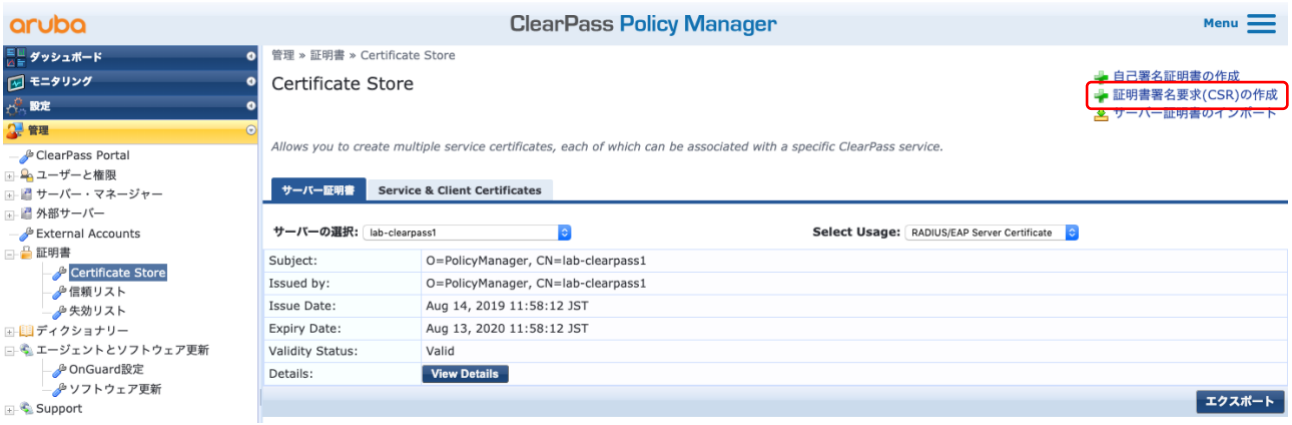
第 6章 ClearPass Onboard の設定

6.1 クライアント証明書を手動発行する無線 LAN の 802.1X 認証(EAP-TLS)

本セクションでは ClearPass を認証局として手動でクライアント証明書を発行して端末にインストールし、認証する手順について説明しています。なお、本設定を行うには Onboard ライセンスが必要です。

6.1.1 ClearPass の認証局設定

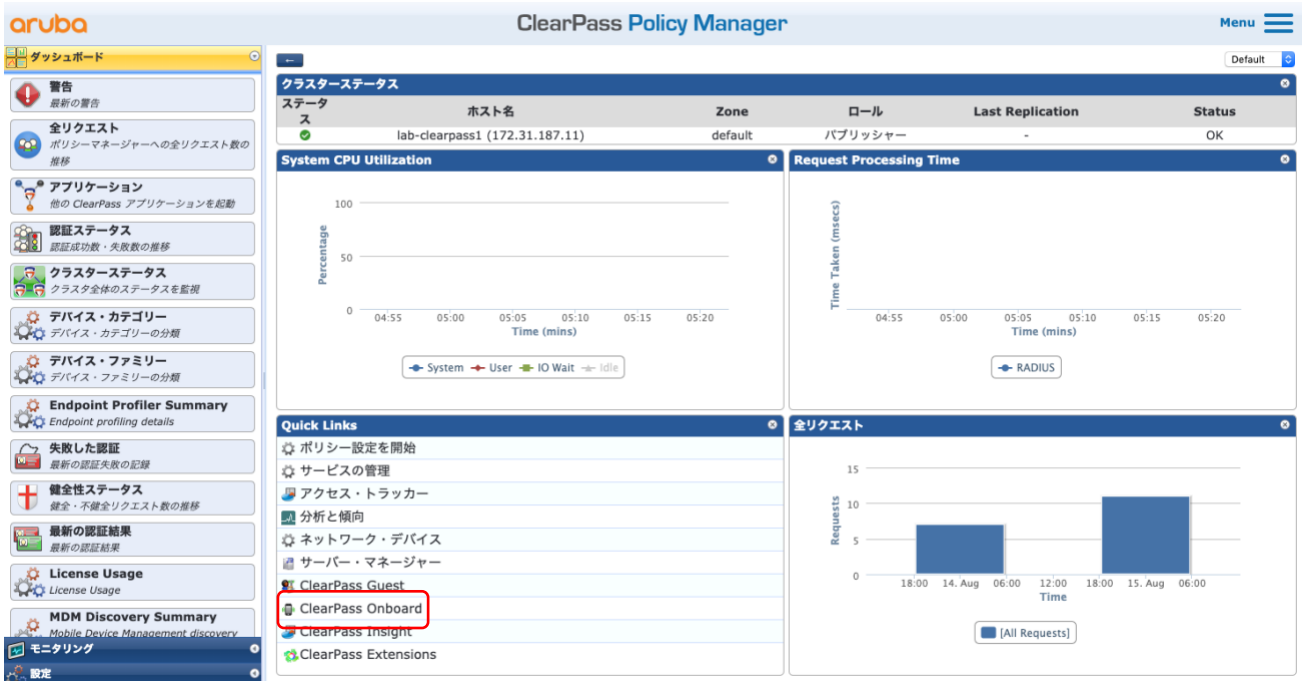
1) まず CSR の発行を行います。「管理」>「証明書」>「Certificate Store」と開き、「証明書署名要求(CSR)の作成」をクリックます。



2) 任意の秘密鍵パスワードを設定し、「送信」をクリックします。

3) 「Download CSR」をクリックすると PC のローカルに”CertSignRequest.csr”ファイルがダウンロードされます。

4) 「ダッシュボード」>「Quick Links」から「ClearPass Onboard」をクリックします。別ウィンドウ(別タブ)で ClearPass Onboard が表示されます。



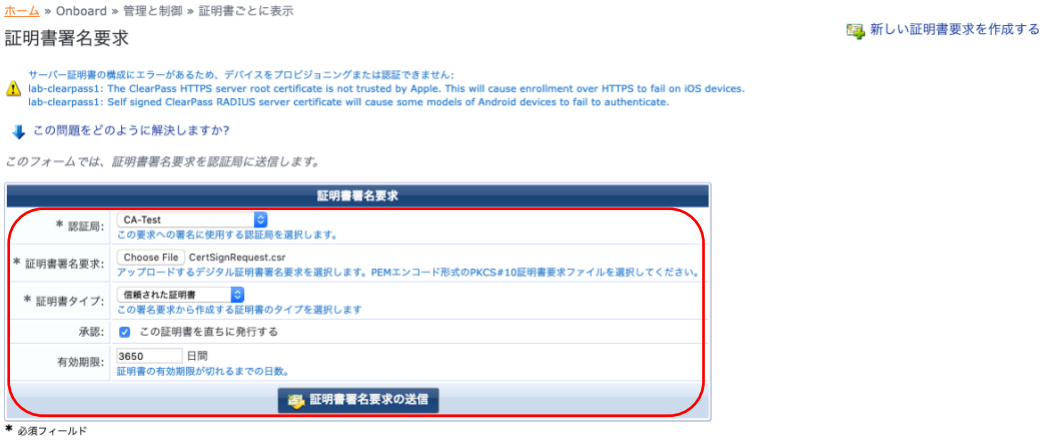
5) 「Onboard」>「証明期間」を開き「新しい認証局を作成します」をクリックします。

6) 認証局の設定を行います。モードは「ルート CA」を選択し、赤枠で囲っている部分の設定を行います。設定が終わったら「認証局の作成」をクリックします。

7) 認証局が作成されていることを確認します。

8) 「Onboard」>「管理と制御」>「証明書ごとに表示」と開き「証明書署名要求をアップロードする」をクリックします。

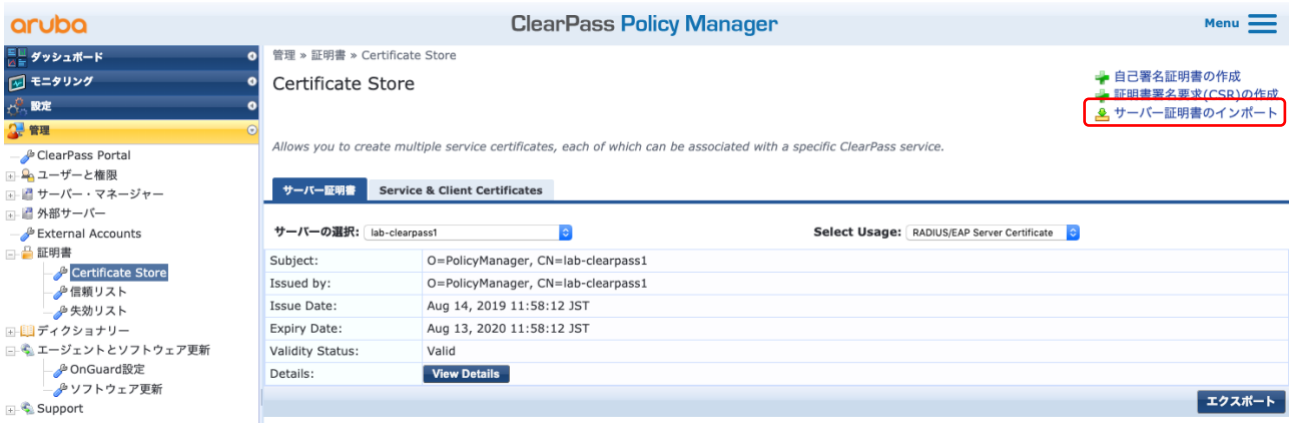
9) 認証局に”本手順で作成した認証局”、証明書署名要求はダウンロードした”CertSignRequest.csr”ファイル、証明書タイプに「信頼された証明書」を選択し、「この証明書を直ちに発行する」へチェックを入れ、有効期限を設定して「証明書署名要求の送信」をクリック



10) CSR が読み込まれると証明書の管理画面にサーバー証明書が作成されたことが確認できます。

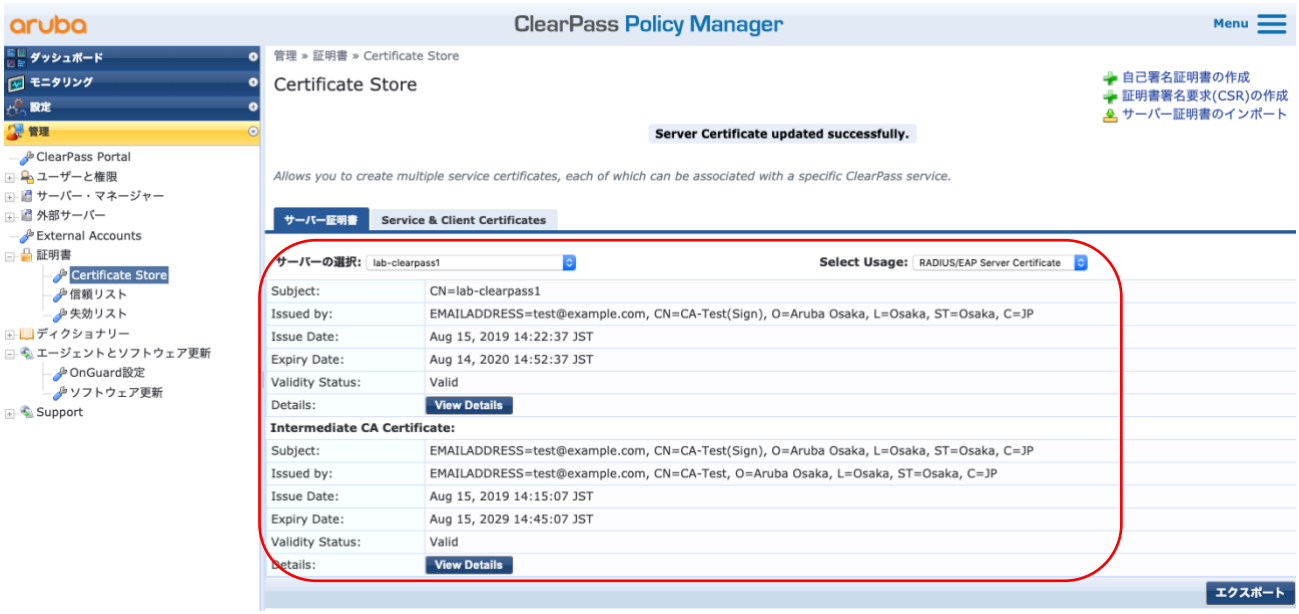
11) 作成されたサーバー証明書を選択し、「証明書のエクスポート」をクリックし、形式を「バイナリ証明書(.crt)」にして「証明書のエクスポート」をクリックします。PC のローカルに”(ClearPass サーバー名).crt”ファイルがダウンロードされます。

12) ClearPass Policy Manager の画面に戻り、「管理」>「証明書」>「Certificate Store」と開き、「サーバー証明書のインポート」をクリックます。



13) Certificate Type に「サーバー証明書」を選択し、証明書ファイルにダウンロードした”ClearPass サーバー名”.crt ファイルを選択して「インポート」をクリックします。

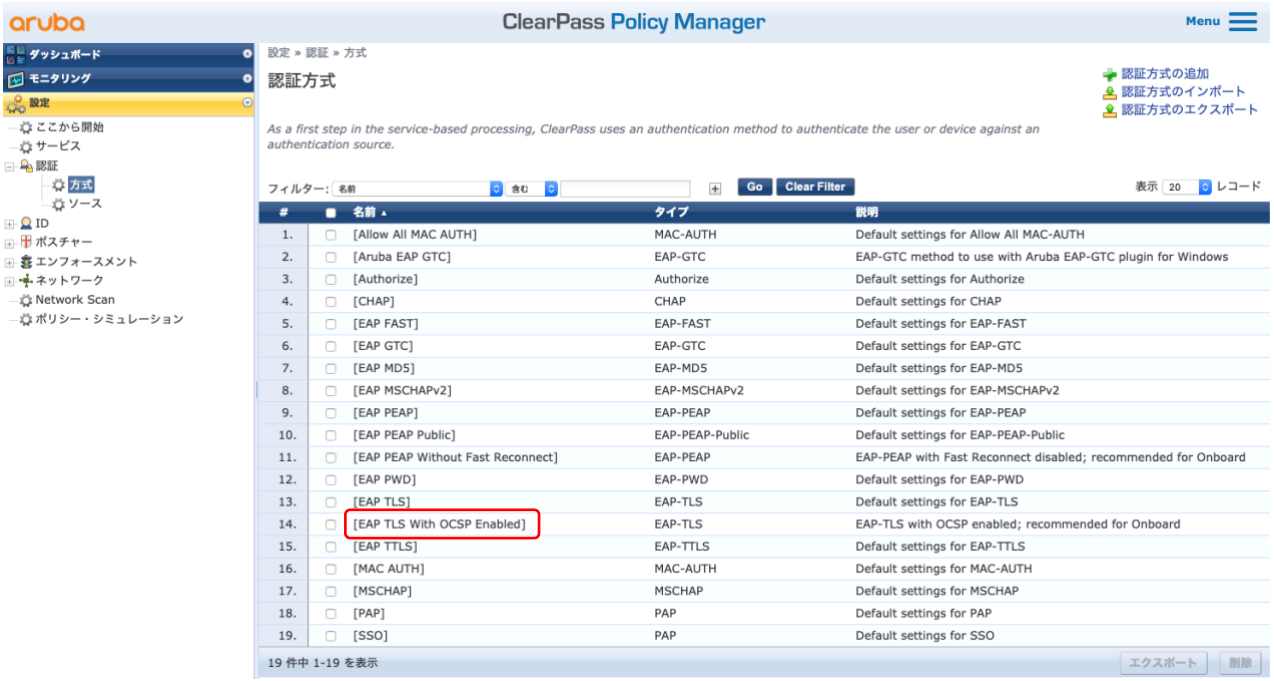
14) サーバー証明書がインポートされていることを確認します。



6.1.2 ClearPass の認証方式設定

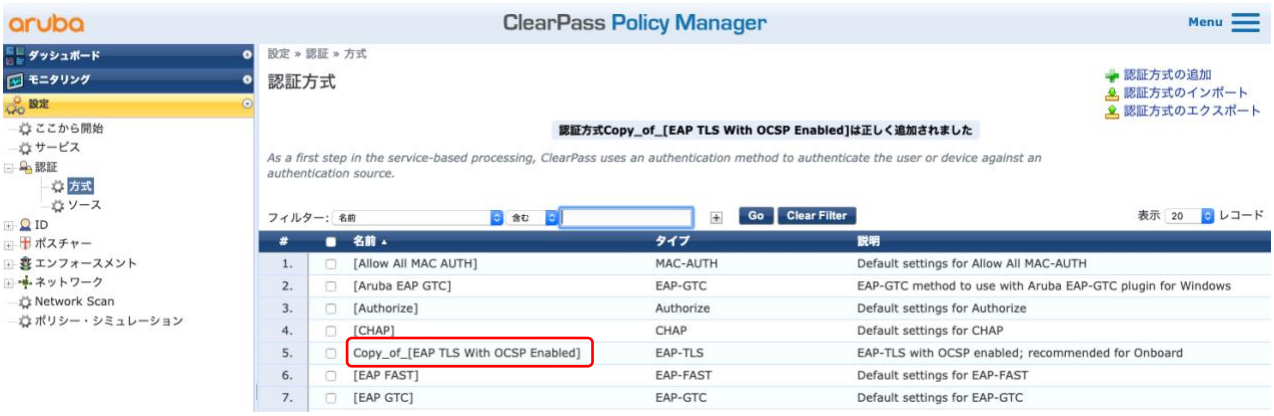
1) 発行するクライアント証明書の失効管理を行うため、OSCP の設定を行います。ClearPass Onboard へアクセスし、「Onboard」>「証明期間」を開き、作成した認証局の OSCP URL の末尾の数字(この場合は”2”)を確認します。

2) ClearPass Policy Manager へ戻り「設定」>「認証」>「方式」と開き、デフォルトで定義されている”[EAP TLS With OCSP Enabled]”をクリックします。



3) 「コピー」をクリックします。

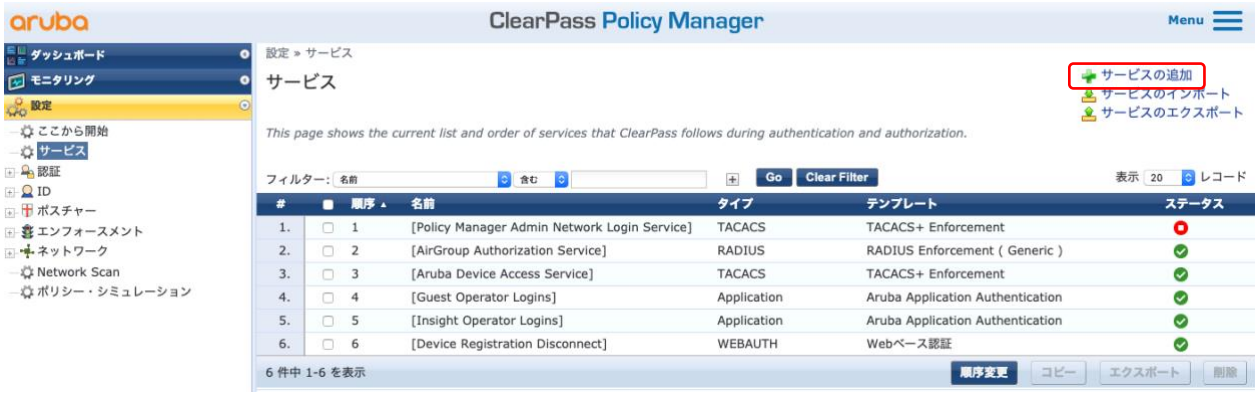
4) 一覧にコピーされた”Copy_of_[EAP TLS With OCSP Enabled]”をクリックします。



5) OCSP URL デフォルト値の末尾の数字を確認した数字に変更します。(本例では”1”を”2”に変更)変更したら「保存」をクリックします。(1 で表示されている OCSP URL 全体をコピー&ペーストする形でも対応できますが、OCSP URL に ClearPass のホスト名が入っており、ClearPass の冗長時に影響がありますので、末尾の数字のみを変える形で説明しています。)

6.1.3 ClearPass のサービス設定

1) 設定」>「サービス」を開き、「サービスの追加」をクリックします。



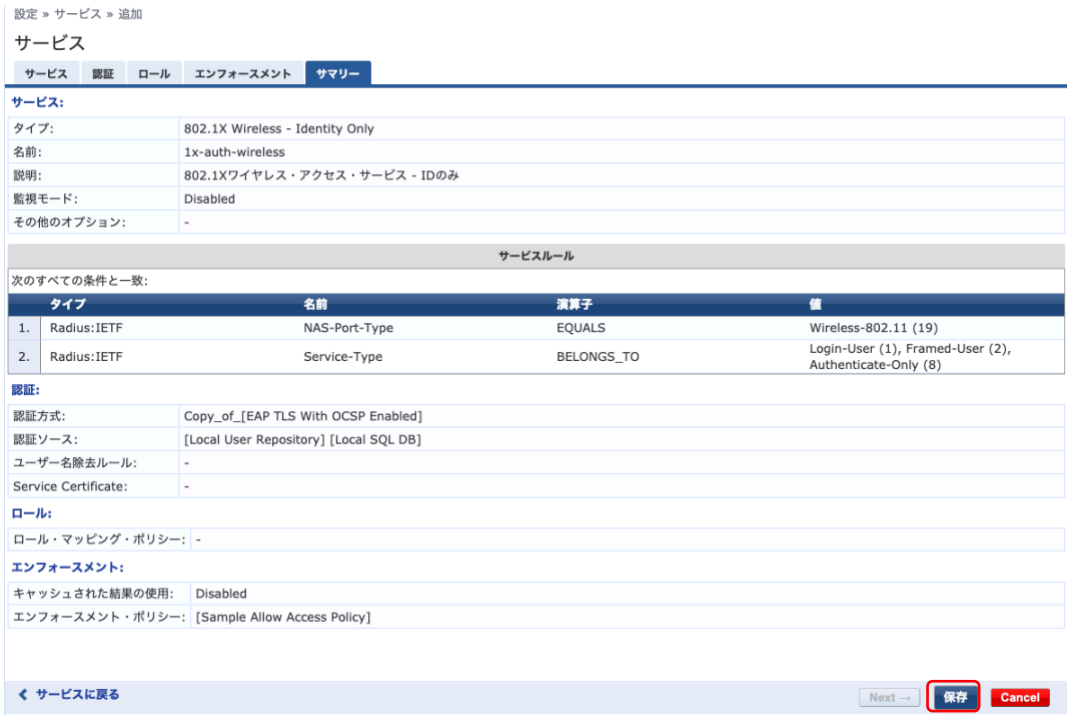
2) サービスのタイプで「802.1X Wireless – Identity Only」を選択し、任意の名前を入力して右下の「Next」 をクリックします。

3) 認証方式にデフォルトで入っている項目を全て Remove し、先程作成した「Copy_of_[EAP TLS With OCSP Enabled]」を追加、認証ソースにて「Select to Add」をクリックし、「Local User Repository」をクリックして追加し、右下の「Next」をクリック

4) ロールマッピングポリシーは特に選択せず、そのまま右下の「Next」をクリックします。

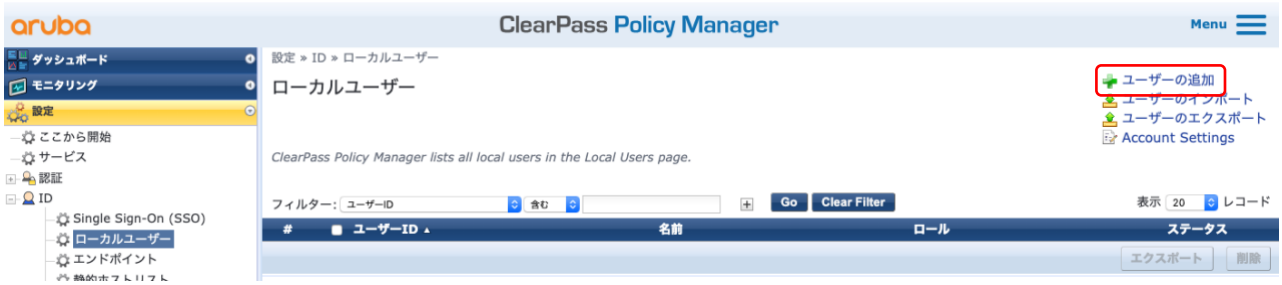
5) エンフォースメントポリシーはデフォルトの「Sample Allow Access Policy」が選択されていることを確認して右下の「Next」をクリックします。

6) 設定した内容のサマリーが表示されるので確認して右下の「保存」をクリックします。

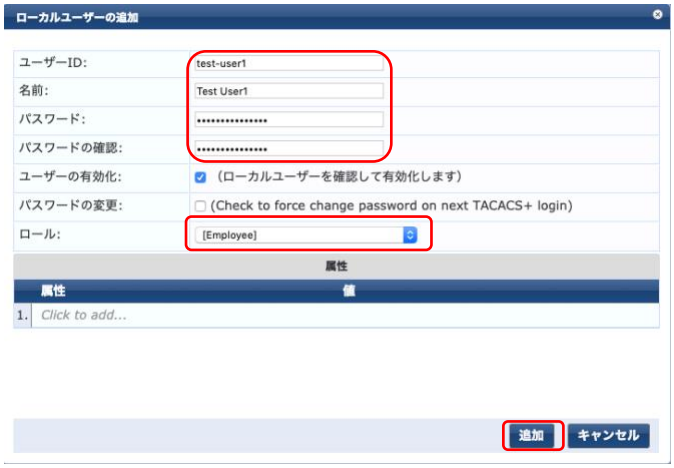


6.1.4 ClearPass へユーザー追加設定

1) 「設定」>「ID」>「ローカルユーザー」と開き、「ユーザーの追加」をクリックします。



2) ユーザーID、名前、パスワードに任意の値を入力し、ロールは[Employee]を選択して「追加」をクリックします。



6.1.5 ClearPass でのクライアント証明書発行

1) ClearPass Onboard へアクセスし、「Onboard」>「管理と制御」>「証明書ごとに表示」と開き、「新しい証明書署名要求」をクリックします。

2) 認証局に作成した認証局、証明書タイプに「TLS クライアント証明書」を選択し、必要項目(一般名は作成したローカルユーザー名)を埋め、「承認」にチェックを入れ、有効期限をセットして「証明書要求の作成」をクリックします。

3) クライアント証明書が作成されたことを確認します。

4) 証明書のエクスポートを行います。証明書をクリックして「証明書のエクスポート」クリックします。形式を「PKCS#12 証明書およびキー(.p12)」を選択し、パスフレーズを設定して「証明書のエクスポート」をクリックすると、”(ユーザー名.p12)”の証明書が PC のローカルにダウンロードされます。

6.1.6 Aruba IAP 及び Aruba Mobility Controller の設定

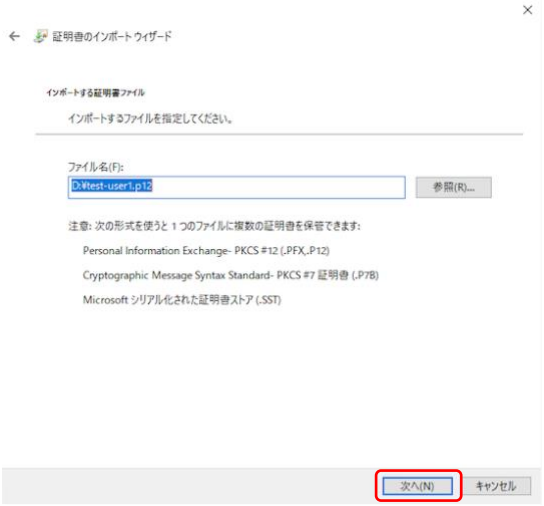
「無線 LAN の 802.1X 認証(EAP-PEAP)」の「Aruba IAP の設定」及び「Aruba Mobility Controller の設定」と同じですので、そちらを参考にして設定を行って下さい。

6.1.7 Aruba IAP 及び Aruba Mobility Controller での 802.1X 認証(EAP-TLS)動作確認

(1) Windows10 クライアントの設定

1) エクスポートした証明書を認証する端末にコピーし、ダブルクリックすると証明書のインポートウィザードが開始されます。「現在のユーザー」を選択し「次へ」をクリックします。

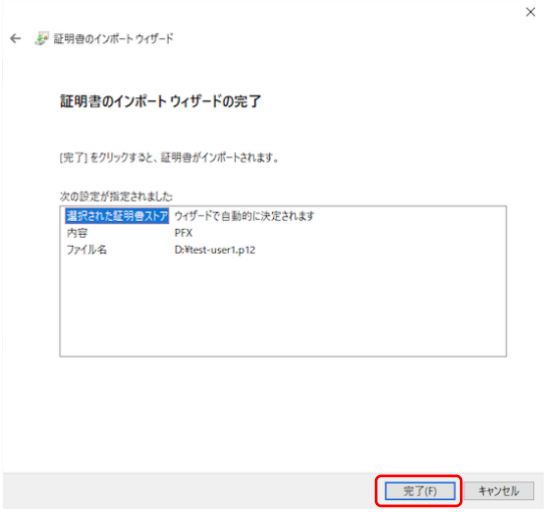
2) インポートするファイルが正しいことを確認して「次へ」をクリックします。



3) クライアント証明書をエクスポートした時に設定したパスフレーズをパスワードの欄に入力して「次へ」をクリックします。

4) そのまま「次へ」をクリックします。

5) 「完了」をクリックします。



6) 「はい」をクリックしてインストールします。

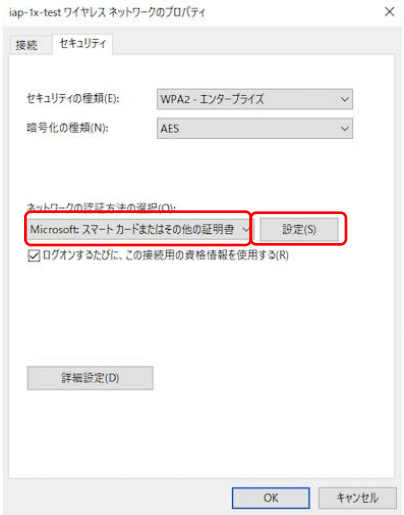
7) 「コントロールパネル」>「ネットワークとインターネット」>「ネットワークと共有センター」を開き、「新しい接続またはネットワークのセットアップ」をクリックします。

8) 「ワイヤレスネットワークに手動で接続します」を選択して「次へ」をクリックします。

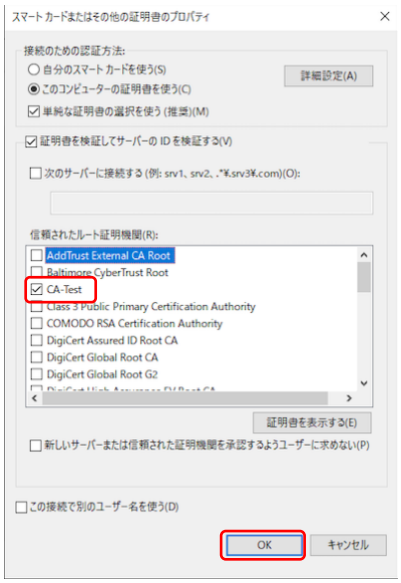
9) ネットワーク名に接続する SSID 名を入力し、セキュリティの種類で「WPA2-エンタープライズ」を選択して「次へ」をクリックします。

10) 「接続の設定を変更します」をクリックします。

11) ワイヤレスネットワークのプロパティが表示されますので、ネットワークの認証方法の選択を「Microsoft: スマートカードまたはその他の証明書」にして「設定」をクリックします。



12) インストールした証明書にチェックを入れ「OK」をクリックします。



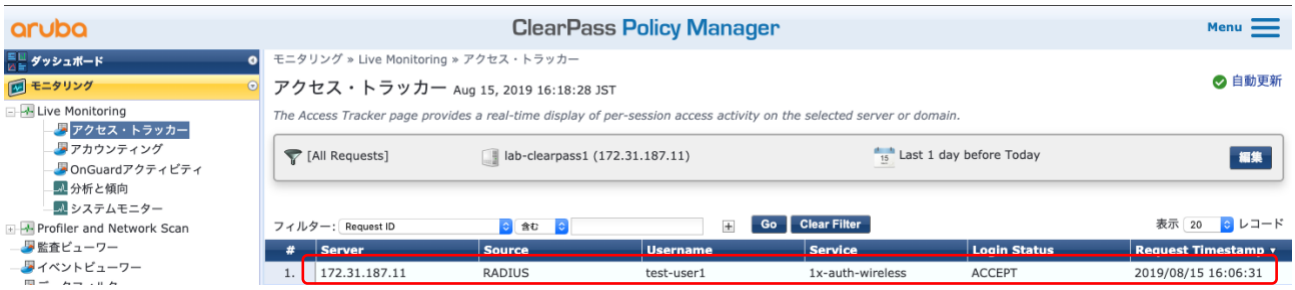
13) ワイヤレスネットワークのプロパティに戻るので、「詳細設定」をクリックします。

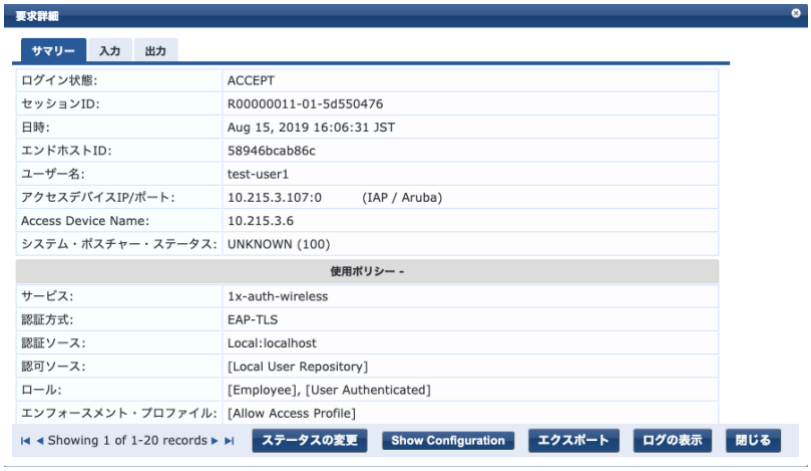
14) 「認証モードを指定する」にチェックを入れ、「ユーザー認証」を選択して「OK」をクリックします。ワイヤレスネットワークのプロパティに戻るので「OK」をクリックして閉じます。

(2) 動作確認(Aruba IAP の場合)

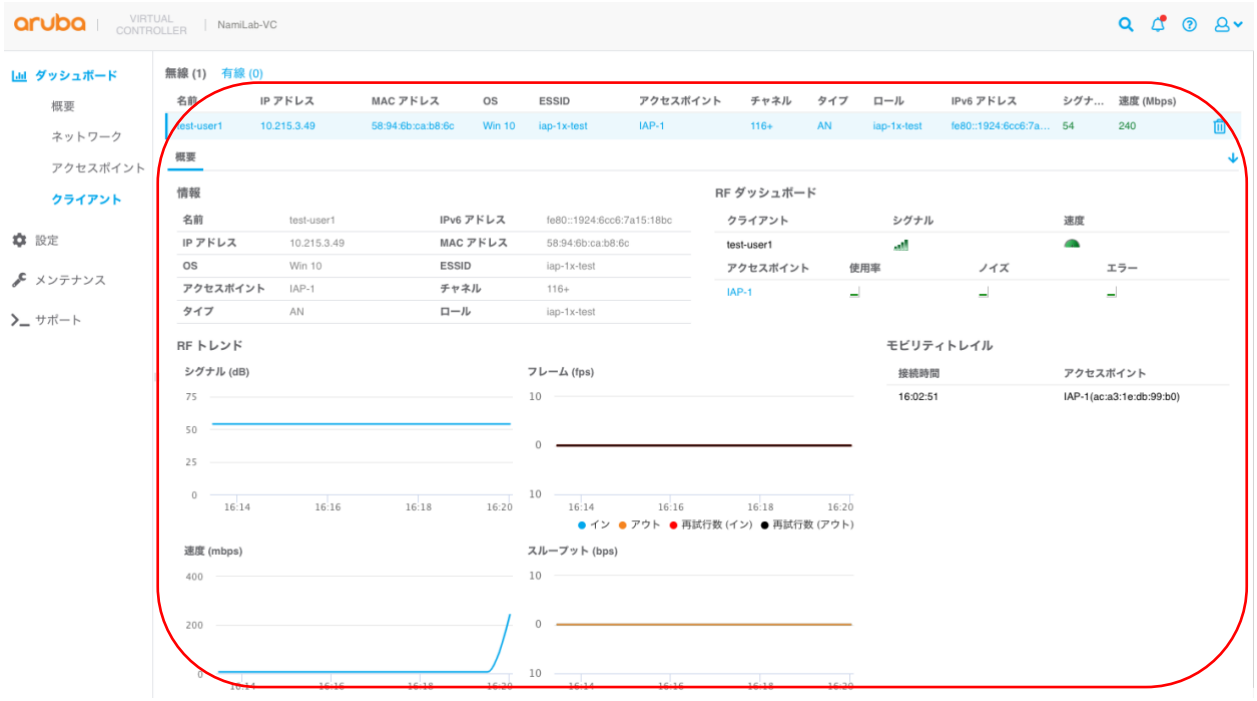
1) クライアントを SSID に接続します。

2) 接続ができたら ClearPass の「モニタリング」>「Live Monitoring」>「アクセス・トラッカー」を開くと、IAP からの認証履歴が表示されていますので、クリックすると詳細を確認することができます。





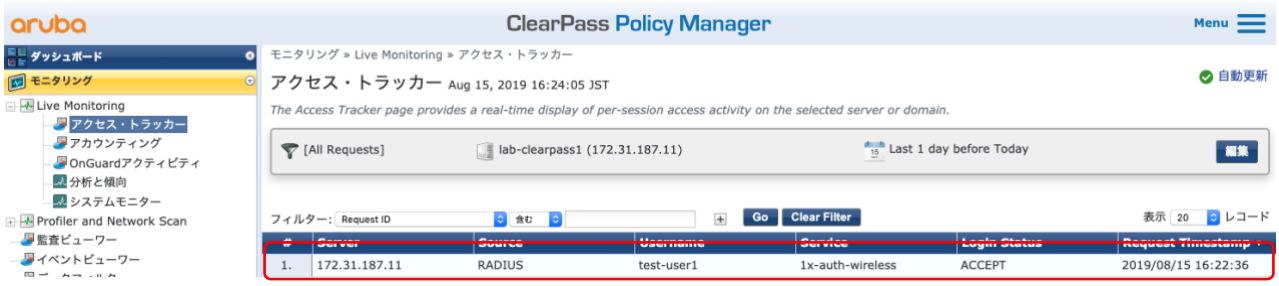
3) IAP の「ダッシュボード」>「クライアント」でも接続されていることが確認できます。



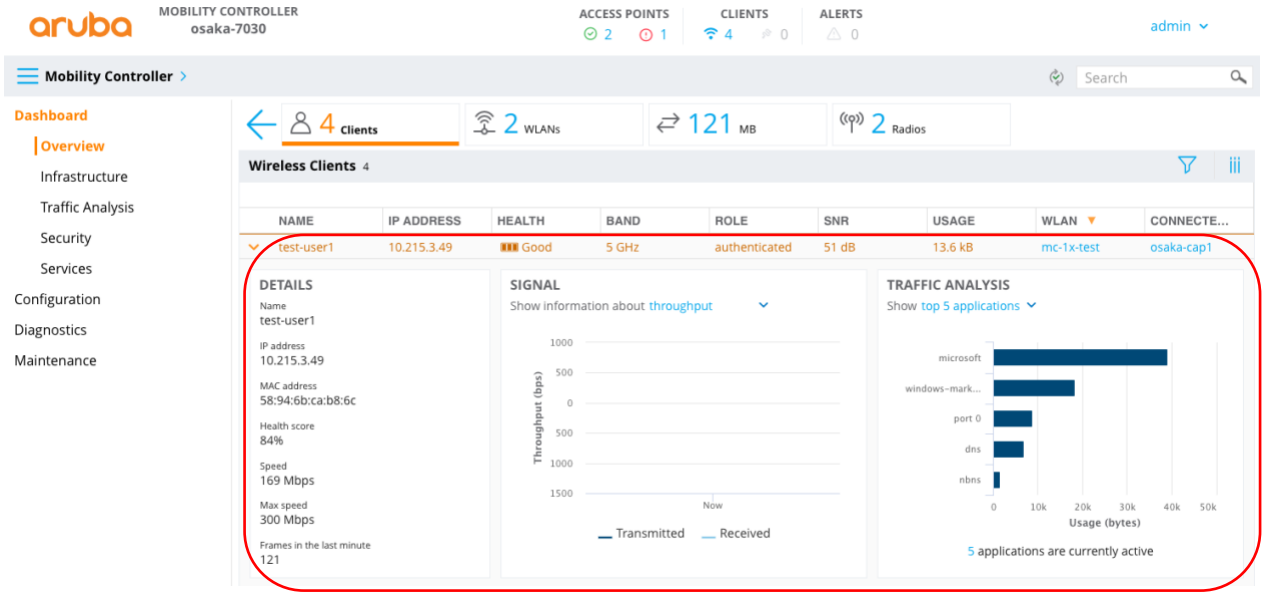
(3) 動作確認(Aruba Mobility Controller の場合)

1) クライアントを SSID に接続します。

2) 接続ができたら ClearPass の「モニタリング」>「Live Monitoring」>「アクセス・トラッカー」を開くと、コントローラーからの認証履歴が表示されていますので、クリックすると詳細を確認することができます。



3) コントローラーの「Dashboard」>「Overview」>「Clients」でも接続されていることが確認できます。



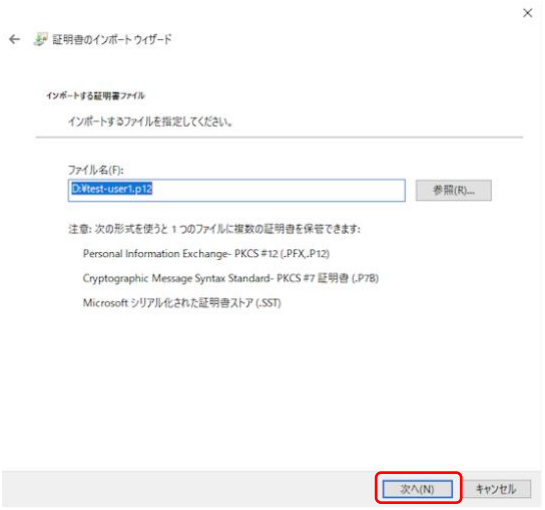
6.1.8 [参考]Windows 端末でクライアント証明書をコンピュータストアにインストールして認証する場合

Windows クライアントにおいて通常のコンピュータ認証はクライアントが AD へ参加していることが前提となりますが、クライアント証明書をユーザーでなく、ローカルコンピュータにインストールしてコンピューター認証のような対応を行いたい場合の設定例を説明します。

(1) Windows10 クライアントの設定

1) エクスポートした証明書を認証する端末にコピーし、ダブルクリックすると証明書のインポートウィザードが開始されます。「現在のユーザー」を選択し「次へ」をクリックします。

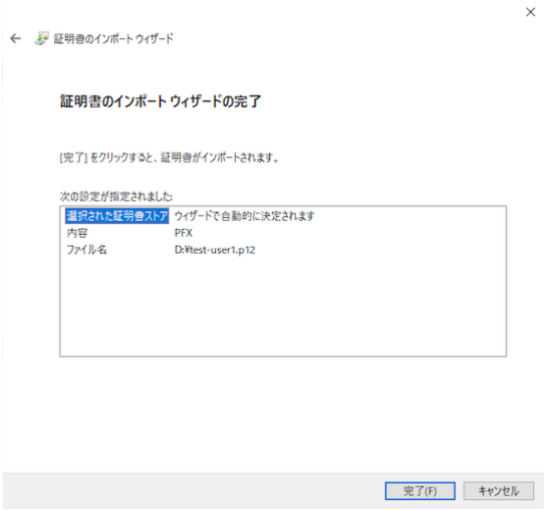
2) インポートするファイルが正しいことを確認して「次へ」をクリックします。



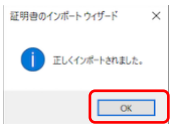
3) クライアント証明書をエクスポートした時に設定したパスフレーズをパスワードの欄に入力して「次へ」をクリックします。

4) そのまま「次へ」をクリックします。

5) 「完了」をクリックします。



6) インポートが完了するので「OK」をクリックして終了します。



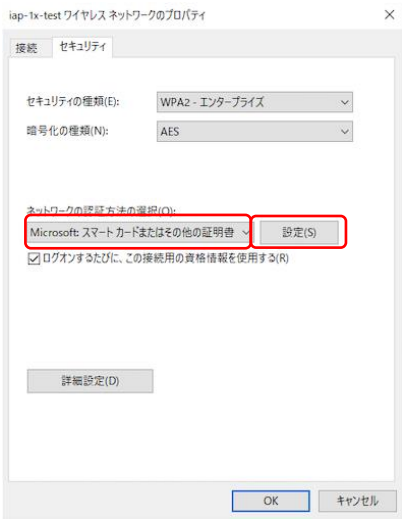
7) 「コントロールパネル」>「ネットワークとインターネット」>「ネットワークと共有センター」を開き、「新しい接続またはネットワークのセットアップ」をクリックします。

8) 「ワイヤレスネットワークに手動で接続します」を選択して「次へ」をクリックします。

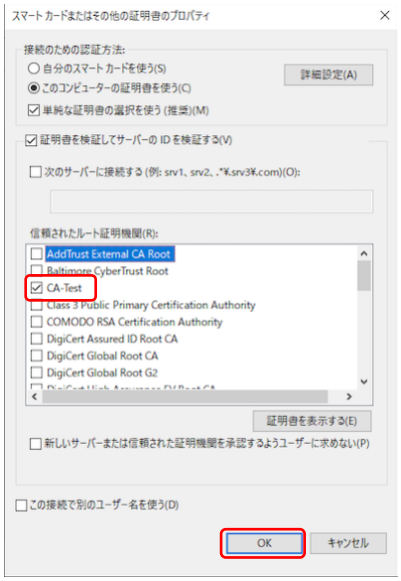
9) ネットワーク名に接続する SSID 名を入力し、セキュリティの種類で「WPA2-エンタープライズ」を選択して「次へ」をクリックします。

10) 「接続の設定を変更します」をクリックします。

11) ワイヤレスネットワークのプロパティが表示されますので、ネットワークの認証方法の選択を「Microsoft: スマートカードまたはその他の証明書」にして「設定」をクリックします。



12) インストールした証明書にチェックを入れ「OK」をクリックします。

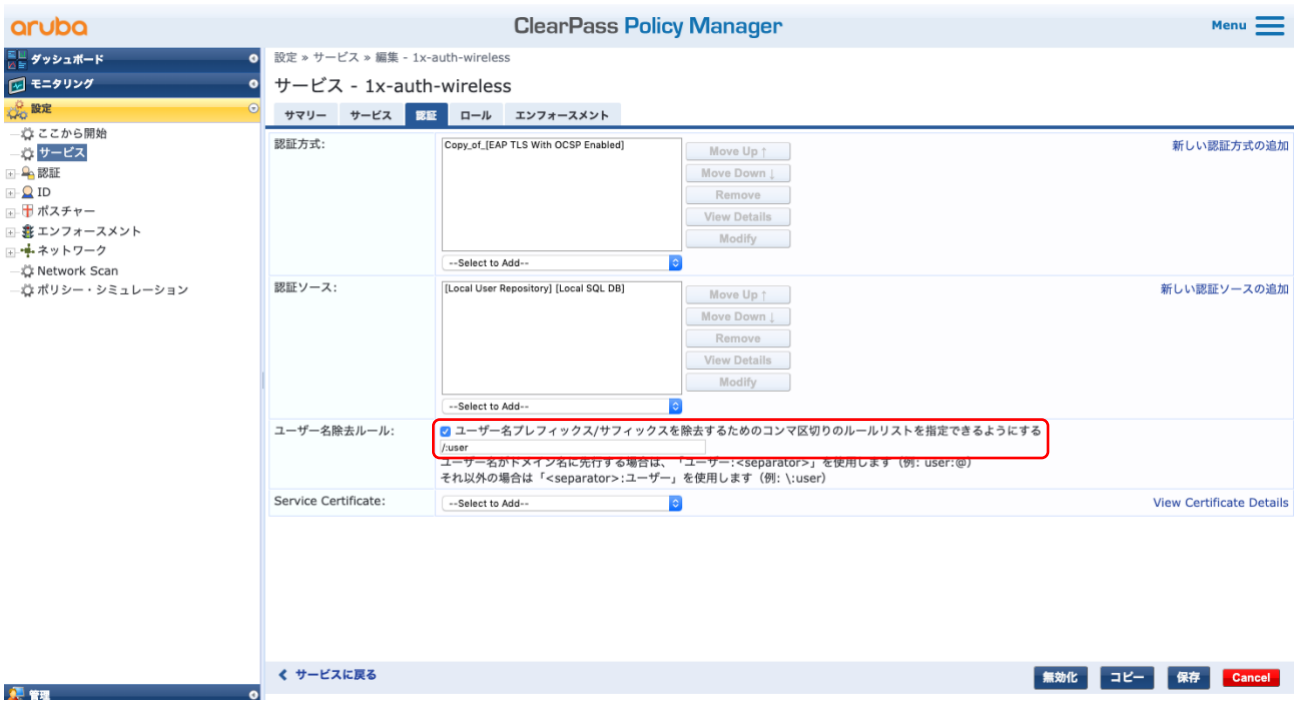


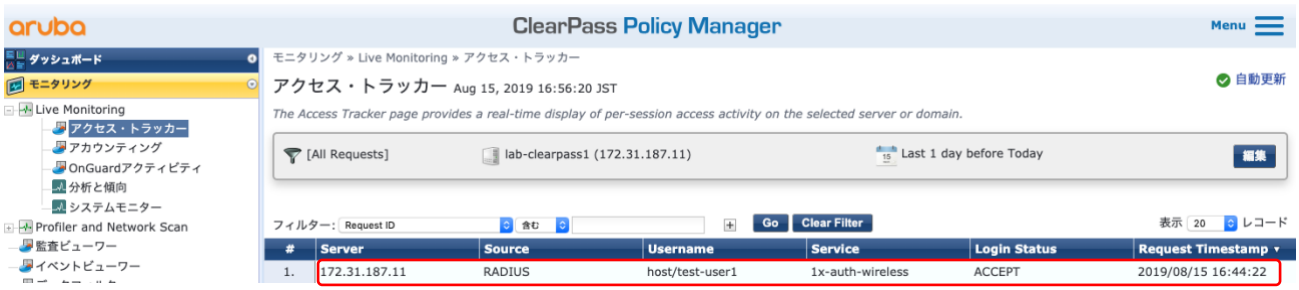
13) ワイヤレスネットワークのプロパティに戻るので、「詳細設定」をクリックします。

14) 「認証モードを指定する」にチェックを入れ、「ユーザー認証」を選択して「OK」をクリックします。ワイヤレスネットワークのプロパティに戻るので「OK」をクリックして閉じます。

(2) ClearPass の設定

Windows クライアントでコンピューターの認証を設定すると、認証時のユーザー名に"host/"が付加されて認証リクエストが送信されてくるためローカルユーザー名と一致せず認証に失敗します。そのため、サービスの認証設定で下記のようにユーザー名除去ルールで"/:user"を設定することで、ClearPass の認証では"host/"が付加されてリクエストが来ても、ユーザー名部分のみで認証できるようになります。





6.2 クライアント証明書を手動発行する有線 LAN の 802.1X 認証(EAP-TLS)

6.2.1 ClearPass の認証局設定

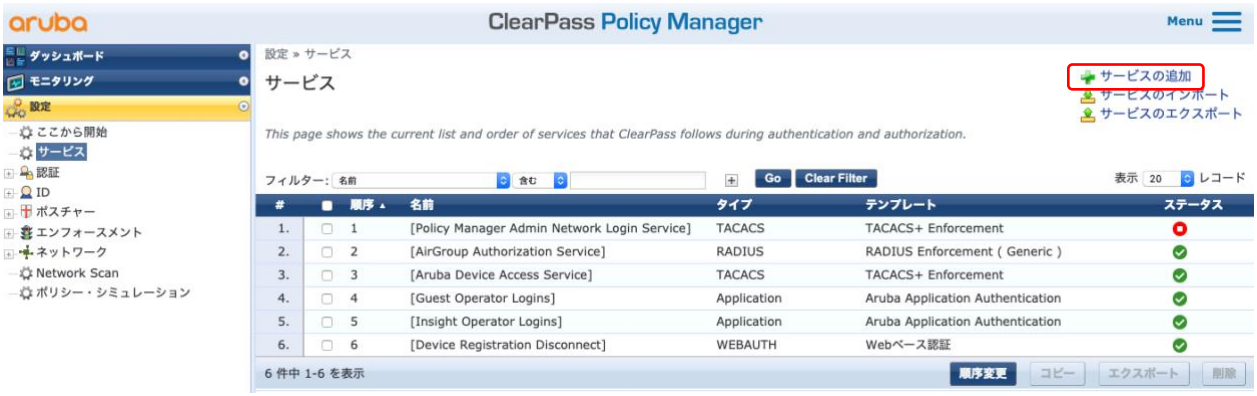
「無線 LAN の 802.1X 認証(EAP-TLS)」の「ClearPass の認証局設定」と同じですので、そちらを参考にして設定を行って下さい。

6.2.2 ClearPass の認証方式設定

「無線 LAN の 802.1X 認証(EAP-TLS)」の「ClearPass の認証方式設定」と同じですので、そちらを参考にして設定を行って下さい。

6.2.3 ClearPass のサービス設定

1) 「設定」>「サービス」を開き、「サービスの追加」をクリックします。



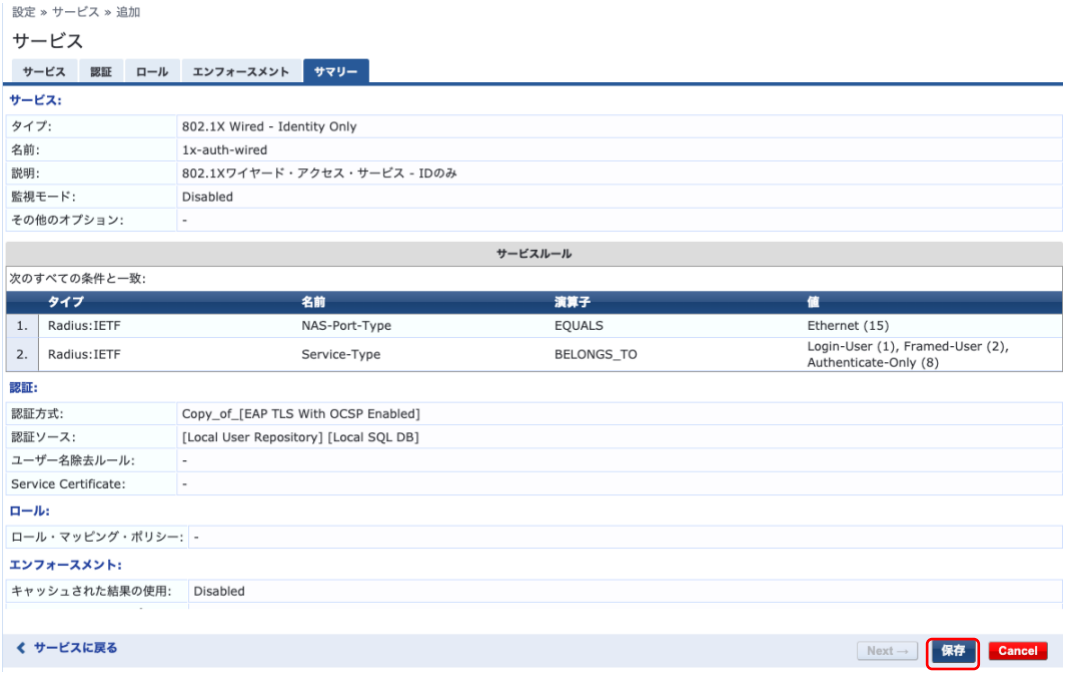
2) サービスのタイプで「802.1X Wireless – Identity Only」を選択し、任意の名前を入力して右下の「Next」 をクリックします。

3) 認証方式にデフォルトで入っている項目を全て Remove し、先程作成した「Copy_of_[EAP TLS With OCSP Enabled]」を追加、認証ソースにて「Select to Add」をクリックし、「Local User Repository」をクリックして追加し、右下の「Next」をクリック

4) ロールマッピングポリシーは特に選択せず、そのまま右下の「Next」をクリックします。

5) エンフォースメントポリシーはデフォルトの「Sample Allow Access Policy」が選択されていることを確認して右下の「Next」をクリックします。

6) 設定した内容のサマリーが表示されるので確認して右下の「保存」をクリックします。



6.2.4 ClearPass へのユーザー追加設定

「無線 LAN の 802.1X 認証(EAP-PEAP)」の「ClearPass へユーザー追加設定」と同じですので、そちらを参考にして設定を行って下さい。

6.2.5 ArubaOS Switch の設定

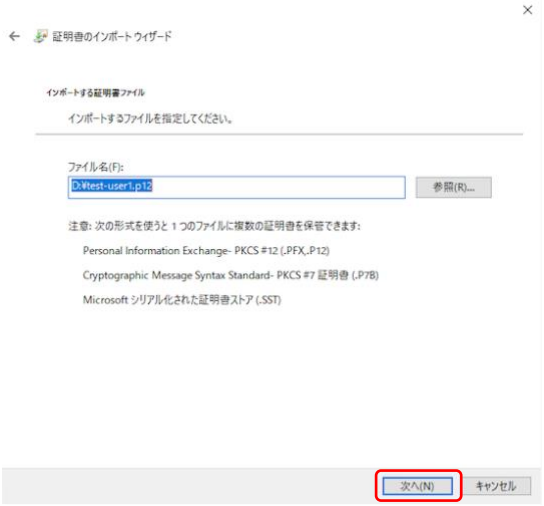
「有線 LAN の 802.1X 認証(EAP-PEAP)」の「ArubaOS Switch の設定」と同じですので、そちらを参考にして設定を行って下さい。

6.2.6 ArubaOS Switch での 802.1X 認証(EAP-TLS)動作確認

(1) Windows10 クライアントの設定

1) エクスポートした証明書を認証する端末にコピーし、ダブルクリックすると証明書のインポートウィザードが開始されます。「現在のユーザー」を選択し「次へ」をクリックします。

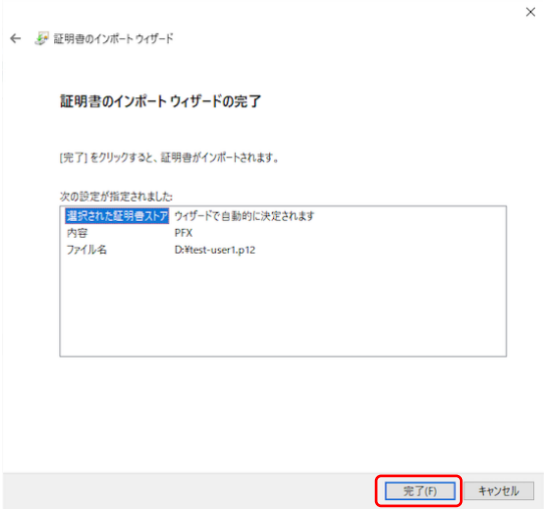
2) インポートするファイルが正しいことを確認して「次へ」をクリックします。



3) クライアント証明書をエクスポートした時に設定したパスフレーズをパスワードの欄に入力して「次へ」をクリックします。

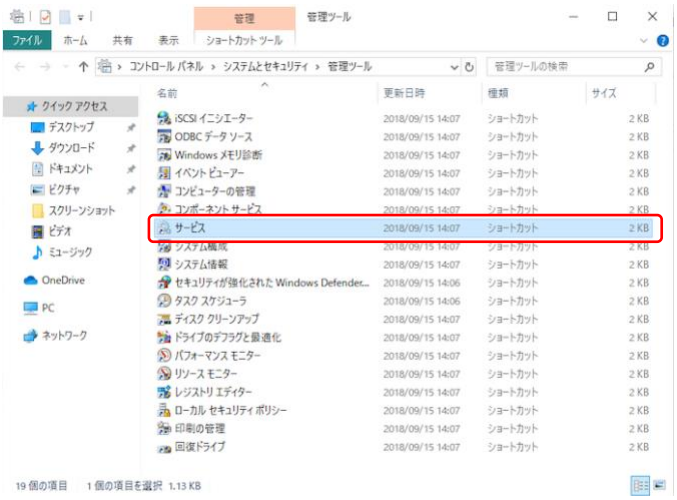
4) そのまま「次へ」をクリックします。

5) 「完了」をクリックします。

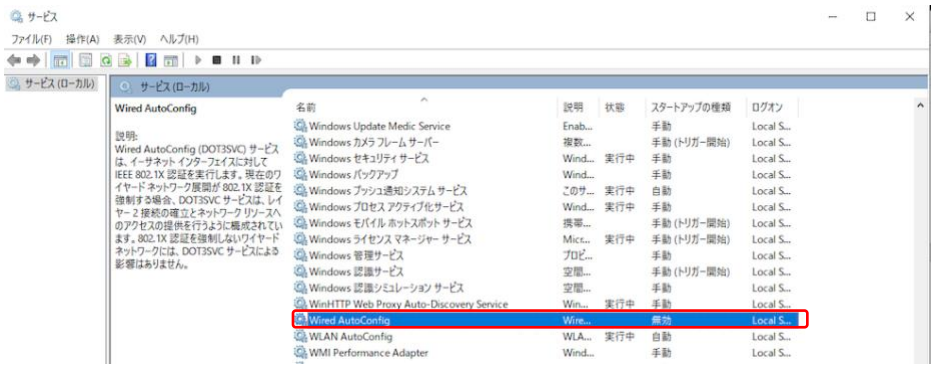


6) 「はい」をクリックしてインストールします。

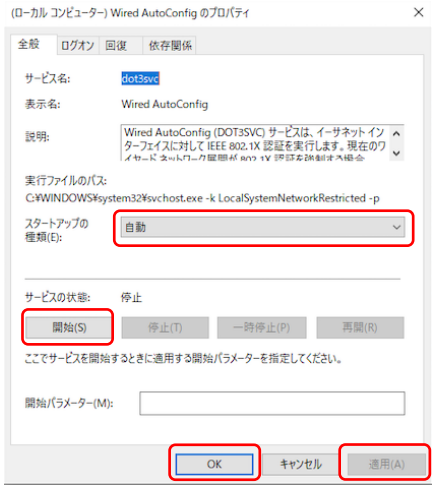
7) 「コントロールパネル」>「システムとセキュリティ」>「管理ツール」を開き、「サービス」をダブルクリックします。



8) 「Wired AutoConfig」をダブルクリックします。



9) スタートアップの種類を「自動」にして「適用」をクリックし、その後「開始」をクリックします。サービスの状態が実行中になったら、「OK」をクリックします。

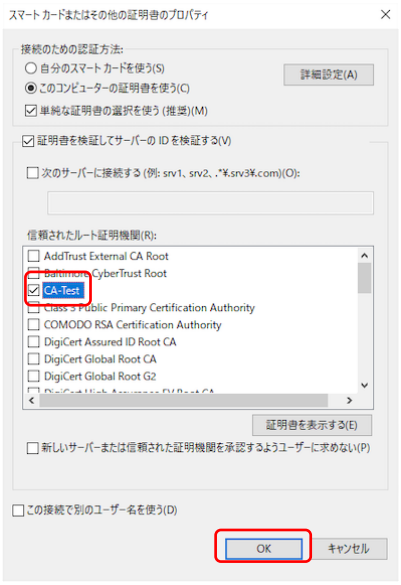


10) 「コントロールパネル」>「ネットワークとインターネット」>「ネットワークと共有センター」を開き、「アダプターの設定の変更」をクリックします。

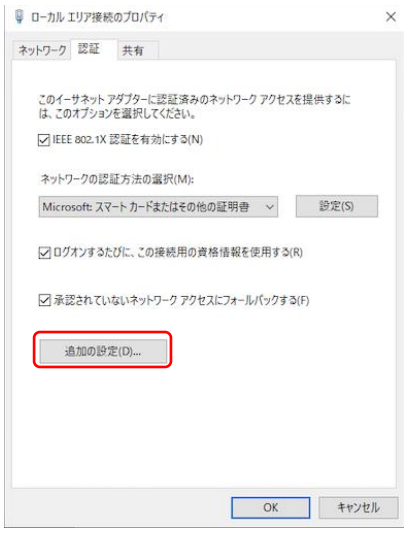
11) 「ローカルエリア接続」を右クリックしプロパティを表示します。

12) ローカルエリア接続のプロパティが表示されますので、ネットワーク認証方法で「Microsoft: スマートカードまたはその他の証明書」を選択し、「設定」をクリックします。

13) 保護された EAP のプロパティが表示されますので、インポートした証明機関にチェックを入れ「OK」をクリックします。



14) ローカルエリア接続のプロパティに戻るので、「追加の設定」をクリックします。

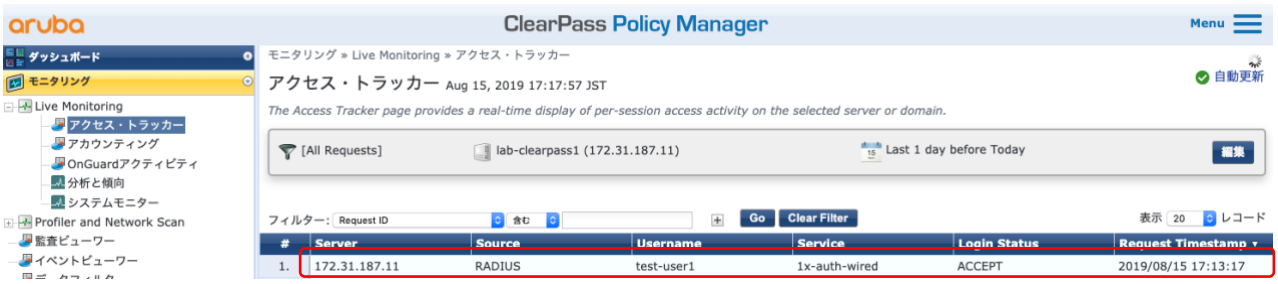


15) 「認証モードを指定する」にチェックを入れ、「ユーザー認証」を選択して「OK」をクリックします。ローカルエリア接続のプロパティに戻るので「OK」をクリックして閉じます。

(2) 動作確認

1) クライアントをスイッチの認証ポートに接続します。

2) 接続ができたら ClearPass の「モニタリング」>「Live Monitoring」>「アクセス・トラッカー」を開くと、スイッチからの認証履歴が表示されていますので、クリックすると詳細を確認することができます。



3) スイッチの方でも認証できていることが確認できます。

```
Aruba (config)# show port-access clients

 Port Access Client Status
  Port  Client Name   MAC Address       IP Address      User Role         Type  VLAN
  ----- ------------- ----------------- --------------- ----------------- ----- ---
  1     test-user1    68b599-fb4c88     10.215.3.227                      8021X 1

Aruba (config)# show port-access authenticator clients
 Port Access Authenticator Client Status

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No
  Use LLDP data to authenticate [No] : No
  Dot1X EAP Identifier Compliance [Disabled] : Disabled

  Port  Client Name           MAC Address       IP Address      Client Status
  ----- --------------------- ----------------- --------------- --------------------
  1     test-user1            68b599-fb4c88     10.215.3.227    Authenticated
```

6.3 クライアント証明書及びネットワーク設定の自動発行型無線 LAN の 802.1X 認証(EAP-TLS)

前セクションでは ClearPass Onboard の認証局機能を使って、手動でクライアント証明書を発行して認証を行いましたが、本章では Onboard を使って端末にクライアント証明書及びネットワーク設定を自動発行する手順について説明します。なお、本設定を行うには Onboard ライセンスが必要です。

6.3.1 ClearPass の認証局設定

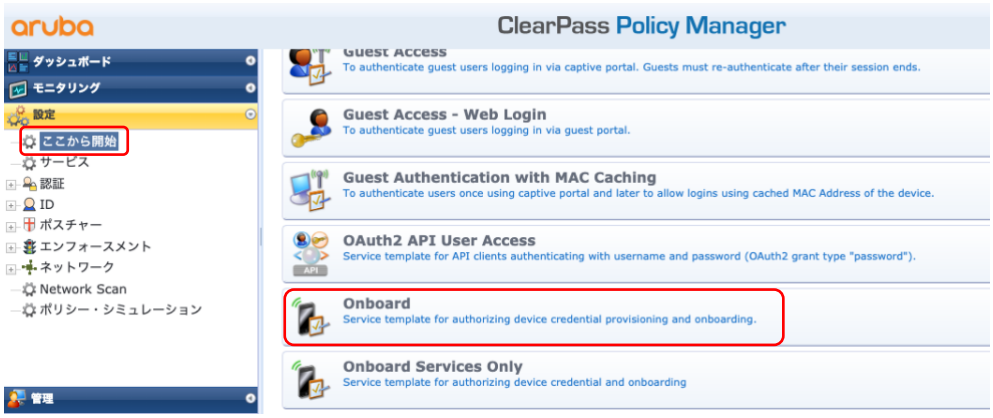
「無線 LAN の 802.1X 認証(EAP-TLS)」の「ClearPass の認証局設定」と同じですので、そちらを参考にして設定を行って下さい。

6.3.2 ClearPass の認証方式の設定

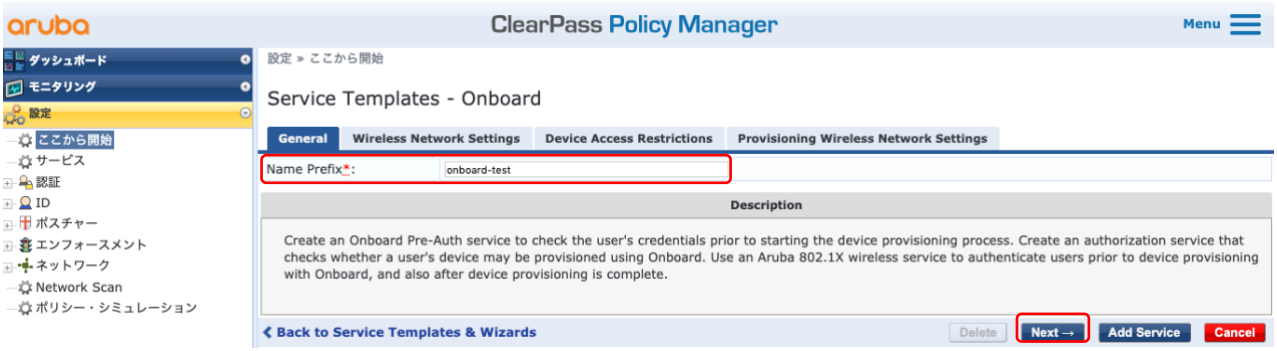
「無線 LAN の 802.1X 認証(EAP-TLS)」の「ClearPass の認証方式設定」と同じですので、そちらを参考にして設定を行って下さい。

6.3.3 Onboard 用サービスの作成

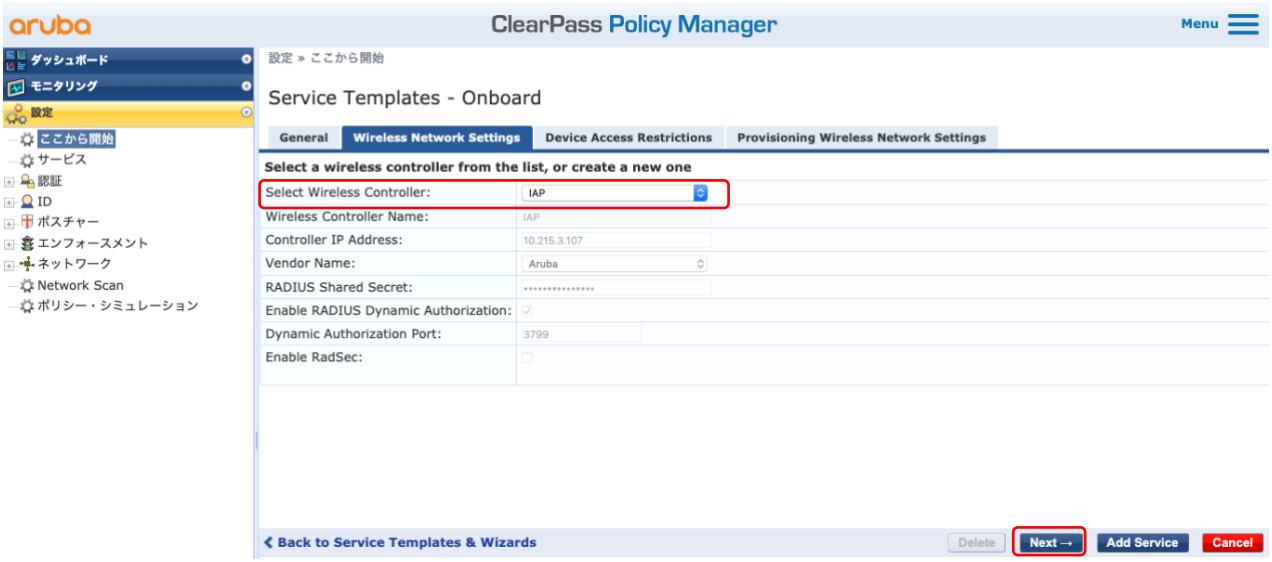
1) 「設定」>「ここから開始」を開き、「Onboard」をクリックします。



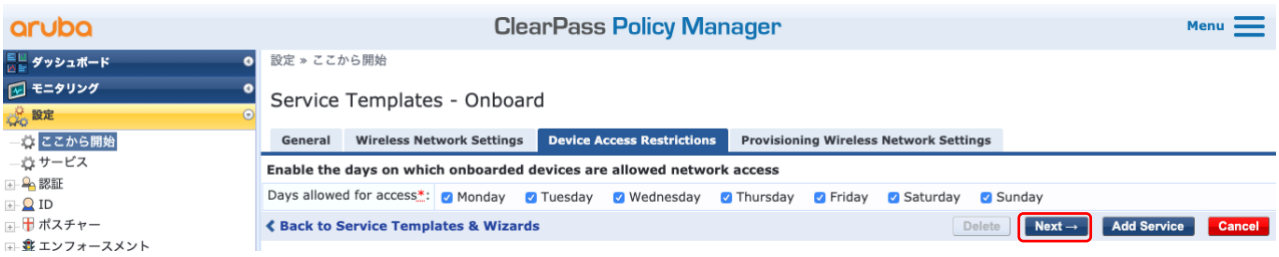
2) 本ウィザードで Onboard に関係するサービスが作成されますので、その頭につける任意の名前を入力して、「Next」をクリックします。



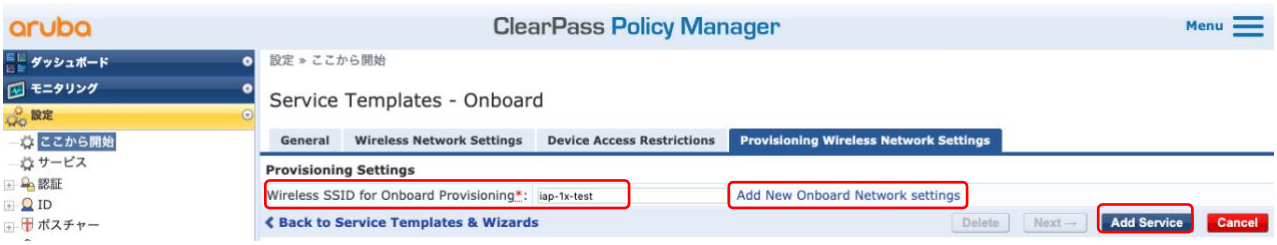
3) RADIUS クライアントとして登録されているネットワーク機器が選択できますので、連携する無線コントローラー(IAP もしくは物理コントローラーどちらも可能)を選択し「Next」をクリックします。(もし登録されていない場合は必要なパラメーターを入力して新規登録するか、「RADIUS クライアントの登録」を参考に設定を行って下さい。)登録されているコントローラーを選択すると必要なパラメーターは自動入力されます。



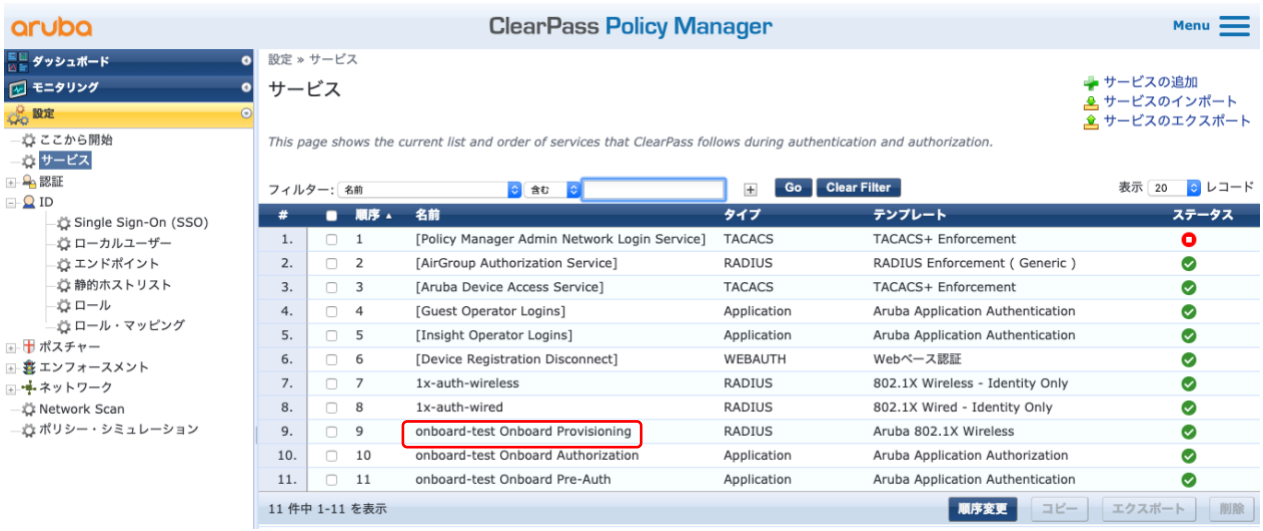
4) そのまま「Next」をクリックします。



5) 最終的に端末が接続する SSID 名(802.1X 認証を行なって接続する SSID)を入力し、「Add New Onboard setting」をクリックすると別ウィンドウ(別タブ)に Onboard の設定画面が開きますが、一旦こちらの画面に戻り「Add Service」をクリックします。



6) サービスが自動的に 3 つ作成されますので、作成した「xxx Onboard Provisioning」をクリックします。



7) 認証タブへ進み、認証方式に「ClearPass の認証方式設定」で作成した”Copy_of_[EAP TLS With OCSP Enabled]”を追加し最上位に移動します。デフォルトで入っている”[EAP TLS With OCSP Enabled]”は削除します。認証ソースにて、”[Local User Repository]”を追加し最上位に移動します。デフォルトで入っている”[Guest Device Repository]”は削除し、「保存」をクリックします。

8) 同様に「xxx Onboard Authorization」の認可タブの認可ソースも”[Local User Repository]”を追加し、デフォルトで入っている”[Guest Device Repository]”は削除し、「保存」をクリックします。

9) また同様に「xxx Onboard Pre-Auth」の認証タブの認証ソースも”[Local User Repository]”を追加し、デフォルトで入っている”[Guest Device Repository]”は削除し、「保存」をクリックします。

6.3.4 ネットワーク設定の作成

1) 1 つ前の手順で開いた Onboard の設定画面を表示します。右上の「新しいネットワークを作成します」をクリックします。

2) 名前に任意のネットワーク設定名、SSID に最終的に端末が接続する SSID 名(802.1X 認証を行なって接続する SSID)を入力して「信頼」をクリックします。

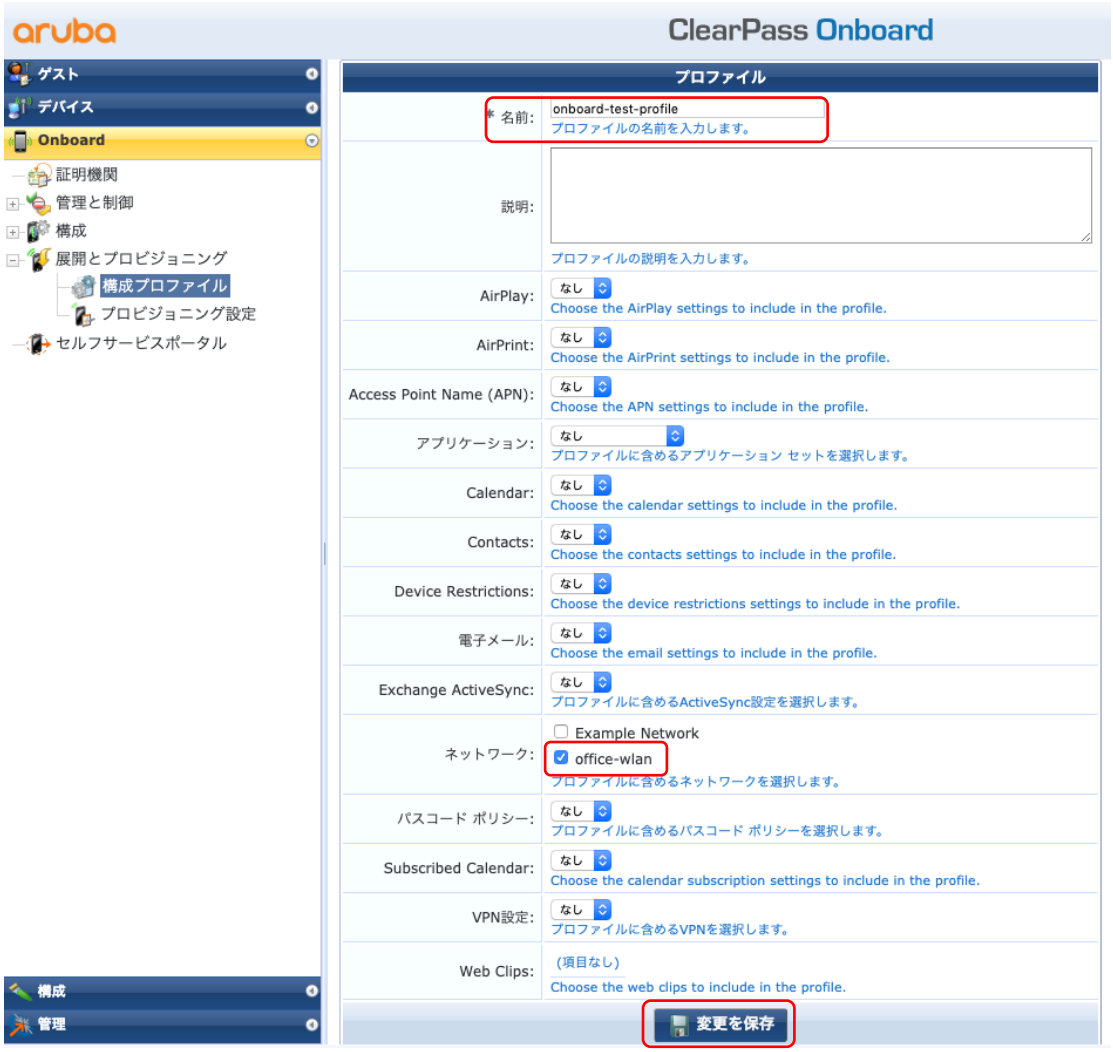
3) Onboard の対象端末に iOS 端末が含まれる場合は、Configure Trusted Servers を「Manually configure certificate trusted servers」に設定して「設定を保存」をクリックします。iOS 端末が含まれない場合は、そのまま「設定を保存」をクリックします。

4) ネットワーク設定が保存されます。

6.3.5 構成プロファイルの作成

1) 「Onboard」>「展開とプロビジョニング」を開き、「新しい構成プロファイルを作成します」をクリックします。

2) 名前に任意の構成プロファイル名を入力し、作成したネットワーク設定にチェックを入れ、「変更を保存」をクリックします。



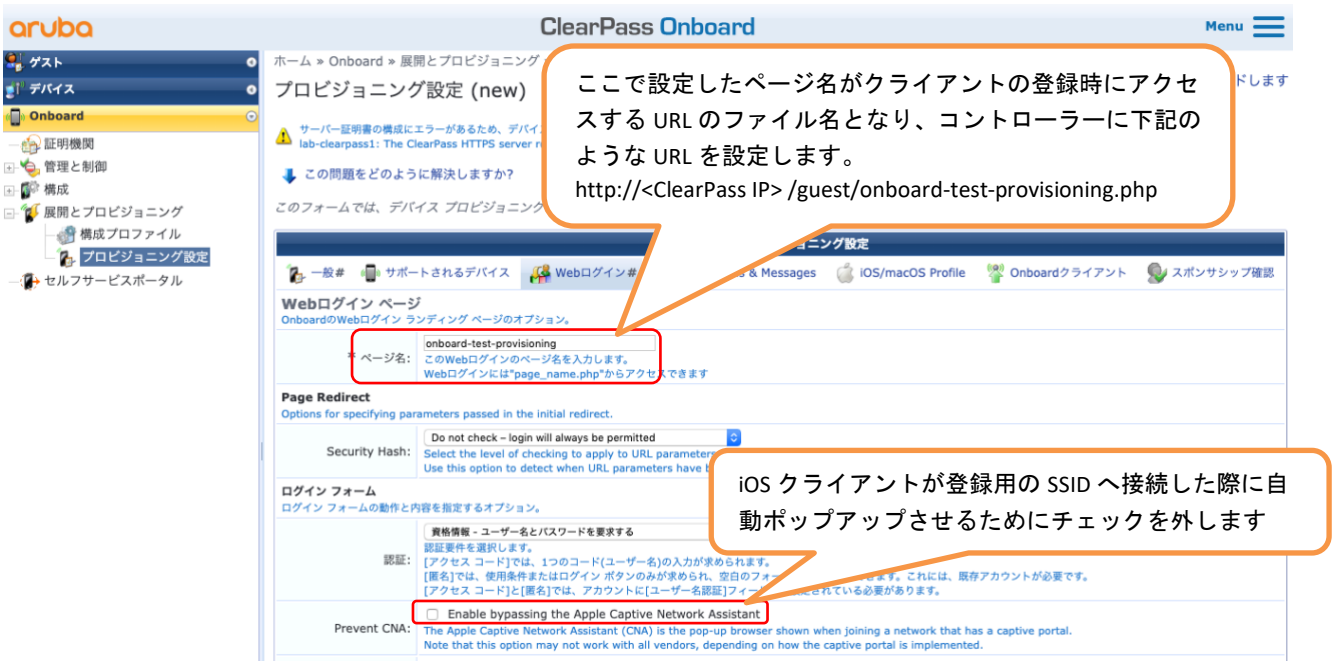
3) 構成プロファイルが保存されます。

6.3.6 プロビジョニング設定の作成

1) 「Onboard」>「展開とプロビジョニング」を開き、「新しいプロビジョニング設定を作成します」をクリックします。

2) 名前に任意のプロビジョニング設定名、組織に任意の名前を入力し、識別情報では作成した認証局を選択します。構成プロファイルは作成したプロファイルを選択し、デバイス最大数にユーザーあたりの証明書発行数を設定して、作成したネットワーク設定にチェックを入れ、上部の「Web ログイン」をクリックします。

3) サポートされるデバイスではそのまま「次へ」をクリックし、Web ログインではページ名に任意の名前を入力し、iOS 端末を Onboard で使う場合は「Enable bypassing the Apple Captive Network Assistant」のチェックを外し、上部の「Onboard クライアント」をクリックします。



4) Onboard クライアントでは、プロビジョニングアドレスに「管理ポートの IP アドレス」を選択し、証明書の検証を「この Web サーバーの証明書を検証しません」にして「変更を保存」をクリックします。

5) プロビジョニング設定が保存されます。

6.3.7 HTTPS Provisioning Error への対応(iOS 端末向け)

iOS クライアントをプロビジョニングする場合、HTTPS を使用すると iOS が信頼する認証局が署名した証明書が必要となります。実際には HTTPS が推奨となりますが、検証時はこれを回避するために、HTTPS の適用を無効にします。

参考 URL : https://support.apple.com/ja-jp/HT204132

1) ClearPass Guest において「構成」>「認証」を開き、「ゲストアクセスへの HTTPS の適用」のチェックを外して「変更を保存」をクリックします。

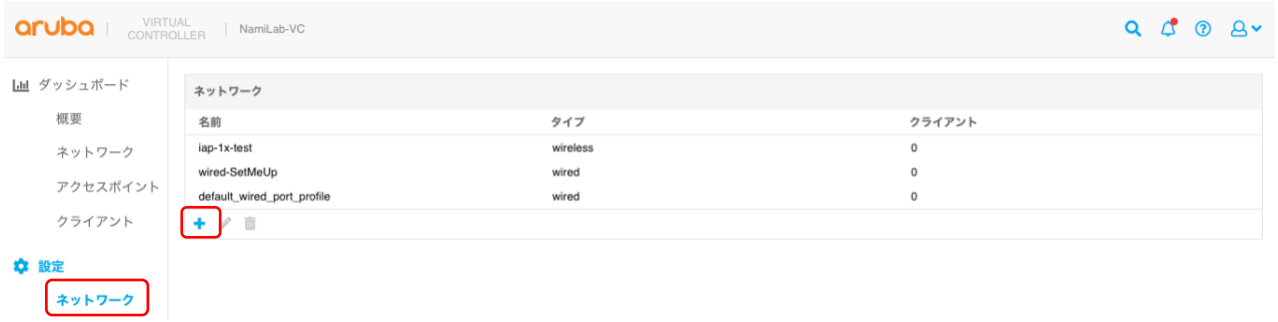
6.3.8 Aruba IAP 及び Aruba Mobility Controller の認証設定

「無線 LAN の 802.1X 認証(EAP-PEAP)」の「Aruba IAP の設定」及び「Aruba Mobility Controller の設定」と同じですので、そちらを参考にして設定を行って下さい。

6.3.9 Aruba IAP での登録用 SSID の設定

IAP においてクライアントへ証明書を自動発行するために接続する登録用 SSID の設定を行います。

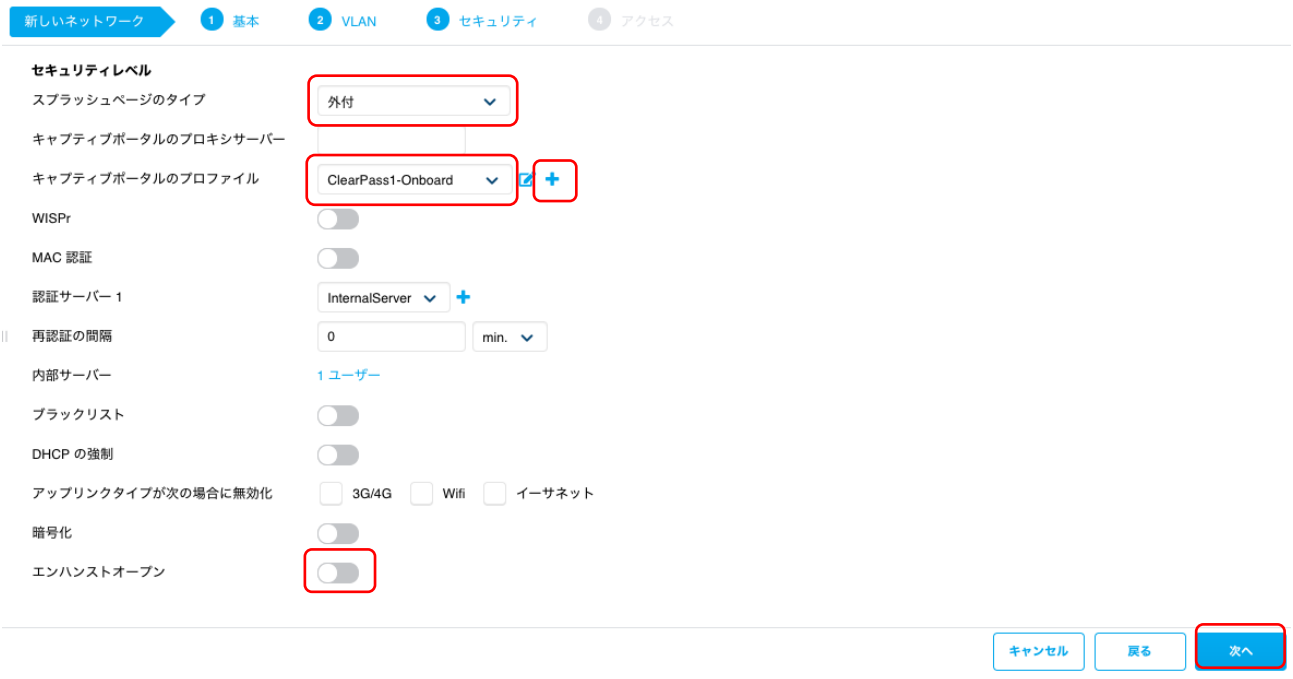
1) 「設定」>「ネットワーク」を開き、「+」をクリックします。



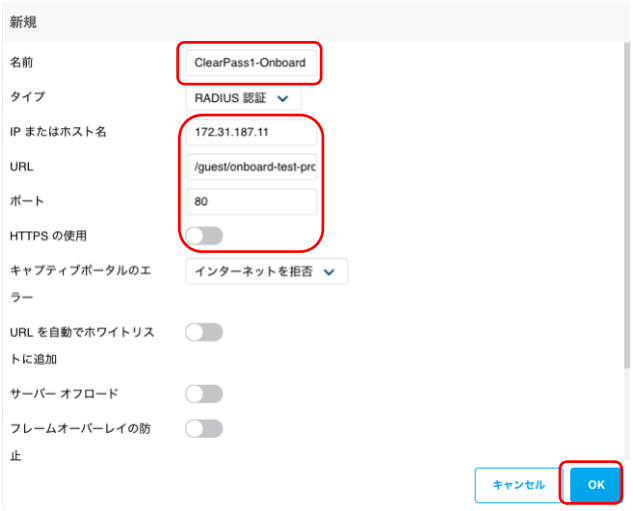
2) SSID の名前を入力し、主な用途を「ゲスト」にして「次へ」をクリックします。

3) クライアント IP と VLAN の割り当てはデフォルトのまま、「次へ」をクリックします。

4) スプラッシュページのタイプを「外付」にして、キャプティブポータルのプロファイルの「+」をクリックして認証サーバーを追加し、エンハンスドオープンをオフにして「次へ」をクリックします。



認証サーバー追加の設定を行うには任意の名前、IP またはホスト名に ClearPass の IP アドレス、URL に Onboard で設定したページ名の URL の IP またはホスト名以降(URL が" http://<ClearPass IP> /guest/onboard-test-provisioning.php "の場合は" /guest/onboard-test-provisioning.php"を貼り付け、今回 iOS 端末向けに HTTP で動作確認するため、ポートは 80、HTTPS の使用はオフにして「OK」をクリックします。



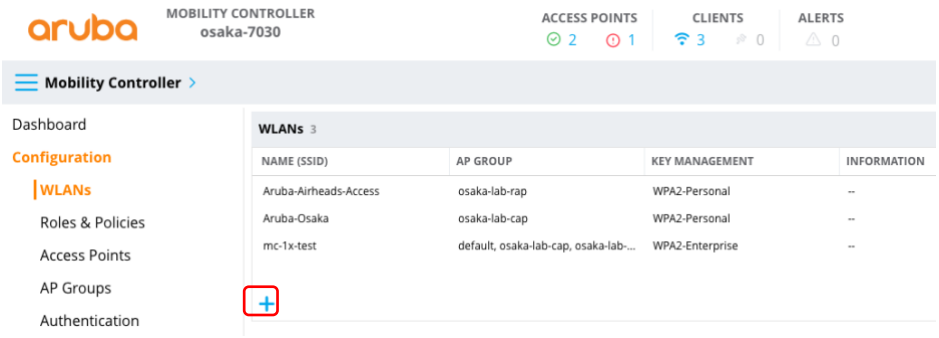
5) アクセスルールはデフォルトのまま「終了」をクリックします。

6.3.10 Aruba Mobility Controller での登録用 SSID の設定

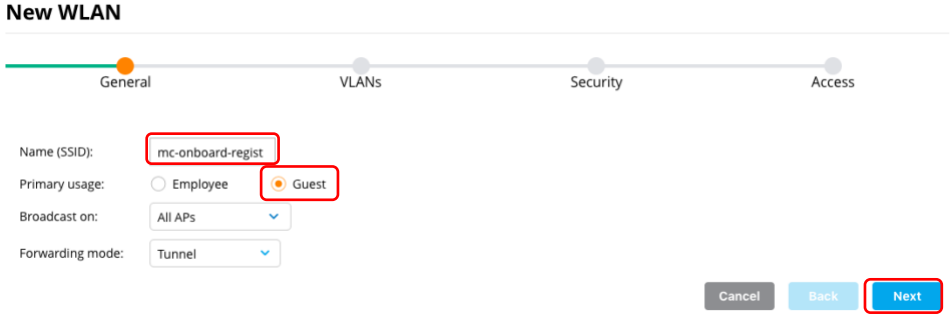
Mobility Controller においてクライアントへ証明書を自動発行するために接続する登録用 SSID の設定を行います。

※本説明は AOS8 Standalone MC で行なっております。

1) SSID の作成を行います。「Mobility Controller」>「Configuration」>「WLANs」と開き、「+」をクリックします。

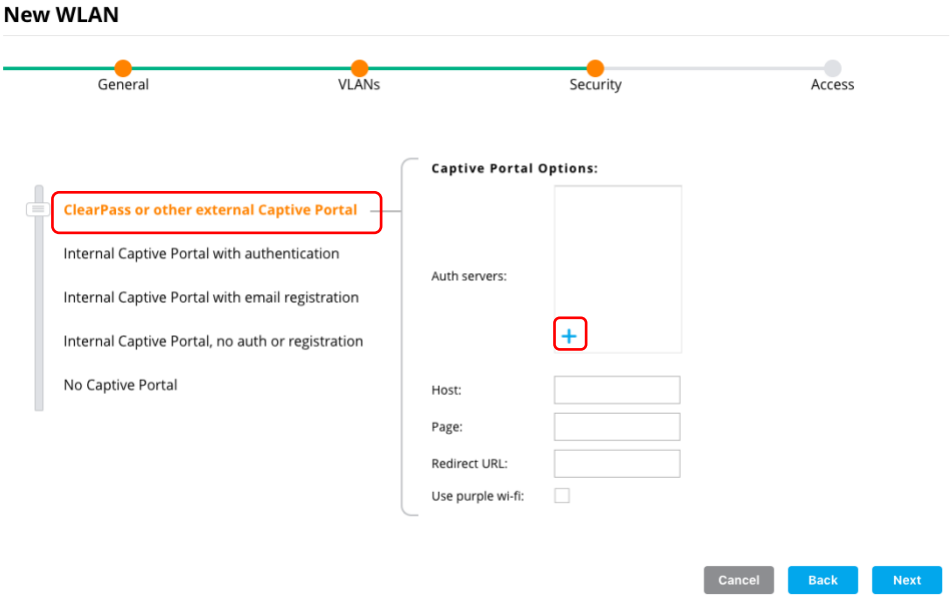


2) SSID の名前を入力し、Primary usage を「Guest」にして、「Next」をクリックします。

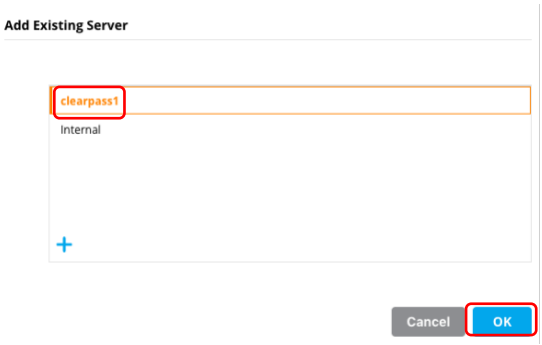


3) VLAN は特に指定がなければそのまま「Next」をクリックします。

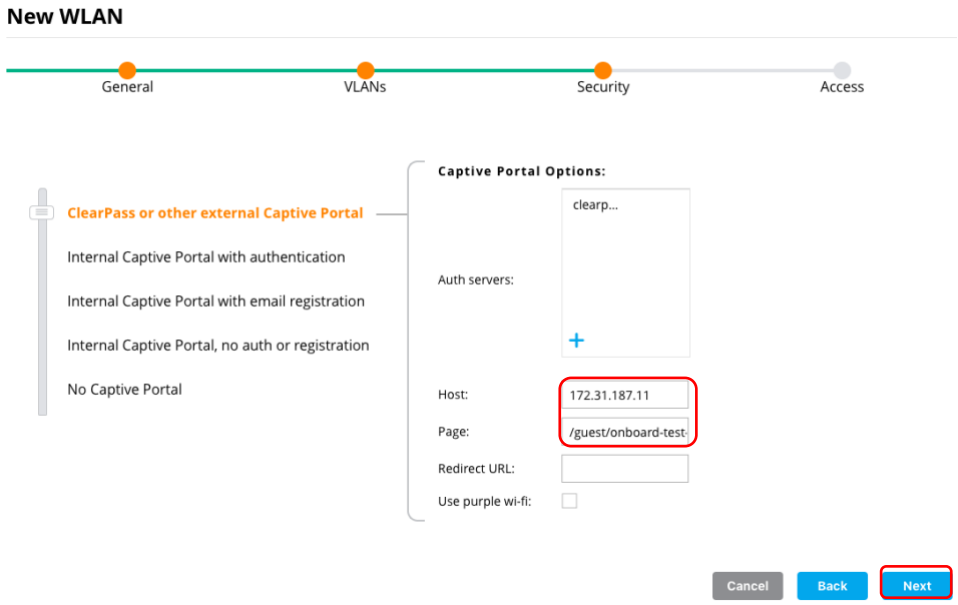
4) 左の選択肢より「ClearPass or other external Captive Portal」を選択し、Auth Servers の「+」をクリックします。



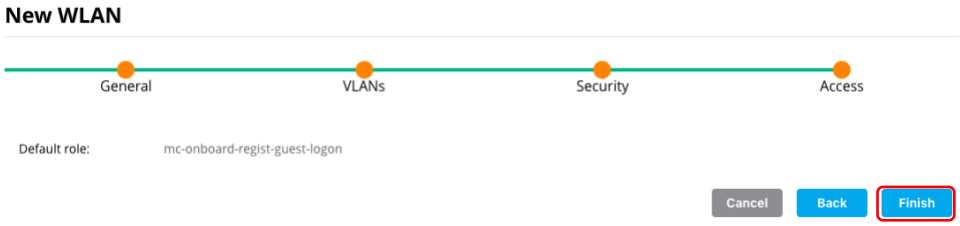
5) 「無線 LAN の 802.1X 認証(EAP-PEAP)」の「Aruba Mobility Controller の設定」で既に ClearPass が認証サーバーとして登録されていれば一覧に表示されていますので、選択して「OK」をクリックします。もし作成されていなければ「無線 LAN の 802.1X 認証(EAP-PEAP)」の「Aruba Mobility Controller の設定」を参考についかを行なって下さい。



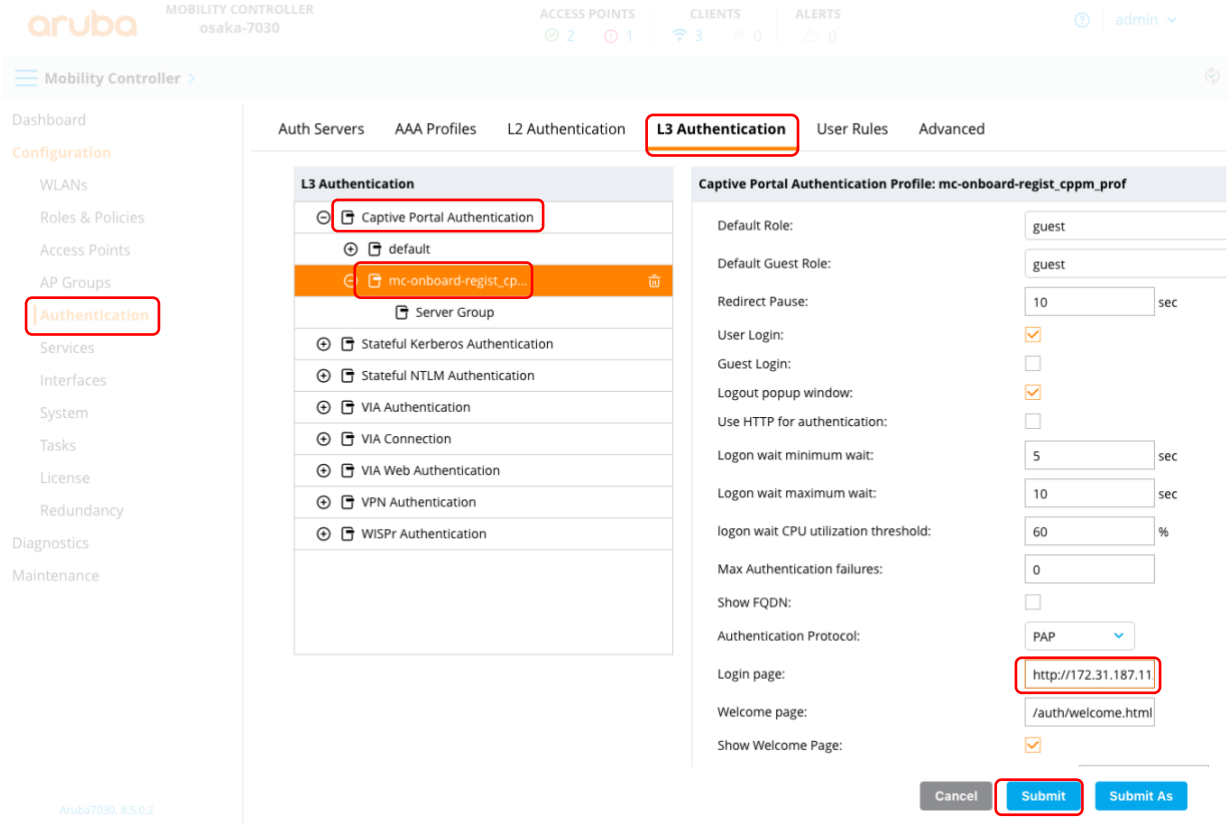
6) Host に ClearPass の IP アドレス、URL に Onboard で設定したページ名の URL の IP またはホスト名以降(URL が" http://<ClearPass IP> /guest/onboard-test-provisioning.php "の場合は" /guest/onboard-test-provisioning.php"を貼り付け「Next」をクリックします。



7) 「Finish」をクリックします。クリックしたら右上の「Pending Changes」>「Deploy Changes」とクリックして設定を反映します。



8) 今回 iOS 端末向けに HTTP で動作確認するため、「Mobility Controller」>「Configuration」>「Authentication」>「L3 Authentication」と開き、「Captive Portal Authentication」の作成した登録用 SSID の名前がついたプロファイルをクリックし、Login Page の URL が”https://～”となっているので”s”を削除し、”http://～”へ変更して「Submit」をクリックします。クリックしたら右上の「Pending Changes」>「Deploy Changes」とクリックして設定を反映します。

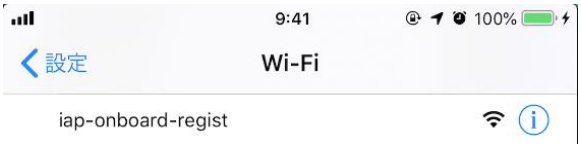


6.3.11 Aruba IAP での証明書発行及び 802.1X 認証(EAP-TLS)動作確認

(1) iOS の場合

本例では iPhone 7 Plus (iOS 12.4)を使用しています。

1) iPhone を登録用 SSID へ接続します。



2) ログイン画面が表示されますので、ユーザー名及びパスワードを入力して「ログイン」をクリックします。

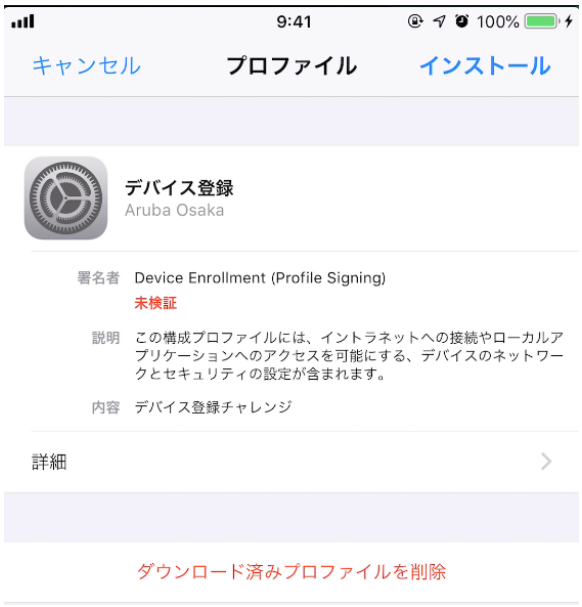
3) 「証明書のインストール」をクリックします。

4) 「プロファイルのインストール」をタップします。

5) 「閉じる」をタップします。

6) 「設定」>「一般」>「プロファイル」と進むと、「デバイス登録」がダウンロードされ一覧に表示されますのでタップします。

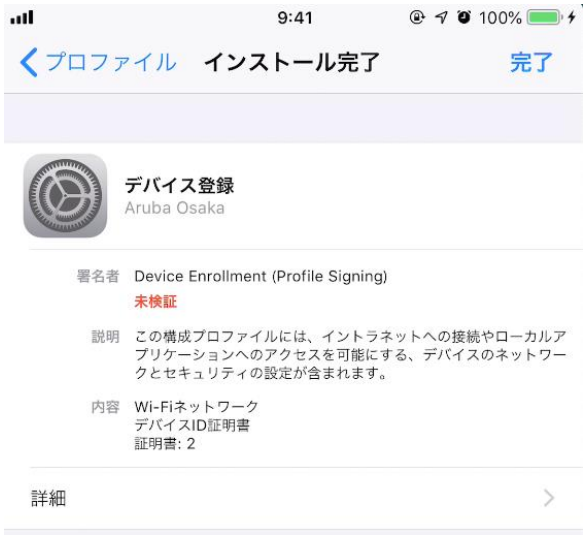
7) プロファイルのインストールが表示れますので、「インストール」をタップします。



8) パスコードの入力を求められますので入力します。警告が表示されますので「インストール」をタップします。確認を求められますので「インストール」をタップします。

9) 警告が表示されますので「インストール」をタップします。確認を求められますので「インストール」をタップします。

10) プロファイル、証明書のインストールが完了しますので「完了」をタップします。



11) 実際に利用する SSID に接続します。接続ができたら ClearPass の「モニタリング」>「Live Monitoring」>「アクセス・トラッカー」を開くと、IAP からの認証履歴が表示されていますので、クリックすると詳細を確認することができます。

12) IAP の「ダッシュボード」>「クライアント」でも接続されていることが確認できます。

13) ClearPass Onboard の「管理と制御」の「デバイスごとに表示」、「ユーザー名ごとに表示」、「証明書ごとに表示」で発行された証明書について確認することができます。(証明書の失効などもこちらから対応できます)

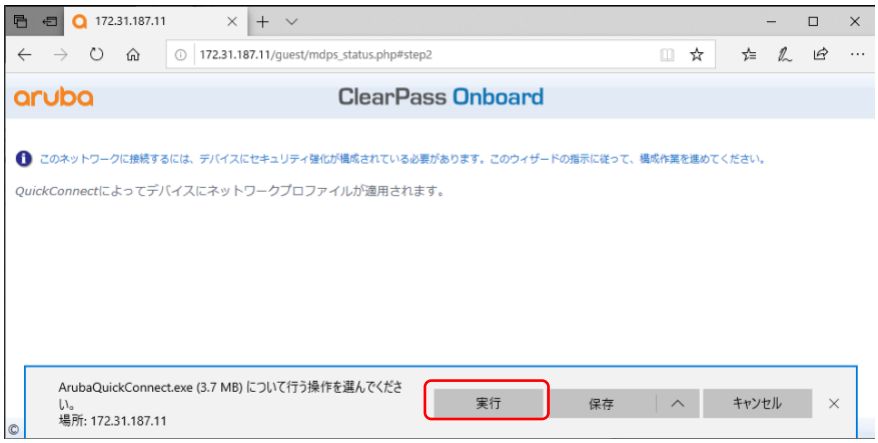
(2) Windows10 の場合

1) Windows10 クライアントを登録用の SSID へ接続します。

2) ログイン画面が表示されますので、ユーザー名及びパスワードを入力して「ログイン」をクリックします。

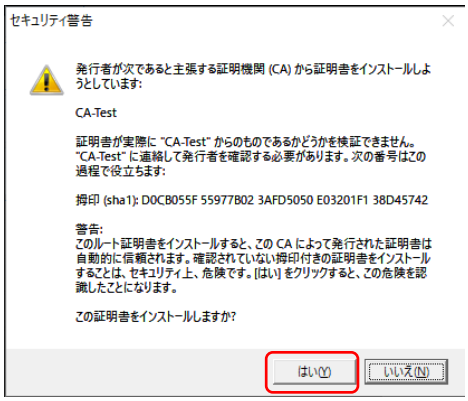
3) ログインに成功したら、「QuickConnect の起動」をクリックします。

4) 「実行」をクリックします。OS のセキュリティ設定によっては警告が表示される場合もありますが、「実行」をクリックして下さい。



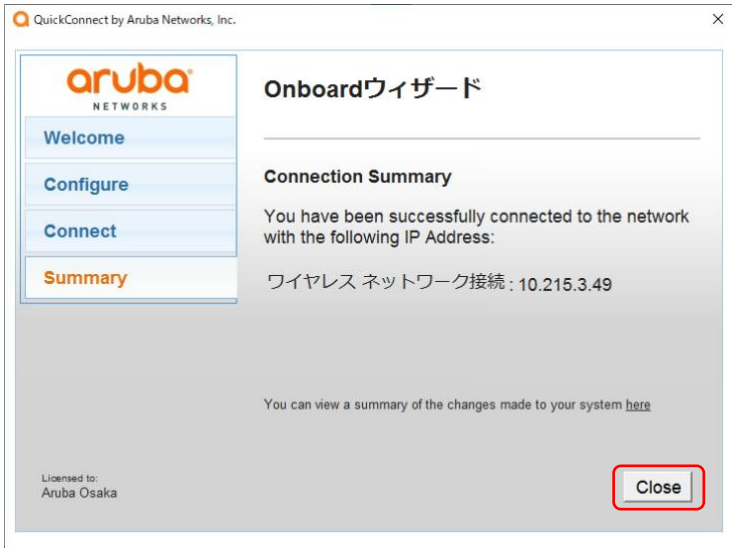
5) Onboard ウィザードが表示されます。「Next」をクリックします。

6) 証明書のインストールで警告が表示されますので「はい」をクリックします。

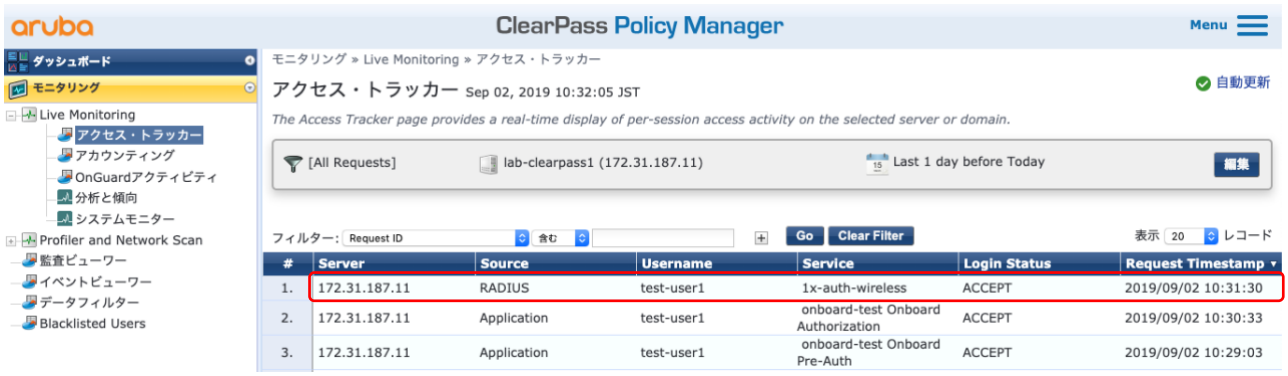


7) 証明書のインストール、無線接続の設定が完了となります。「Connect」をクリックします。

8) 実際に利用する SSID に接続され、証明書による認証が行われネットワークが利用できるようになります。「Close」をクリックします。



9) 接続ができたら ClearPass の「モニタリング」>「Live Monitoring」>「アクセス・トラッカー」を開くと、IAP からの認証履歴が表示されていますので、クリックすると詳細を確認することができます。



10) IAP の「ダッシュボード」>「クライアント」でも接続されていることが確認できます。

11) ClearPass Onboard の「管理と制御」の「デバイスごとに表示」、「ユーザー名ごとに表示」、「証明書ごとに表示」で発行された証明書について確認することができます。(証明書の失効などもこちらから対応できます)

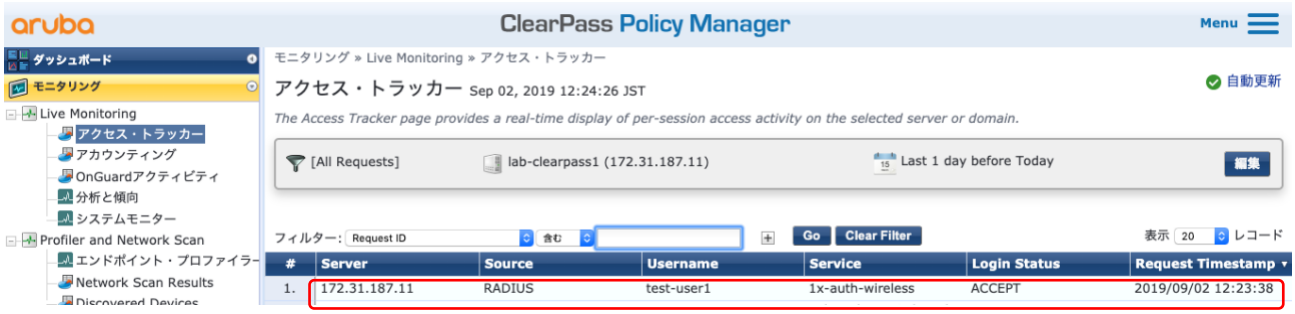
6.3.12 Aruba Mobility Controller での証明書発行及び 802.1X 認証(EAP-TLS)動作確認

(1) iOS の場合

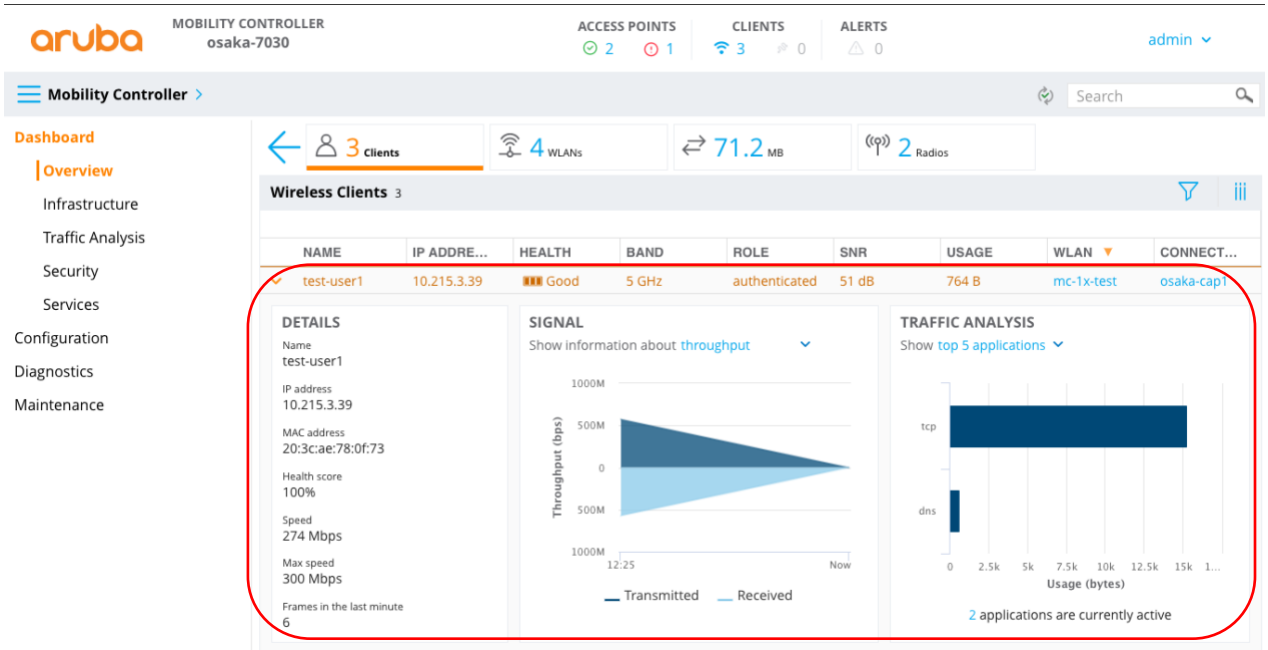
本例では iPhone 7 Plus (iOS 12.4)を使用しています。

1) クライアントの登録手順は「Aruba IAP での証明書発行及び 802.1X 認証(EAP-TLS)動作確認」の「iOS の場合」と同じですので、そちらを参考に実施して下さい。

2) 実際に利用する SSID に接続します。接続ができたら ClearPass の「モニタリング」>「Live Monitoring」>「アクセス・トラッカー」を開くと、コントローラーからの認証履歴が表示されていますので、クリックすると詳細を確認することができます。



3) コントローラーの「Dashboard」>「Overview」>「Clients」でも接続されていることが確認できます。

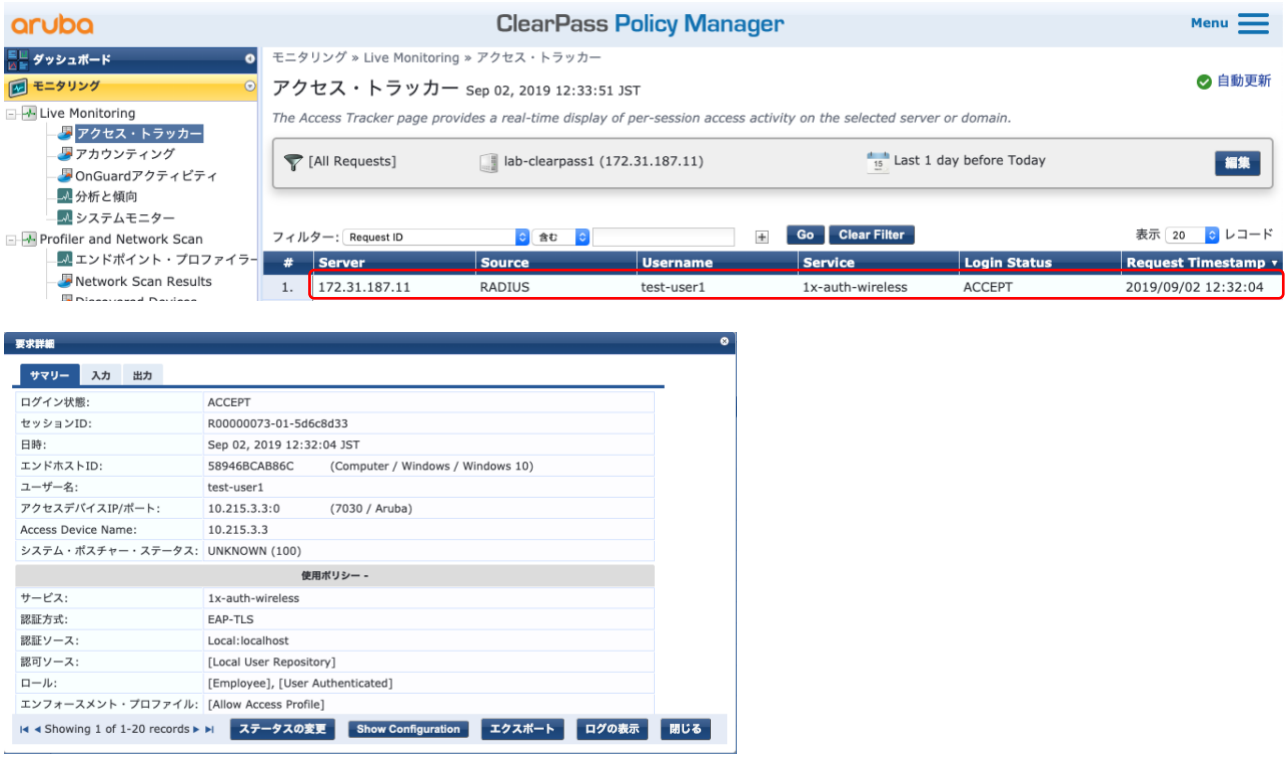


4) ClearPass Onboard の「管理と制御」の「デバイスごとに表示」、「ユーザー名ごとに表示」、「証明書ごとに表示」で発行された証明書について確認することができます。(証明書の失効などもこちらから対応できます)

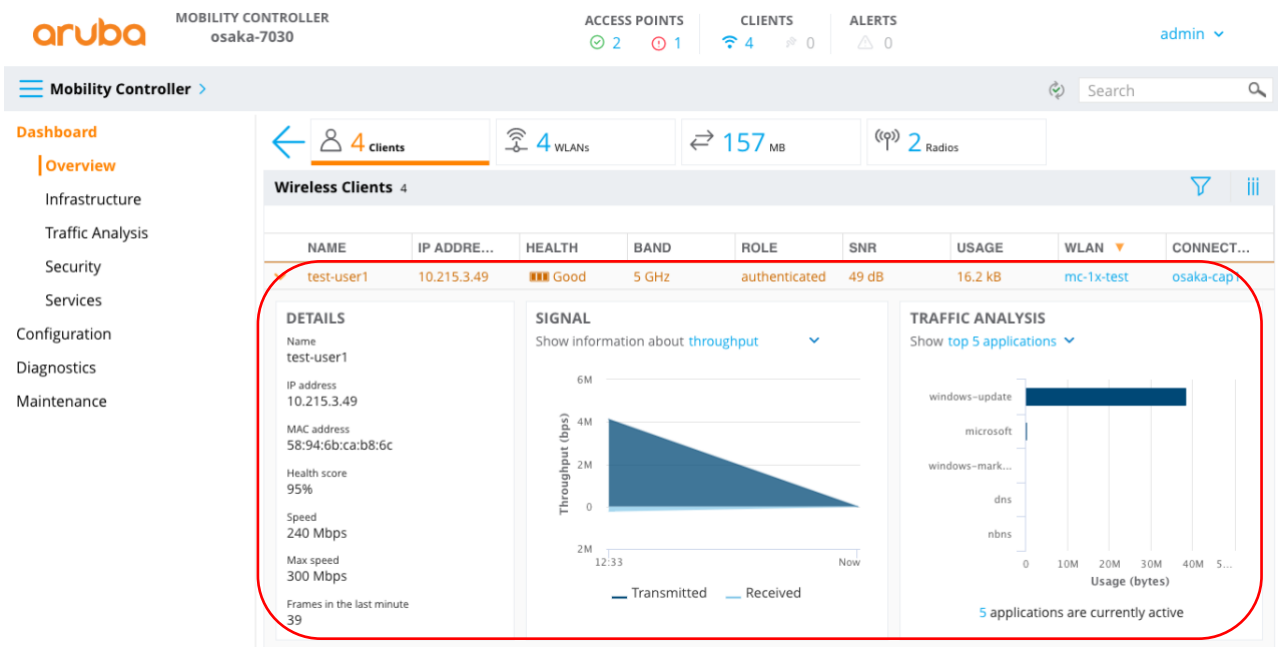
(2) Windows10 の場合

1) クライアントの登録手順は「Aruba IAP での証明書発行及び 802.1X 認証(EAP-TLS)動作確認」の「Windows10 の場合」と同じですので、そちらを参考に実施して下さい。

2) 実際に利用する SSID に接続します。接続ができたら ClearPass の「モニタリング」>「Live Monitoring」>「アクセス・トラッカー」を開くと、コントローラーからの認証履歴が表示されていますので、クリックすると詳細を確認することができます。



3) コントローラーの「Dashboard」>「Overview」>「Clients」でも接続されていることが確認できます。



4) ClearPass Onboard の「管理と制御」の「デバイスごとに表示」、「ユーザー名ごとに表示」、「証明書ごとに表示」で発行された証明書について確認することができます。(証明書の失効などもこちらから対応できます)