

NetAttest EPS

認証連携設定例

【連携機器】 MSM4xx シリーズ、MSM7xx シリーズ

【Case】 IEEE802.1x EAP-TLS 認証、VASCO ワンタイムパスワード認証

Rev1.0

株式会社ソリトンシステムズ

はじめに

本書について

本書は CA 内蔵 RADIUS サーバーアプライアンス NetAttest EPS と HP 社製 無線アクセスポイント、無線コントローラー MSM シリーズの IEEE802.1x EAP-TLS 環境での接続とゲストアクセス用ワンタイムパスワード認証(PAP)について、設定例を示したものです。設定例は管理者アカウントでログインし、設定可能な状態になっていることを前提として記述します。



表記方法

表記方法	説明
『 』	参照するドキュメントを示します。
「 」	参照する章、節、ボタンやメニュー名、強調する単語を示します。
[キー]	キーボード上のキーを表します。
[キー1]+[キー2]	[キー1]を押しながら[キー2]を押すことを表します。

表記方法(コマンドライン)

表記方法	説明
%, \$, >	一般ユーザーのプロンプトを表します。
#	特権ユーザーのプロンプトを表します。
[filename]	[] は省略可能な項目を示します。この例では、filename は省略してもよいことを示しています。

アイコンについて

アイコン	説明
	利用の参考となる補足的な情報をまとめています。
	注意事項を説明しています。場合によっては、データの消失、機器の破損の可能性があります。

画面表示例について

このマニュアルで使用している画面(画面キャプチャ)やコマンド実行結果は、実機での表示と若干の違いがある場合があります。

ご注意

本書は、当社での検証に基づき、NetAttest EPS 及び MSM4xx シリーズ、MSM7xx シリーズの操作方法を記載したものです。すべての環境での動作を保証するものではありません。

NetAttest[®]は、株式会社ソリトンシステムズの登録商標です。

その他、本書に掲載されている会社名、製品名は、それぞれ各社の商標または登録商標です。

本文中に ™、®、©は明記していません。

目次

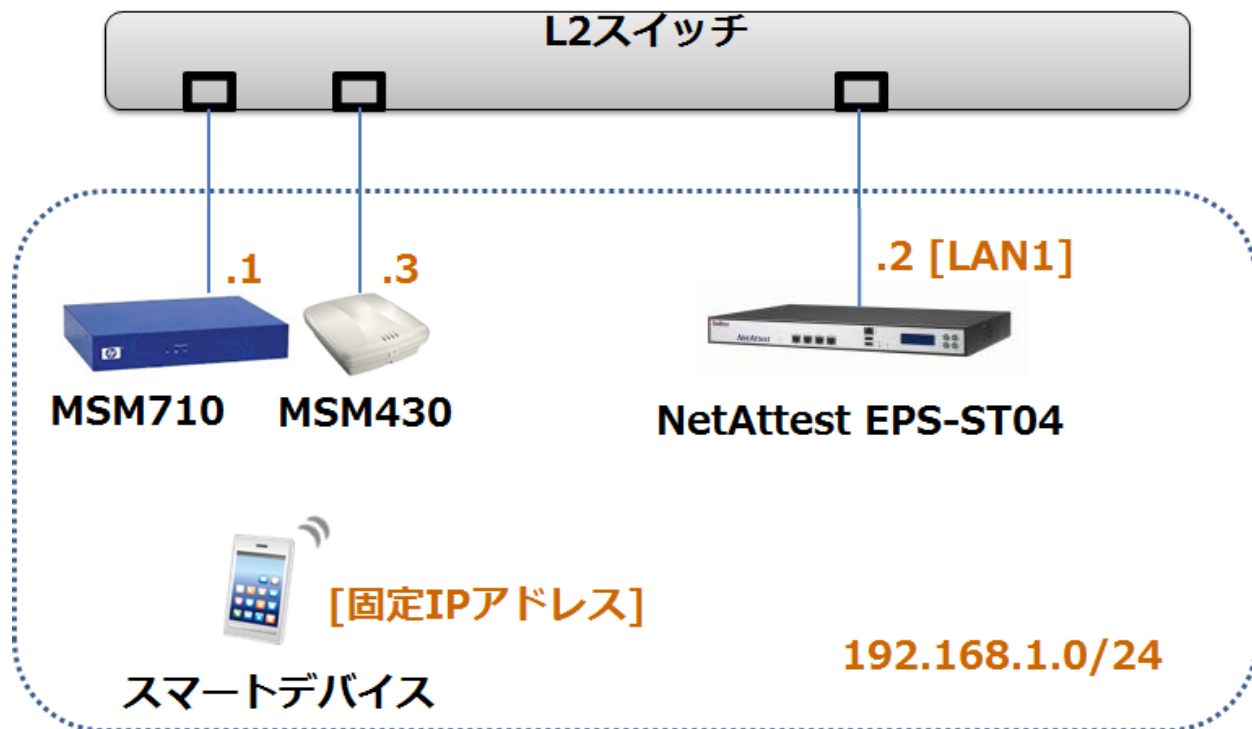
1. 構成.....	6
1-1 構成図.....	6
1-2 環境.....	7
1-2-1 機器.....	7
1-2-2 認証方式.....	7
1-2-3 ネットワーク設定.....	7
2. NetAttest EPS の設定.....	8
2-1 システム初期設定ウィザード.....	8
2-2 システム初期設定ウィザードの実行.....	9
2-3 サービス初期設定ウィザードの実行.....	10
2-4 ユーザーの登録.....	11
2-5 RADIUS クライアントの追加.....	12
2-6 クライアント証明書の発行.....	13
3. MSM4xx シリーズの設定.....	14
3-1 アクセスポイントへのログイン.....	14
3-2 アクセスポイントの初期設定.....	15
3-3 IP アドレスの設定.....	16
3-4 コントローラーの指定.....	17
4. MSM7xx シリーズの設定.....	19
4-1 コントローラーへのログイン.....	19
4-2 End User License Agreement.....	20
4-3 Product Registration.....	20
4-4 国コードの設定.....	21
4-5 ユーザーアカウントの設定.....	21
4-6 Automated workflows.....	22
4-7 コントローラーIP アドレスの変更.....	23
4-8 デフォルトゲートウェイの設定.....	24
4-9 アクセスポイントの接続と認識.....	25
4-10 VLAN の作成.....	26

4-11 RADIUS サーバーの指定	27
4-12 VSC の作成	28
4-13 AP グループの作成	29
4-14 AP 名、グループの変更	30
4-15 グループと VSC の紐付け	31
4-16 コンフィグの同期	32
5. アクセスポイントへの TLS 認証.....	33
5-1 iOS (iPad)	33
5-1-1 iOS へのデジタル証明書のインストール.....	33
5-1-2 サブリカントの設定	34
5-2 Android (Nexus7)	35
5-2-1 Android へのデジタル証明書のインストール.....	35
5-2-2 サブリカントの設定	36
6. アクセスポイントへのゲスト用ワンタイムパスワード認証	37
6-1 NetAttest EPS の設定変更.....	37
6-1-1 DPX ファイルのインポート	37
6-1-2 ユーザーとトークンの紐付け	38
6-2 MSM7xx シリーズの設定変更	39
6-2-1 コントローラーIP アドレスの変更.....	39
6-2-2 DHCP サーバーの起動	40
6-2-3 アクセスポイントの接続と認識	41
6-2-4 RADIUS サーバーの指定	42
6-2-5 VSC の作成	43
6-2-6 AP グループの追加.....	44
6-2-7 AP 名、グループの変更	45
6-2-8 グループと VSC の紐付け.....	46
6-2-9 コンフィグの同期.....	47
6-3 iOS (iPad)	48
7. 証明書配布ソリューション連携について	49

1. 構成

1-1 構成図

システム初期設定ウィザードを使用し、以下の項目を設定します。



1-2 環境

1-2-1 機器

製品名	メーカー	役割	バージョン
NetAttest EPS ST04	Soliton Systems	Authentication Server (認証サーバー)	Ver. 4.6.8
MSM710	HP	Authenticator (認証機器:無線LANコントローラー)	Ver. 6.0.2.2
MSM430	HP	Authenticator (認証機器:無線AP)	Ver. 6.0.2.2
iPad mini	Apple	Client Tablet① (802.1x クライアント)	Ver. 7.1.2
Nexus 7	Google	Client Tablet② (802.1x クライアント)	Ver. 4.4.2

1-2-2 認証方式

IEEE802.1x EAP-TLS 認証、VASCO ワンタイムパスワード認証(PAP)

1-2-3 ネットワーク設定

	IP アドレス	RADIUS port (Authentication)	RADIUS Secret (Key)
NetAttest EPS ST-04	192.168.1.2/24	UDP 1812	secret
MSM710	192.168.1.1/24		secret
MSM430	192.168.1.3/24		secret
Client Tablet①	固定	-	-
Client Tablet②	固定	-	-

2. NetAttest EPS の設定

2-1 システム初期設定ウィザード

NetAttest EPS の初期設定は LAN2(管理インターフェイス)から行います。初期の IP アドレスは「192.168.2.1/24」です。管理端末に適切な IP アドレスを設定し、インターネットエクスプローラーから「<http://192.168.2.1:2181/>」にアクセスします。

下記のような流れでセットアップを行います。

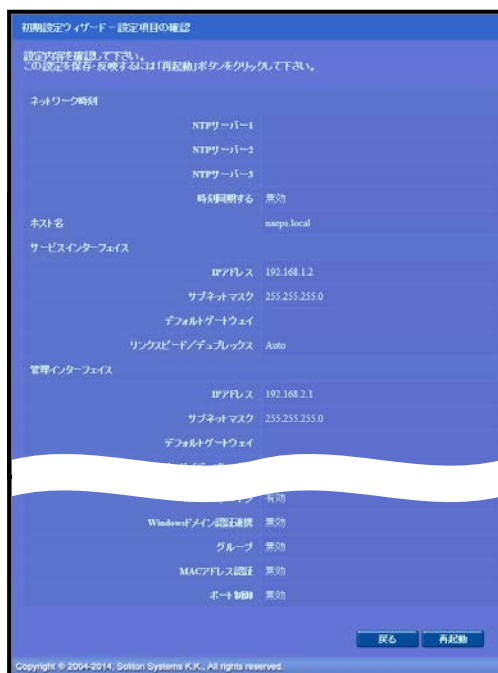
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

2-2 システム初期設定ウィザードの実行

NetAttest EPS の初期設定は LAN2(管理インターフェイス)から行います。初期の IP アドレスは「192.168.2.1/24」です。管理端末に適切な IP アドレスを設定し、インターネットエクスプローラから「http://192.168.2.1:2181/」にアクセスします。

その後、システム初期設定ウィザードを使用し、以下の項目を設定します。

- タイムゾーンと日付・時刻の設定
- ホスト名の設定
- サービスインターフェイスの設定
- 管理インターフェイスの設定
- メインネームサーバーの設定



項目	値
ホスト名	naeps.local
IP アドレス	デフォルト
ライセンス	なし

2-3 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

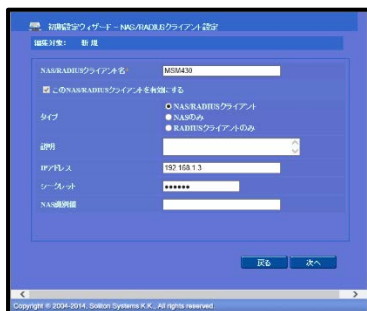
- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定 (全般)
- RADIUS サーバーの基本設定 (EAP)
- RADIUS サーバーの基本設定 (証明書検証)
- NAS/RADIUS クライアント設定



項目	値
EAP 認証タイプ	TLS



項目	値
CA 種別選択	ルート CA
公開鍵方式	RSA
鍵長	2048
CA 名	TestCA



項目	値
NAS/RADIUS クライアント名	MSM430
IP アドレス	192.168.1.3
シークレット	secret

2-4 ユーザーの登録

NetAttest EPS の管理画面より、認証ユーザーの登録を行います。

「ユーザー」→「ユーザー一覧」から、『追加』ボタンでユーザー登録を行います。

The screenshot shows the NetAttest EPS user management interface. The left sidebar has the 'ユーザー' (User) menu item highlighted. The main area shows the 'ユーザー一覧' (User List) page with a table containing one user: 'test user' with ID 'test'. A red box highlights the '追加' (Add) button. An arrow points to the 'ユーザー設定' (User Settings) form, which is pre-filled with 'user01' for the name and ID, and 'password' for the password. The 'OK' button is also highlighted with a red box.

項目	値
姓	user01
ユーザーID	user01
パスワード	password

The final screenshot shows the 'ユーザー一覧' (User List) page after the user 'user01' has been added. The table now contains two users: 'test user' and 'user01'. The 'user01' row is highlighted with a red box.

2-5 RADIUS クライアントの追加

NetAttest EPS の管理画面より、無線 LAN コントローラー MSM710 の登録を行います。
「RADIUS サーバー」→「NAS/RADIUS クライアント」→「NAS/RADIUS クライアント一覧」から、『追加』ボタンで RADIUS クライアント登録を行います。

項目	値
NAS/RADIUSクライアント名	MSM710
IPアドレス	192.168.1.1
シークレット	secret

2-6 クライアント証明書発行

NetAttest EPS の管理画面より、クライアント証明書の発行を行います。

「ユーザー」→「ユーザー一覧」から、該当するユーザーのクライアント証明書を発行します。(クライアント証明書は、user01_02.p12 という名前で保存)

The screenshot shows the NetAttest EPS management interface. The left sidebar contains a navigation menu with 'ユーザー一覧' (User List) highlighted. The main area displays a table of users:

名前	ユーザーID	証明書	タスク
test user	test		発行 変更 削除
user01	user01		発行 変更 削除

A red box highlights the '発行' (Issue) button for user01. An arrow points to a detailed user configuration page for 'user01'. This page includes fields for '姓' (Last Name), '名' (First Name), 'E-Mail', and '詳細情報'. The '認証情報' (Authentication Information) section shows 'ユーザーID' as 'user01' and '有効期限' (Validity Period) set to 365 days. The '証明書ファイルオプション' (Certificate File Options) section has 'パスワード' and 'パスワード(確認)' fields, and a checked checkbox for 'PKCS#12ファイルに証明機関の証明書を含める' (Include CA certificate in PKCS#12 file). A red box highlights the '発行' (Issue) button at the bottom right.

An arrow points to a 'ユーザー証明書のダウンロード' (Download User Certificate) dialog box. It contains the message: 'ユーザー証明書ダウンロードの準備ができました。対象をファイルに保存して下さい。' (User certificate download preparation is complete. Please save the target to a file.) and a 'ダウンロード' (Download) button highlighted with a red box.

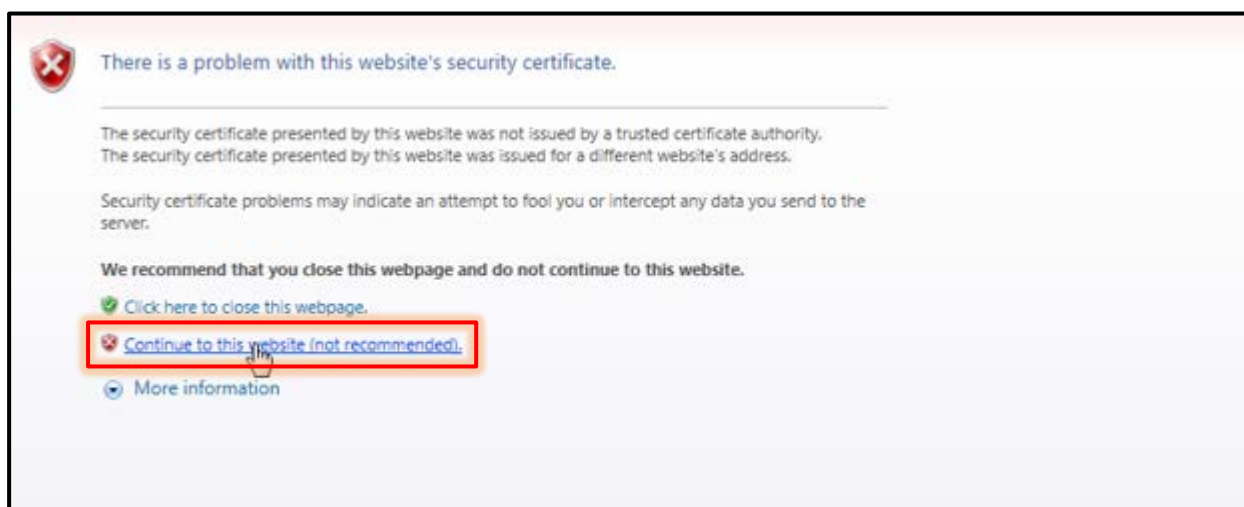
3. MSM4xx シリーズの設定

3-1 アクセスポイントへのログイン

MSM4xx シリーズのデフォルト IP アドレスは 192.168.1.1/24 に設定されています。

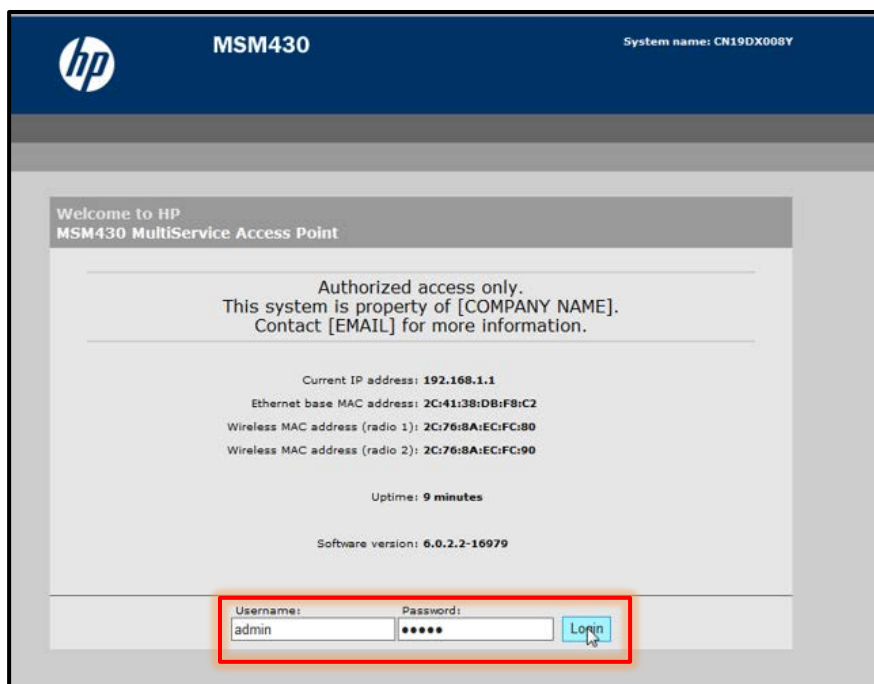
Web ブラウザよりアクセスを行うと、証明書エラーの画面が表示されますが、“Continue to this website”をクリックします。

※MSM4xx シリーズのインターフェイスは DHCP Client も動作していますので、DHCP の環境下では DHCP より IP アドレスが付与されます。



“Continue to this website”をクリックするとログイン画面が表示されます。

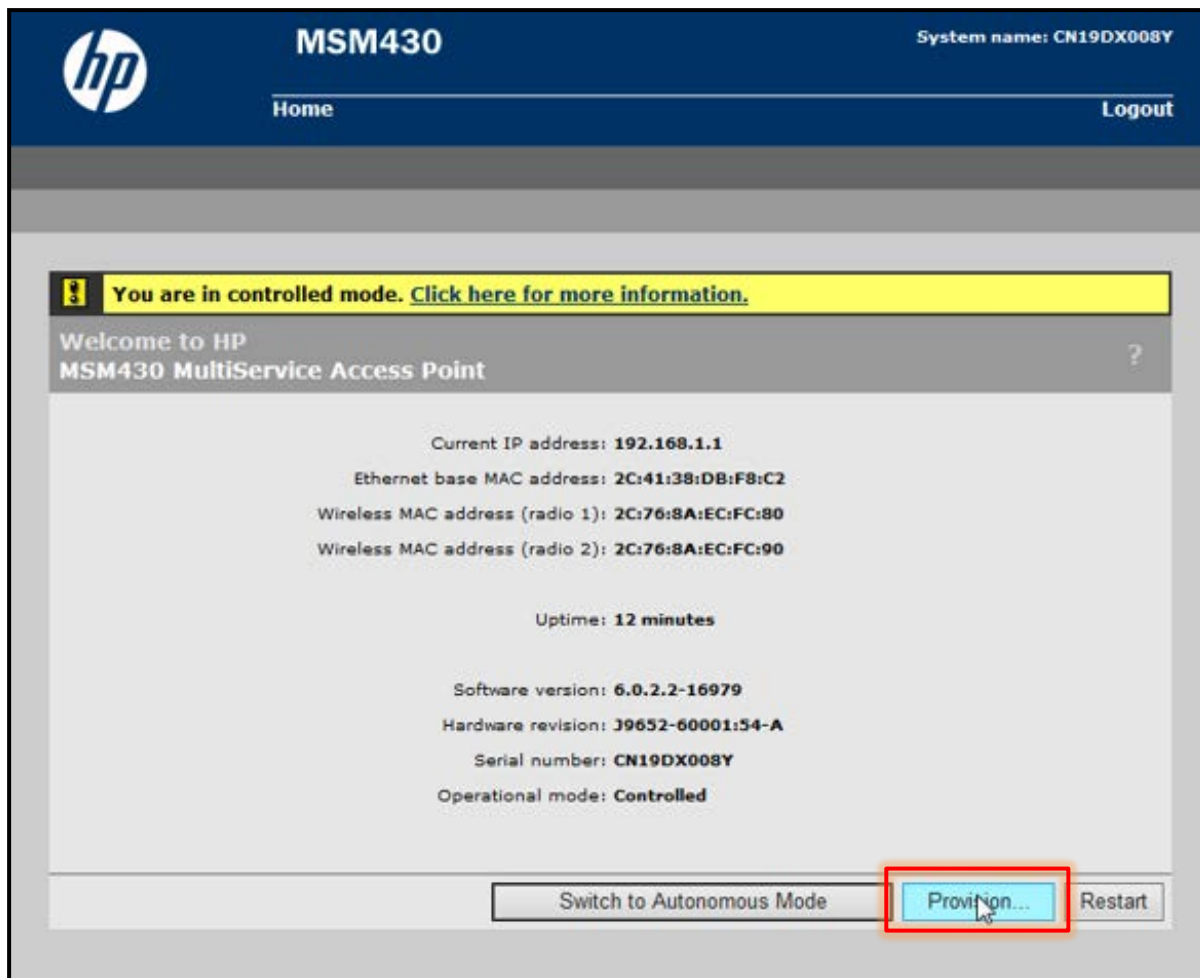
デフォルトのユーザー名、パスワードは“admin”です。“admin”でログインします。



3-2 アクセスポイントの初期設定

コントローラーに接続するために、アクセスポイントの初期設定を行います。
画面の「Provision…」をクリックします。

Switch to Autonomous Mode はアクセスポイントのみで動作させる場合に利用します。
コントローラーで管理する場合は Operation Mode は“Controlled”となります。



3-3 IP アドレスの設定

「Provision…」をクリックすると、Connectivity 設定画面が表示されます。

「Connectivity」をチェックします。また、「Assign IP address via」で“Static”を選択し、「Static IP Settings」に指定の IP アドレス、サブネットマスク、デフォルトゲートウェイを入力します。

項目	値
Assign IP address via	Static
IP address	192.168.1.3
Mask	255.255.255.0
Default gateway	192.168.1.1

最下部の「Save」をクリックします。

3-4 コントローラーの指定

「Discovery」タブをクリックすると、Discovery 設定画面に切り替わります。

「Discovery」をチェックします。「Discovery using Address」にチェックし、「IP address」欄にコントローラーに設定する IP アドレスを入力し、「Add」をクリックします。

項目	値
IP address	192.168.1.1

「Add」をクリックすると、「Address to search for」に入力した IP アドレスが表示されます。

最下部の「Save」をクリックします。

「Connectivity」と「Discovery」の設定が完了したら、左側にある「Info」より「Restart」ボタンをクリックします。

約 1 分後に「Connectivity」にて設定した IP アドレスで起動します。

The screenshot displays the Soliton provisioning interface. On the left, a sidebar contains a 'Summary' section with a table of provisioning status and an 'Info' section with a 'Restart' button highlighted by a red box. The main area shows the 'Discovery' configuration page, which includes options for 'Discover using DNS' and 'Discover using IP address', along with fields for names, addresses, domain names, and controller authentication.

	Provisioned
Connectivity	Yes
Discovery	Yes
Location	No

Once provisioning is complete you must restart the AP for your changes to take effect.

Restart

Restart and stop the provisioning

Discovery

Discover using DNS

Names to search for:

Name:

Domain name:

Primary DNS server:

Secondary DNS server:

Discover using IP address

Addresses to search for:

192.168.1.1

IP address:

Controller authentication

Controller shared secret:

Confirm controller shared secret:

Controller authentication

4. MSM7xx シリーズの設定

4-1 コントローラーへのログイン

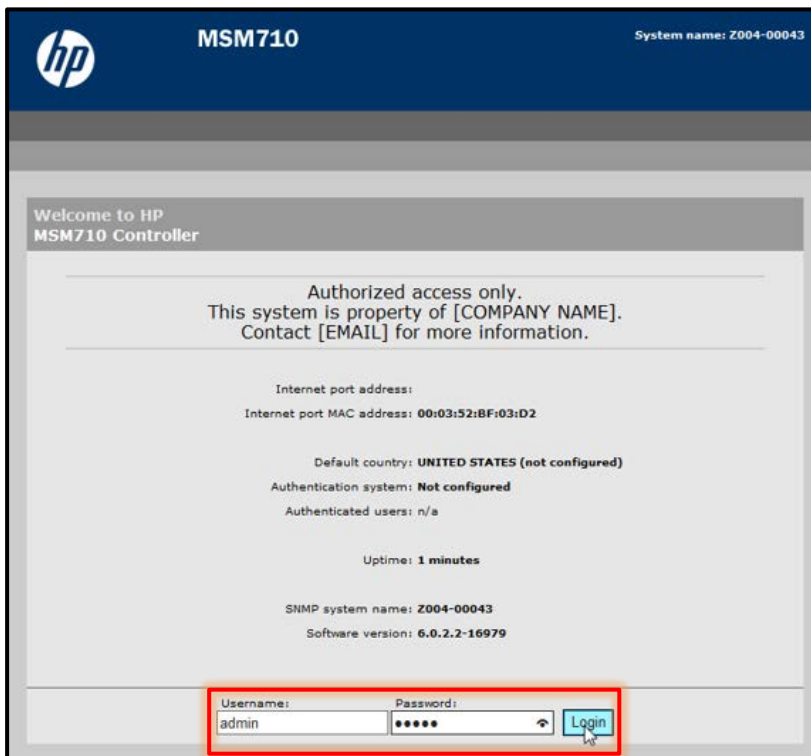
MSM7xx シリーズのデフォルト IP アドレスは 192.168.1.1/24 に設定されています。

Web ブラウザよりアクセスを行うと、証明書エラーの画面が表示されますが、“Continue to this website”をクリックします。



“Continue to this website”をクリックするとログイン画面が表示されます。

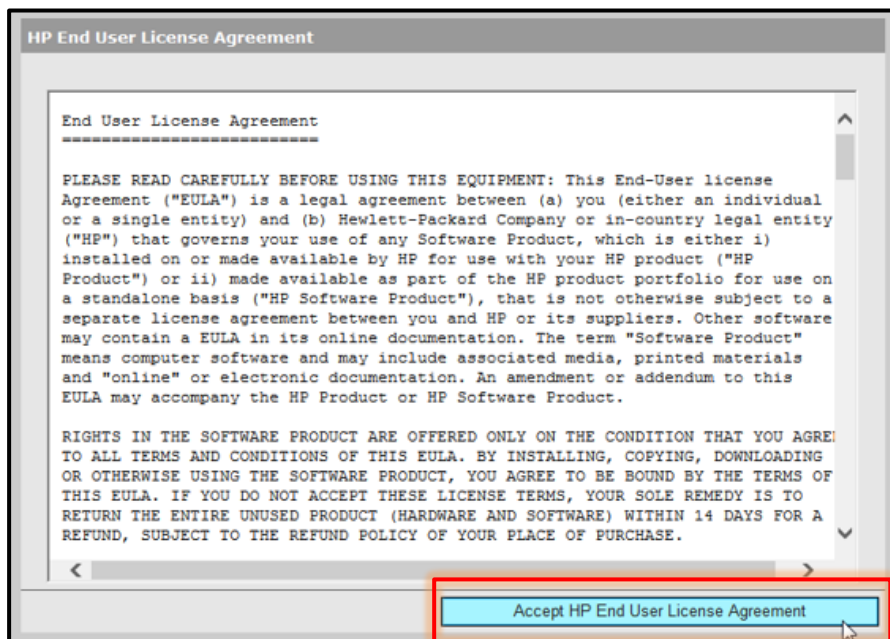
デフォルトのユーザー名、パスワードは“admin”です。“admin”でログインします。



4-2 End User License Agreement

初めてログインを行った場合、End User License Agreement 画面が表示されます。

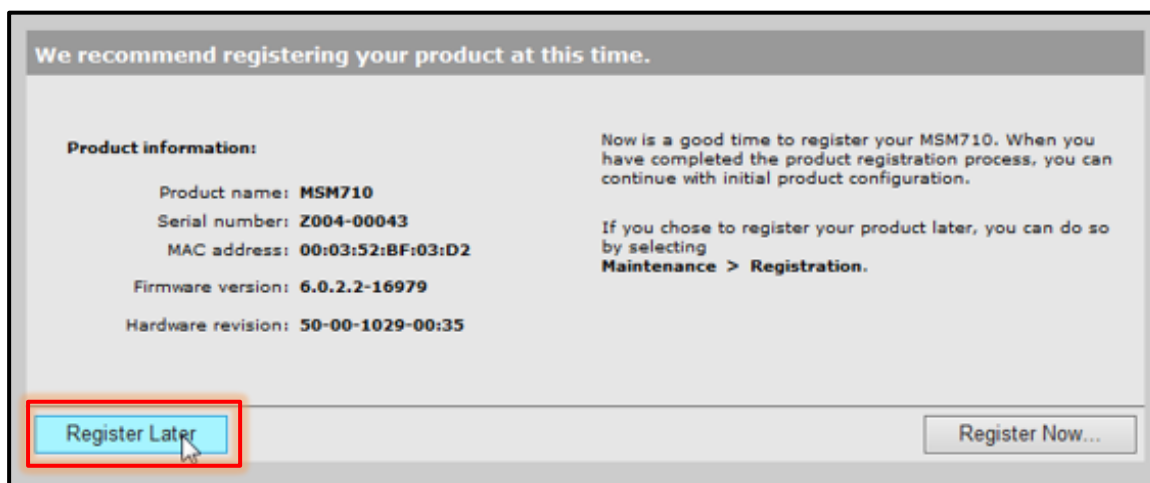
「Accept HP End User License Agreement」 ボタンをクリックします。



4-3 Product Registration

「Accept HP End User License Agreement」 をクリックすると、次は製品登録ページが表示されます。「Register Later」 をクリックします。

※ 「Register Now」 をクリックすると、製品登録 URL へ移行します(Internet に接続している必要があります)。



4-4 国コードの設定

「Register Later」をクリックすると、国コード設定画面が表示されます。
国コードを選択し、「Save」をクリックします。

Configure the country where the product will be used

Country: JAPAN (W52 & W53 & W56) ▼

Please select the country that this product will operate in. This ensures that wireless radio settings will be configured in accordance with local regulations.

Save

項目	値
Country	JAPAN(W52 & W53 & W56)

4-5 ユーザーアカウントの設定

デフォルトだとユーザー名、パスワードは“admin”に設定されています。
変更を行う場合は変更します。今回は「Cancel」をクリックします。

We recommend changing the default administrator password at this time.

Username:

Current password:

New password:

Confirm new password:

Enable Password Console Reset

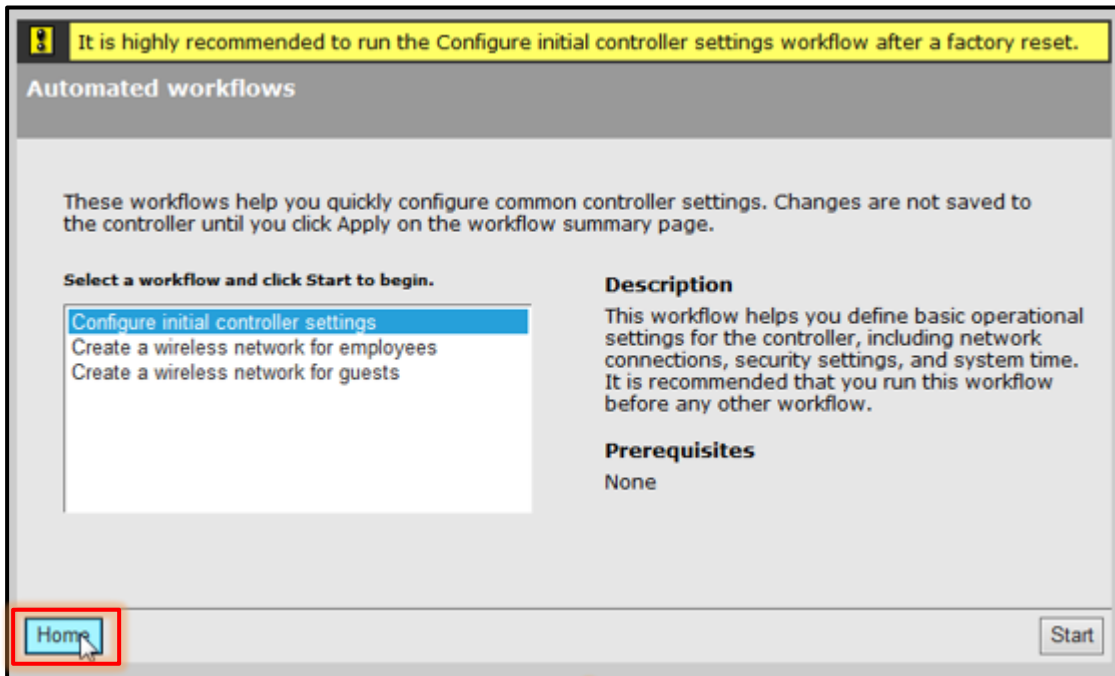
Access to the MSM710 management tool can be restricted by an administrator password. It is highly recommended that you change your unit password, especially if it is exposed to external networks.

For optimum security, your password should be at least six characters long. The password is case-sensitive.

Cancel Save

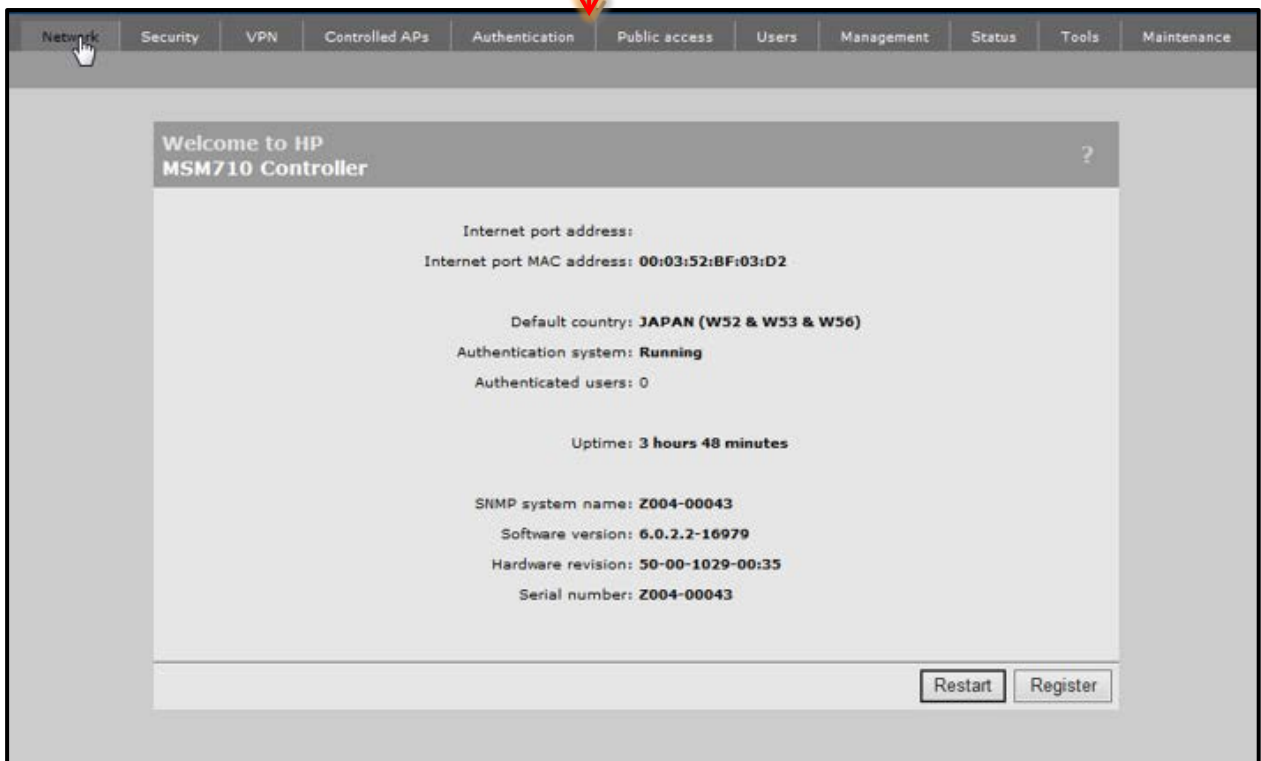
4-6 Automated workflows

問答方式で簡易的にコントローラーの初期設定、SSID の作成ができます。
今回は作成せず、「Home」 ボタンをクリックします。



Home 画面です。

次回ログインからこの画面が表示されます。



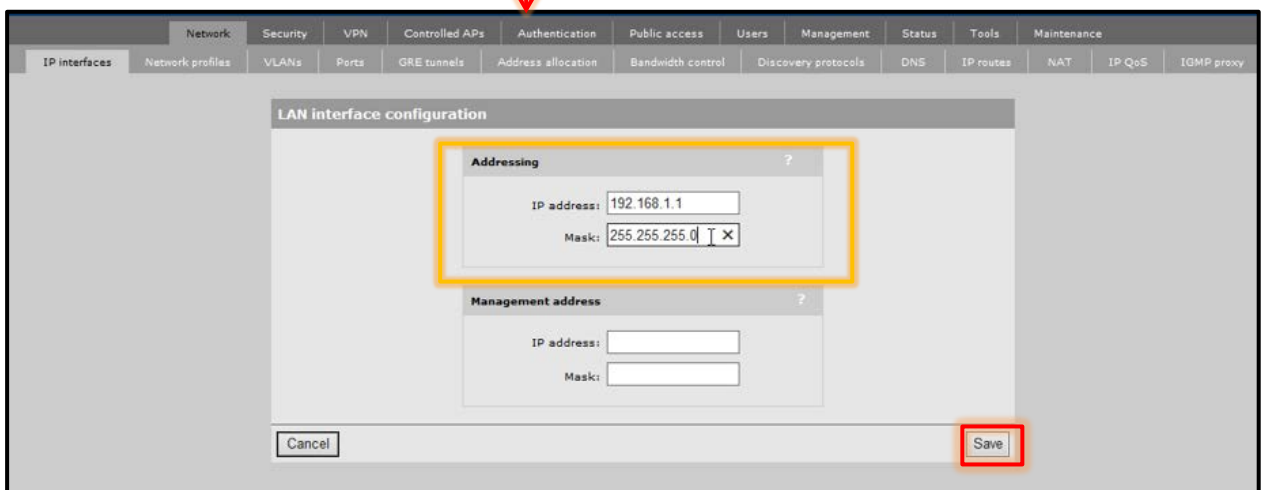
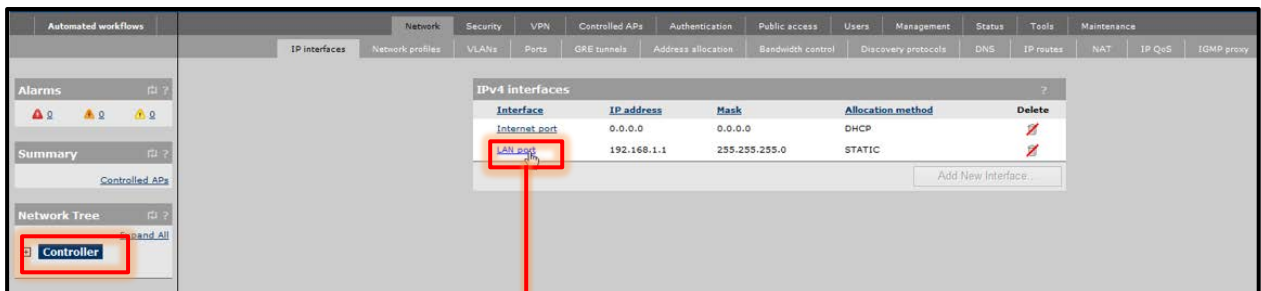
4-7 コントローラーIP アドレスの変更

左側の「Network Tree」より「Controller」をクリックします。

[Network]-[IP interface]より「IPv4 Interface」の「LAN port」をクリックします。

LAN Interface Configuration 画面が表示されますので、「Addressing」で IP アドレス、サブネットマスクを変更し、「Save」をクリックします。

※「Save」を行うと即座に設定が反映されます。アドレスを変更した場合は、変更したアドレスで再度ログインしてください。



項目	値
IP address	192.168.1.1
Mask	255.255.255.0

4-8 デフォルトゲートウェイの設定

[Network]-[IP routes]より「Default routes」のゲートウェイおよびメトリックを設定し、「Add」をクリックします。

The screenshot shows the 'IP routes' configuration page. The 'Default routes' section is highlighted with a yellow box. The 'Add' button is highlighted with a red box. A red arrow points from the 'Add' button to the second screenshot.

項目	値
Gateway	192.168.1.254
Metric	0

The screenshot shows the 'IP routes' configuration page after the default gateway has been added. The 'Default routes' section is highlighted with a red box, showing the entry for the LAN port with gateway 192.168.1.254 and metric 0.

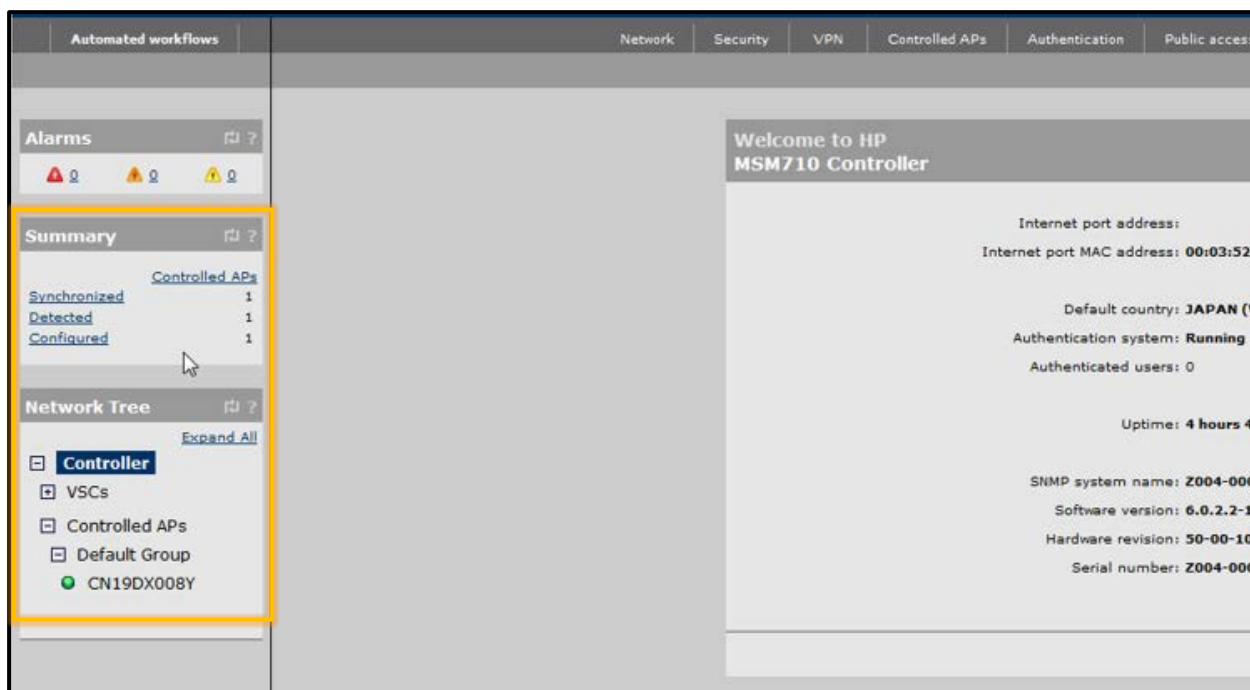
4-9 アクセスポイントの接続と認識

Provisioning 設定を行ったアクセスポイントを接続します。

アクセスポイントとコントローラーが IP 通信できている場合は「summary」欄にアクセスポイントの状態が表示されます。

表示項目	説明
Synchronized	アクセスポイントとコントローラーのコンフィグが同期しています
Unsynchronized	アクセスポイントとコントローラーコンフィグに差異があります
Detected	コントローラーが発見したアクセスポイント数が表示されます
Configured	コントローラーからコンフィグを流したアクセスポイント数が表示されます
Pending	コントローラーがアクセスポイントに対して操作を行っています

正常に認識がされた場合は、「Network Tree」の[Controller]-[Controlled APs]-[Default Group]にアクセスポイントが表示され、インジケータは緑で表示されます。

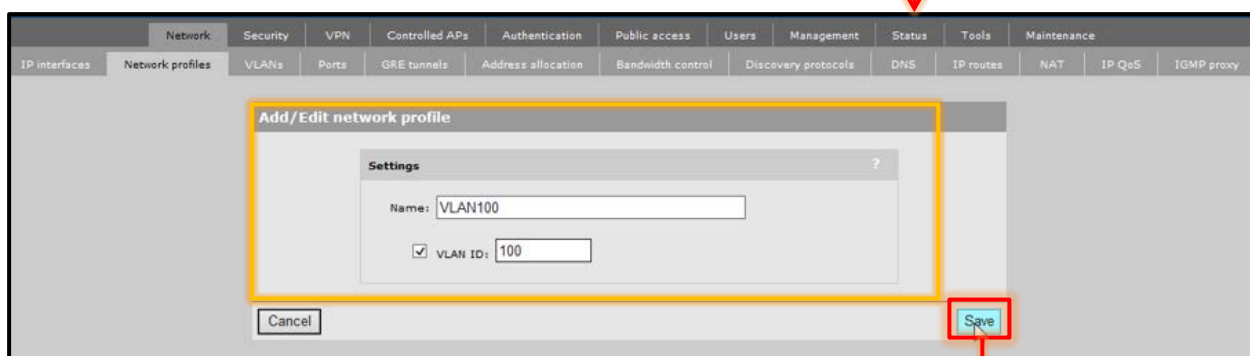


4-10 VLAN の作成

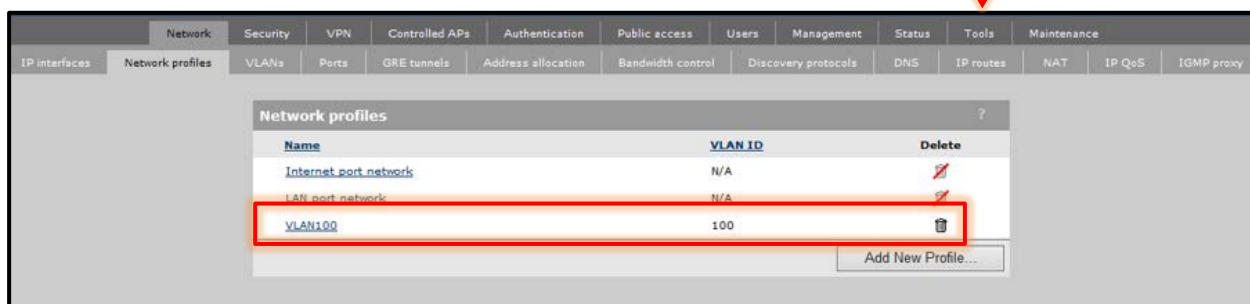
端末の通信データを出力する VLAN を作成します。

「Network Tree」の[Controller]より[Network]-[Network Profiles]の「Add New Profile」をクリックします。「Name」に VLAN を入力し、VLAN ID にチェックを入れ、ID を入力します。「Save」をクリックします。

作成できると Network Profiles 画面に作成した VLAN が表示されます。

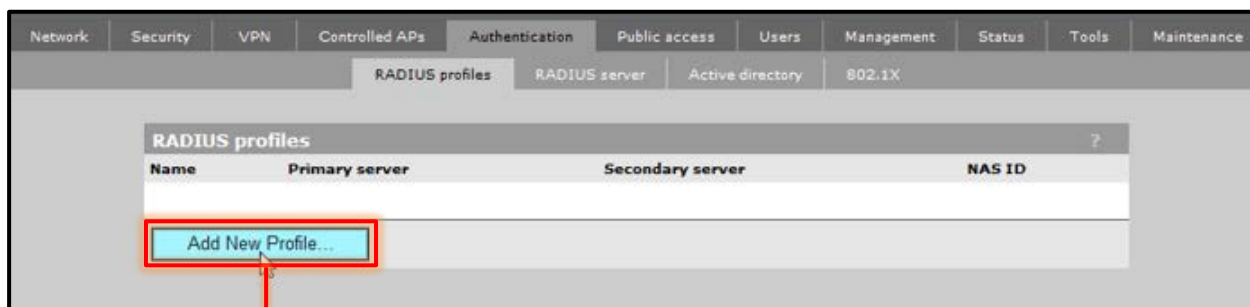


項目	値
Name	VLAN100
VLAN ID	100



4-11 RADIUS サーバーの指定

「Network Tree」の[Controller]より[Authenticate]-[RADIUS profiles]の「Add New Profile」をクリックします。「Profile name」を入力し、必要に応じて「Settings」の内容を変更します。「Primary RADIUS server」にRADIUSサーバーのIPアドレス、シークレットを入力します。「Save」をクリックします。



Add/Edit RADIUS profile

Profile name

Profile name:

Settings

Authentication port:

Accounting port:

Retry interval: seconds

Retry timeout: seconds

Authentication method:

NAS ID:

Always try primary server first

Use message authenticator

Force NAS-Port to ingress VLAN ID

Override NAS ID when acting as a RADIUS proxy

Primary RADIUS server

Server address:

Secret:

Confirm secret:

Secondary RADIUS server (optional)

Server address:

Secret:

Confirm secret:

Authentication realms

Changing the realm configuration will logout all authenticated users.

Associated realms:

Support regular expressions in realm names

New realm:

項目	値
Profile name	NetAttest EPS
Server address	192.168.1.2
Secret	secret



4-12 VSC の作成

HP の MSM シリーズは SSID の Profile の総称として VSC(バーチャルサービスコミュニティ)と呼ばれています。

「Network Tree」の[Controller]-[VSCs]より「Add New VSC Profile」をクリックします。

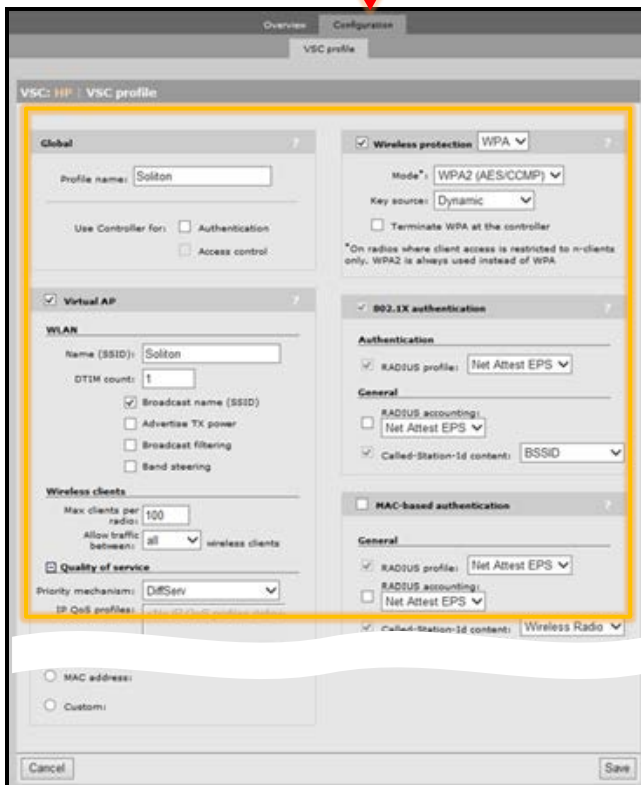
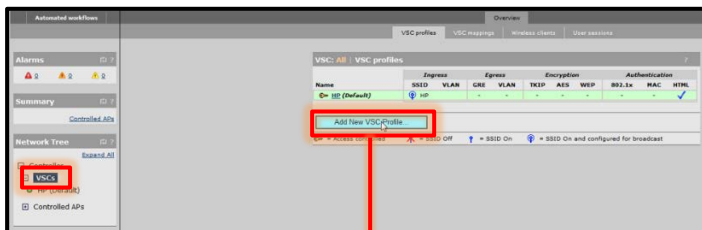
「Profile name」を入力し、「Use Controller for」の「Authentication」、「Access Control」のチェックを外します。

※「Authentication」のチェックを入れると、コントローラー内蔵 RADIUS もしくは、コントローラー内蔵 RADIUS 経由で外部 RADIUS サーバーに問い合わせます。

「Virtual AP」にチェックを入れ、Name(SSID)を入力します。

「Wireless Protection」にチェックを入れ、「WPA」を選択します。「Mode」に「WPA2」を選択し、「Key source」は「Dynamic」を選択します。

「802.1x authentication」の「RADIUS profile」に[4-11]で作成した RADIUS プロファイルを選択します。「Save」をクリックします。



項目	値
Profile name	Soliton
Name(SSID)	Soliton
Wireless Protection	WPA
Mode	WPA2
Key source	Dynamic
Authentication	NetAttes EPS

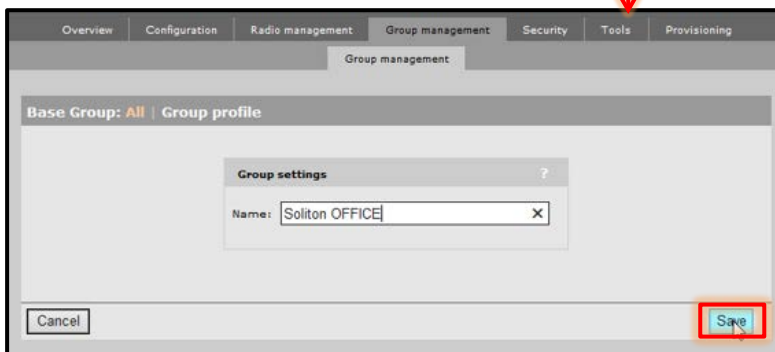
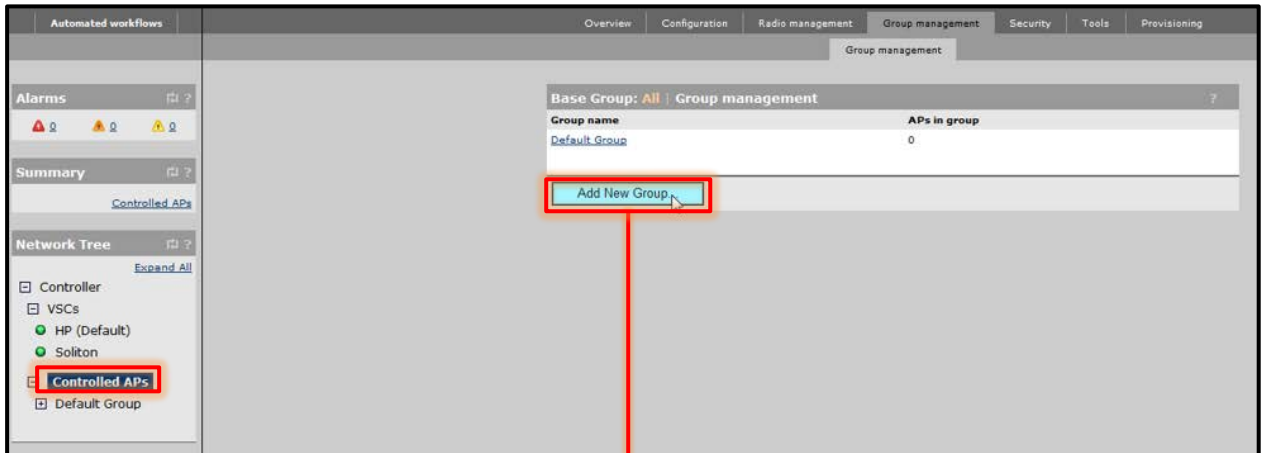
4-13 AP グループの作成

アクセスポイントのグループごとに VSC を選択することができます。

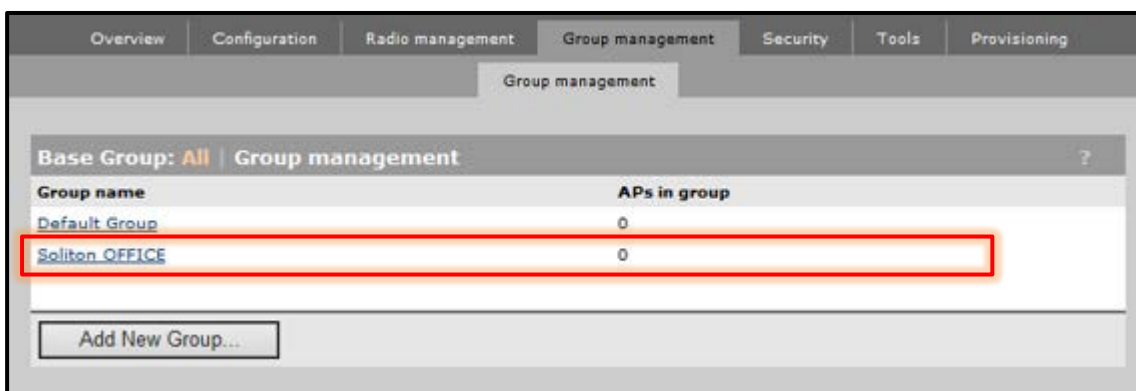
「Network Tree」の [Controller]-[Controlled APs] より [Group management]-[Group management]の「Add New Group」をクリックします。

「Group settings」の「Name」を入力し、「Save」をクリックします。

作成すると「Base Group」に作成したグループが表示されます。



項目	値
Name	Soliton OFFICE



4-14 AP 名、グループの変更

「Network Tree」の[Controller]-[Controlled APs]-[Default Group]に表示されているアクセスポイントをクリックします。

※デフォルトはシリアルナンバーがアクセスポイント名となっています。

[Device management]-[AP management]の「Access point name」を変更し、「Group」は[4-13]で作成したグループを選択します。「Save」をクリックします。

「Save」をクリックすると、[Network Tree]の[Controller]-[Controlled APs]の[Default Group]から作成したグループへアクセスポイントが移動します。

インジケータは黄色になり、「Summary」では「Unsynchronized」となります。

項目	値
Access point name	AP-01
Group	Soliton OFFICE

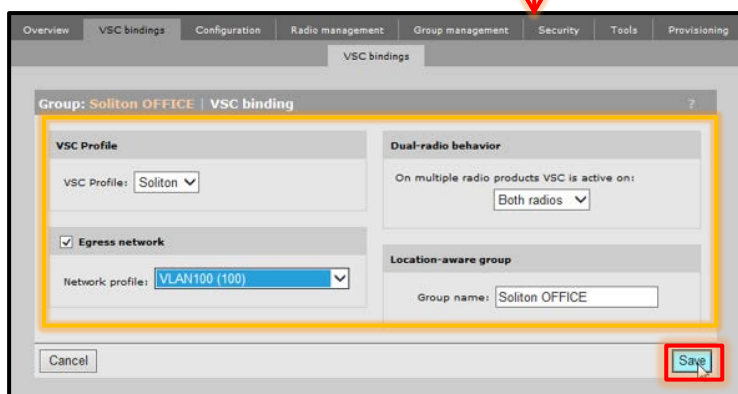
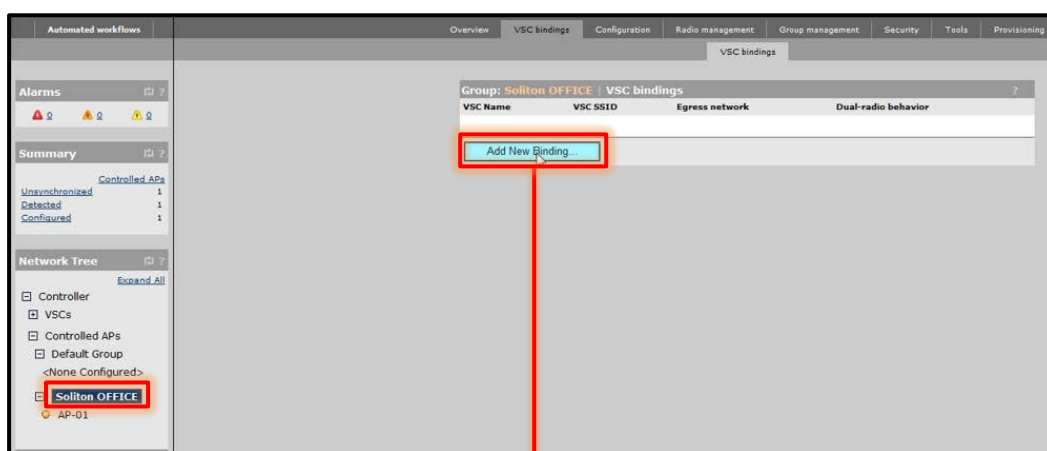
4-15 グループと VSC の紐付け

作成したグループは何も SSID を出力していない状態です。VSC を紐付けることで、SSID を出力します。

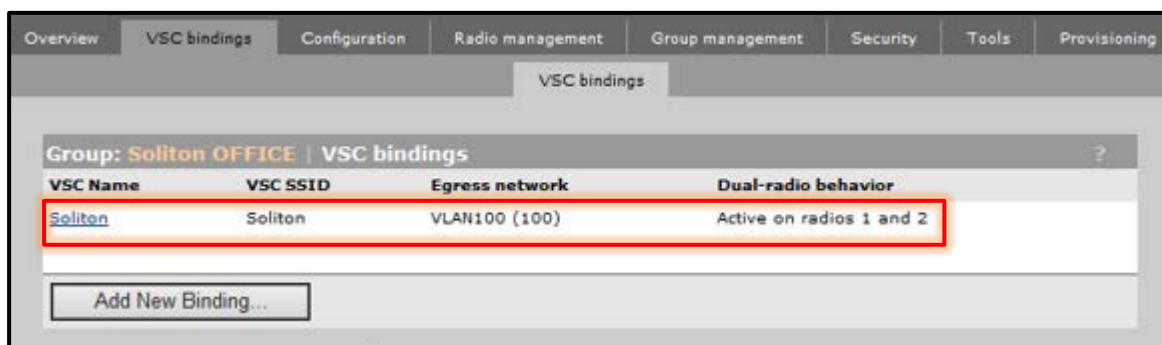
「Network Tree」の[Controller]-[Controlled APs]の作成したグループより[VSC bindings]の「Add New Binding」をクリックします。

「VSC Profile」にて[4-12]で作成した VSC を選択します。「Egress network」にチェックを入れ、「Network Profile」で[4-10]で作成した VLAN を選択します。

※「Egress network」にチェックを入れることで、アクセスポイントから直接指定の VLAN へ出力できるようになります。「Save」をクリックします。

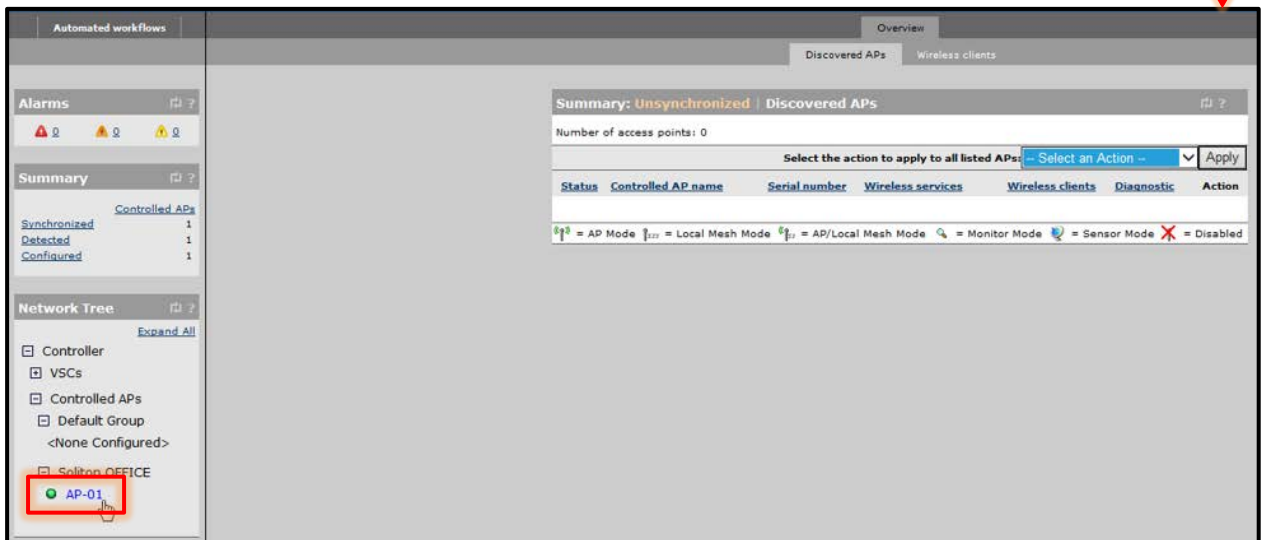
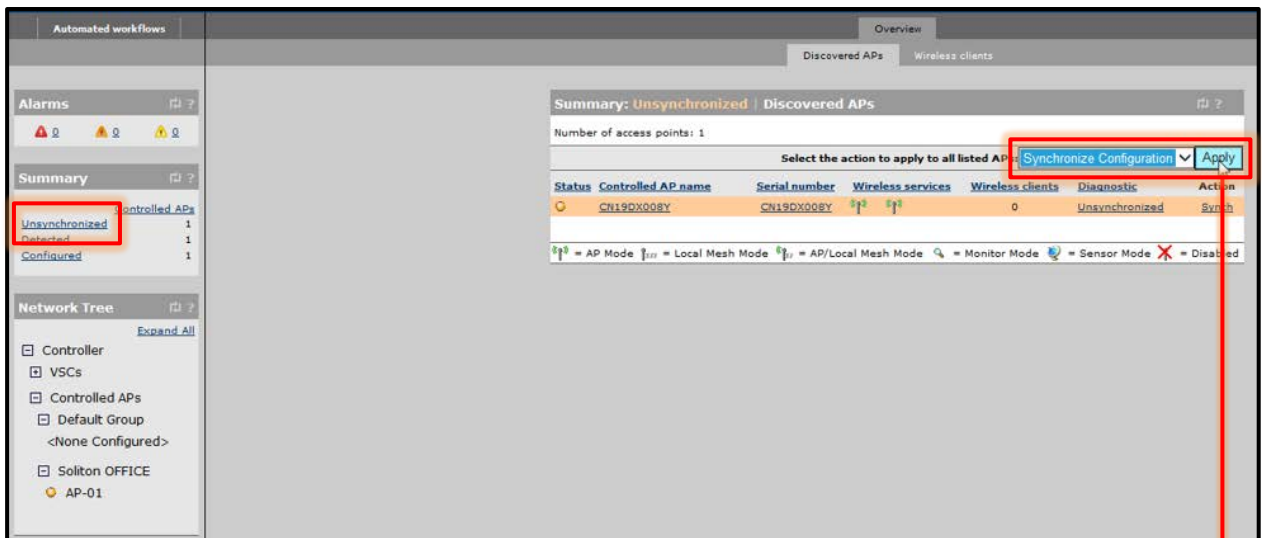


項目	値
VSC Profile	Soliton
Network profile	VLAN100(100)



4-16 コンフィグの同期

ここまでは、アクセスポイントのコンフィグの作成を行いました。コントローラーとアクセスポイントを同期させることによって、アクセスポイントから設定した SSID が出力できるようになります。[Summary]の「Unsynchronized」をクリックし、「Select the action to all listed APs」で「Synchronize Configuration」を選択し、「Apply」をクリックします。[Summary]にて「Synchronized」となり、アクセスポイントのインジケーターが緑に表示されれば、同期が完了となります。



5. アクセスポイントへの TLS 認証

5-1 iOS (iPad)

5-1-1 iOS へのデジタル証明書のインストール

NetAttest EPS から発行したデジタル証明書を iOS デバイスにインストールする方法として、下記の方法などがあります。

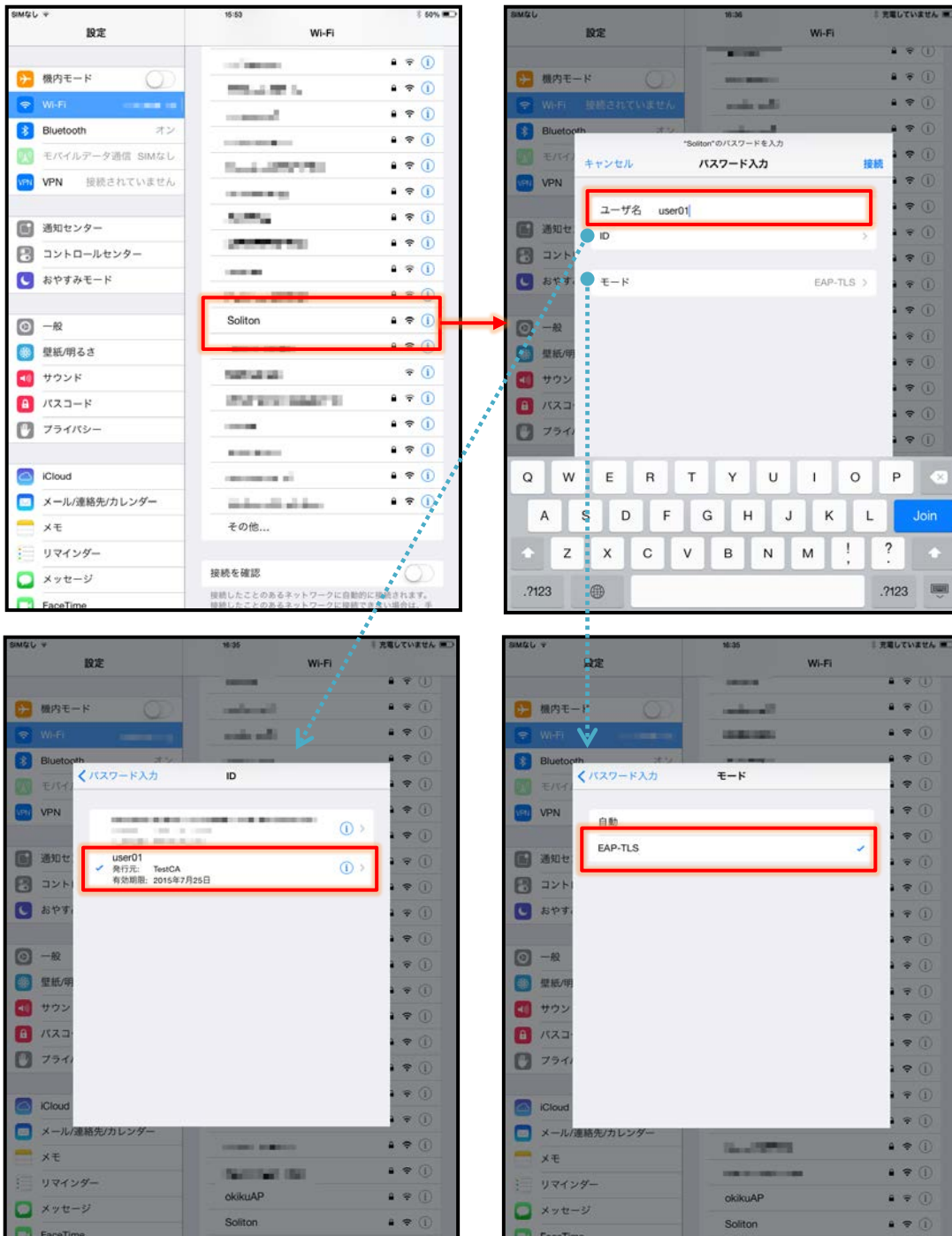
- 1) iPhone 構成ユーティリティ（構成プロファイル）を使う方法
- 2) デジタル証明書をメールに添付し iOS デバイスに送り、インストールする方法
- 3) SCEP で取得する方法(NetAttest EPS-ap を利用できます)

いずれかの方法で CA 証明書とクライアント証明書をインストールします。本書では割愛します。

5-1-2 サプリカントの設定

MSM7xx シリーズで設定した SSID をタップし、サプリカントの設定を行います。

まず、「ユーザ名」には証明書を発行したユーザーアカウントの ID を入力します。次に「モード」より「EAP-TLS」を選択します。その後、「ユーザ名」の下の「ID」よりインストールされたユーザー証明書を selects します。



5-2 Android (Nexus7)

5-2-1 Android へのデジタル証明書のインストール

NetAttest EPS から発行したデジタル証明書を Android デバイスにインストールする方法として、下記 3 つの方法等があります。いずれかの方法で CA 証明書とユーザー証明書をインストールします。手順については、本書では割愛させていただきます。

- 1) SD カードにデジタル証明書を保存し、インストールする方法※1
- 2) デジタル証明書をメールに添付し Android デバイスに送り、インストールする方法※2
- 3) SCEP で取得する方法(NetAttest EPS-ap を利用できます)※3

※1 メーカーや OS バージョンにより、インストール方法が異なる場合があります。事前にご検証ください。

※2 メーカーや OS バージョン、メーカーにより、インストールできない場合があります。事前にご検証ください。

※3 メーカーや OS バージョンにより、EPS-ap Android アプリが正常に動作しない場合があります。事前にご検証ください。

5-2-2 サプリカントの設定

MSM7xx シリーズで設定した SSID をタップし、サプリカントの設定を行います。「ID」には証明書を発行したユーザーアカウントの ID を入力します。また、本書では、CA 証明書を含めた PKCS#12 ファイルをインストールしたため、CA 証明書及びユーザー証明書が同じ名前になっています。CA 証明書を個別にインストールした場合は、その CA 証明書を選択してください。



項目	値
セキュリティ	802.1x EAP
EAP 方式	TLS
CA 証明書	user01
ユーザー証明書	user01
ID	user01

6. アクセスポイントへのゲスト用ワンタイムパスワード認証

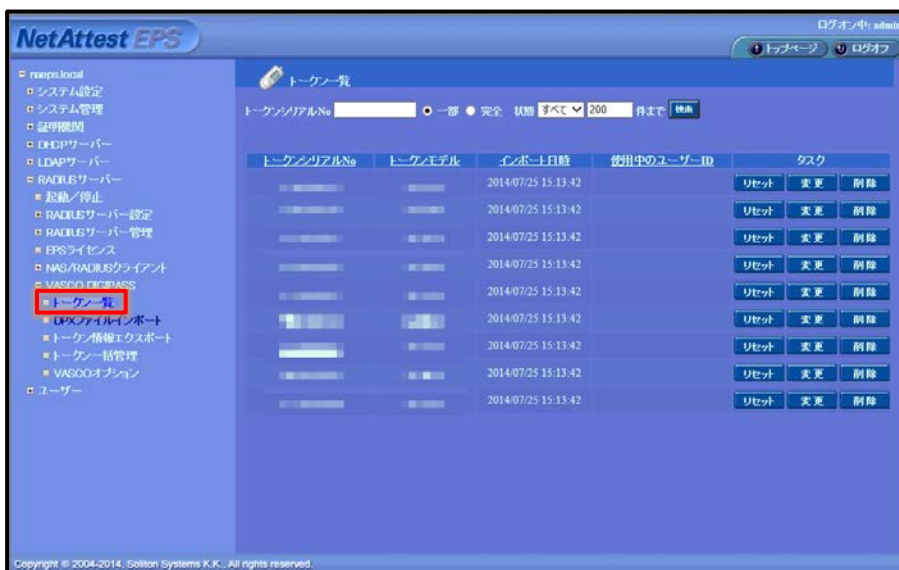
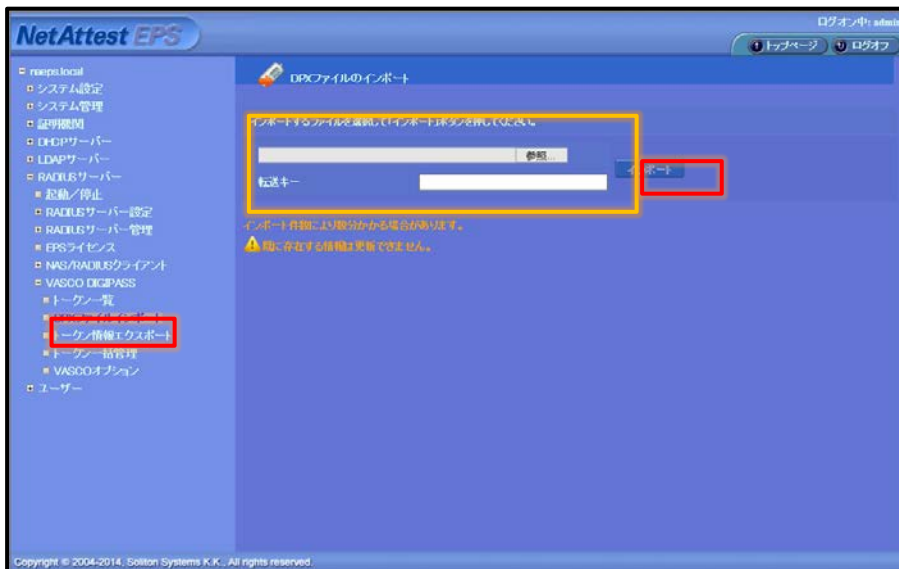
6-1 NetAttest EPS の設定変更

6-1-1 DPX ファイルのインポート

EPS のシステム管理ページより[RADIUS サーバー]-[VASCO DIGIPASS]-[DPX ファイルインポート]にて DPX ファイルを参照し、転送キーを入力します。「インポート」をクリックします。

※DPX ファイルはご購入頂くと、製品と一緒に納品されます。評価用の DPX ファイルもご用意しております。

DPX ファイルをインポートすると、[RADIUS サーバー]-[VASCO DIGIPASS]-[トークン一覧]にて、ご購入頂いた数だけ一覧に表示されます。



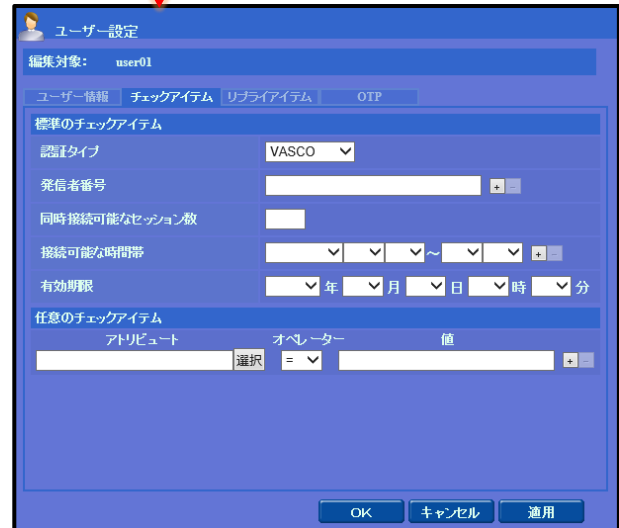
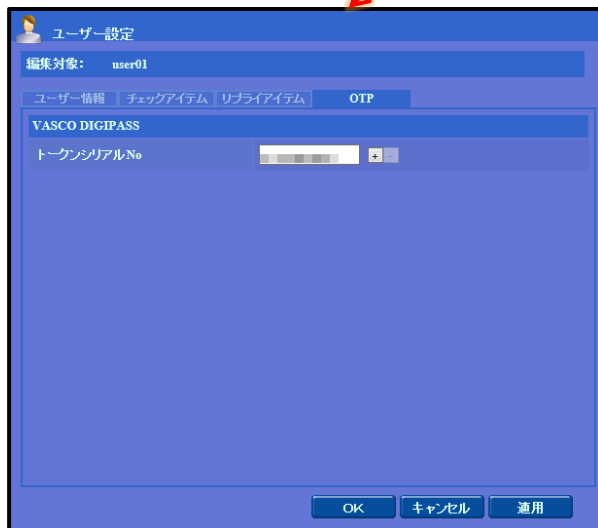
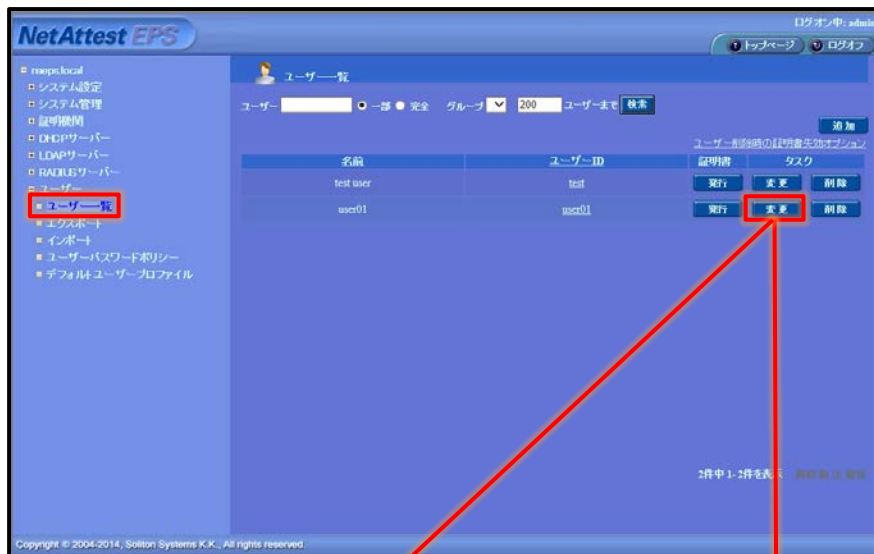
6-1-2 ユーザーとトークンの紐付け

ユーザーとトークンの紐付けを行います。

[ユーザー]-[ユーザー一覧]より、作成済みのユーザーの「変更」をクリックします。

「OTP」タブの「トークンシリアルNo」に、このユーザーに割り当てたいトークンシリアルナンバーを[6-1-1]のトークン一覧の中から選択し、入力します。

「チェックアイテム」タブの「認証タイプ」より「VASCO」を選択します。「適用」をクリックします。



6-2 MSM7xx シリーズの設定変更

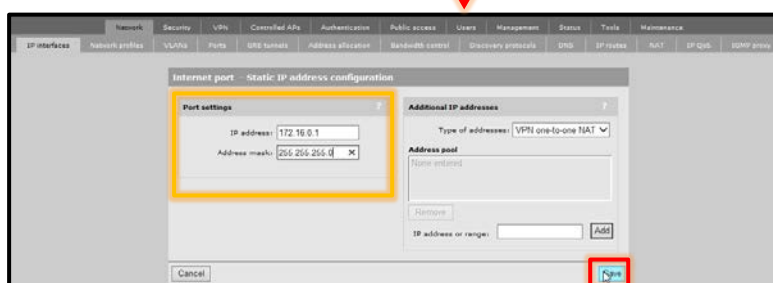
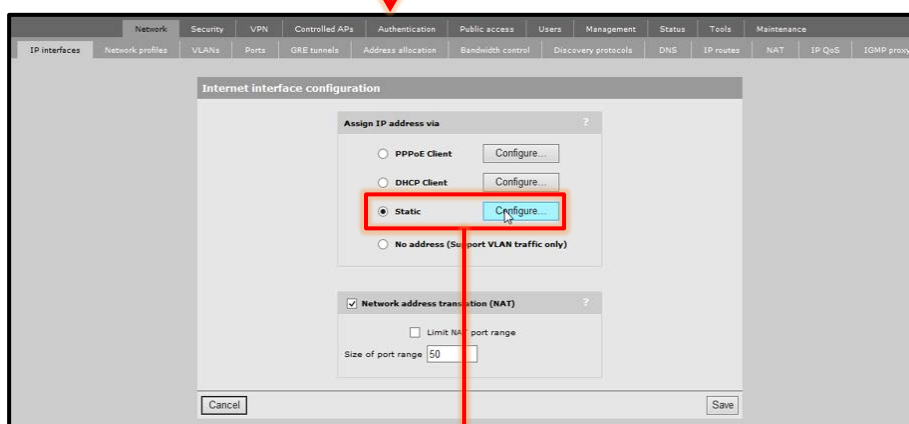
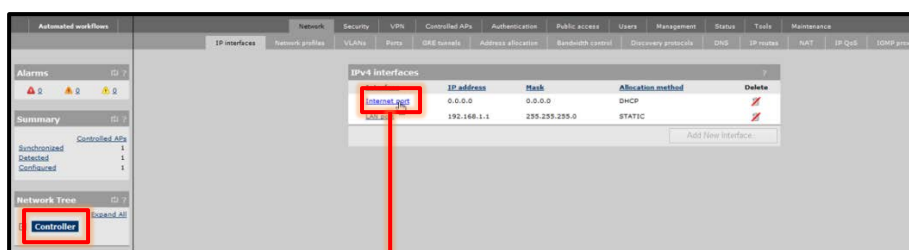
[4. MSM7xx シリーズの設定]が完了している前提で、ゲスト用ワンタイムパスワード認証を行うための MSM7xx シリーズの設定変更方法の説明を行います。

6-2-1 コントローラーIP アドレスの変更

「Network Tree」の[Controller]より[Network]-[IP interfaces]において、「IPv4 interfaces」の「Internet port」をクリックします。

「Assign IP Address via」で「Static」を選択し、「Configure」をクリックします。

「Port settings」において、指定の IP アドレス、サブネットマスクを入力し、「Save」をクリックします。



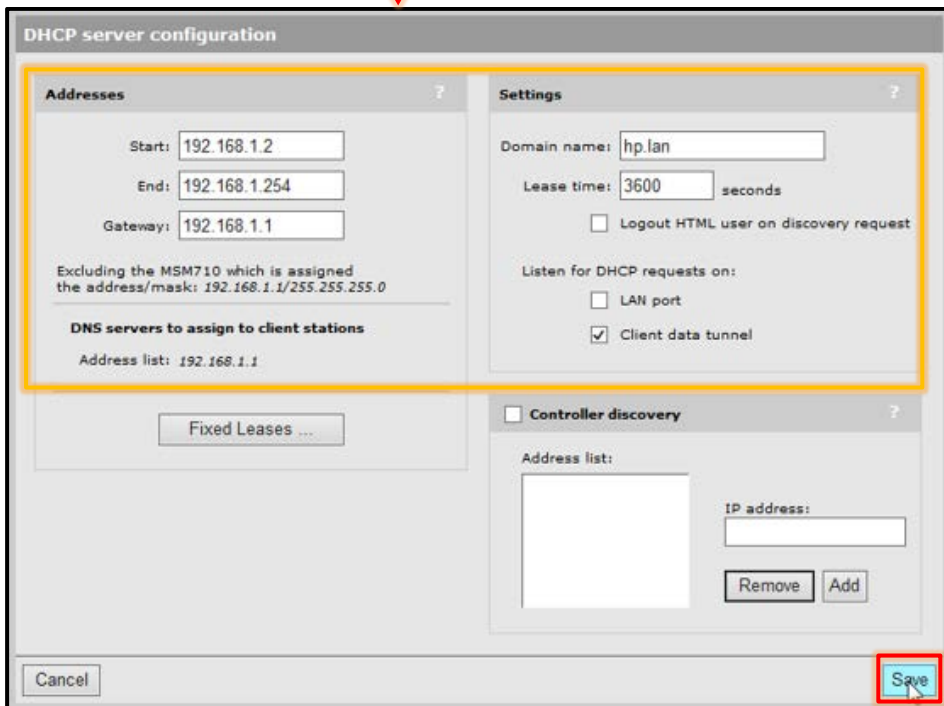
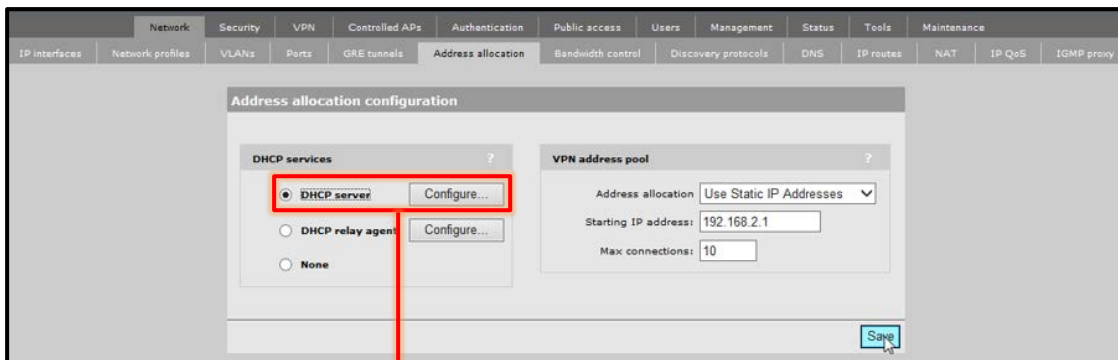
項目	値
IP address	172.16.0.1
Address mask	255.255.255.0

6-2-2 DHCP サーバーの起動

ゲストユーザーに対して、コントローラーから IP アドレスを付与するために、DHCP サーバーを起動します。

「Network Tree」の[Controller]より[Network]-[Address allocation]において、「DHCP services」の「DHCP server」を選択し、「Configure」をクリックします。

「Addresses」において、DHCP プールを設定します。「Settings」において、「LAN port」のチェックを外し、「Save」をクリックします。



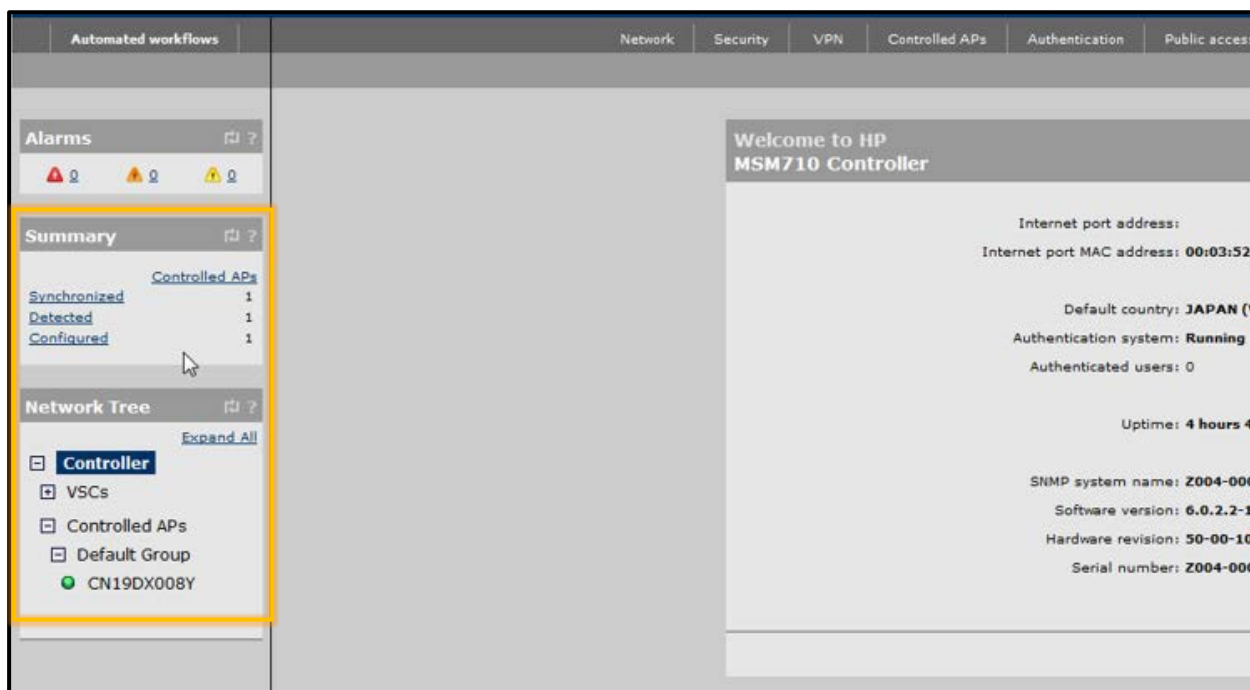
6-2-3 アクセスポイントの接続と認識

Provisioning 設定を行ったアクセスポイントを接続します。

アクセスポイントとコントローラーが IP 通信できている場合は「summary」欄にアクセスポイントの状態が表示されます。

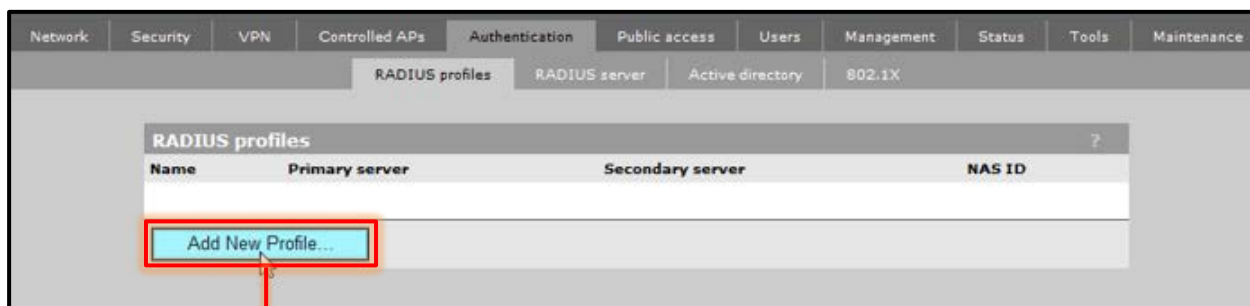
表示項目	説明
Synchronized	アクセスポイントとコントローラーのコンフィグが同期しています
Unsynchronized	アクセスポイントとコントローラーコンフィグに差異があります
Detected	コントローラーが発見したアクセスポイント数が表示されます
Configured	コントローラーからコンフィグを流したアクセスポイント数が表示されます
Pending	コントローラーがアクセスポイントに対して操作を行っています

正常に認識がされた場合は、「Network Tree」の[Controller]-[Controlled APs]-[Default Group]にアクセスポイントが表示され、インジケーターは緑で表示されます。



6-2-4 RADIUS サーバーの指定

「Network Tree」の[Controller]より[Authenticate]-[RADIUS profiles]の「Add New Profile」をクリックします。「Profile name」を入力し、「Settings」の「Authentication method」を「PAP」に変更します。「Primary RADIUS server」に RADIUS サーバーの IP アドレス、シークレットを入力します。「Save」をクリックします。



Add/Edit RADIUS profile

Profile name
Profile name: Net Attest EPS

Settings
 Authentication port: 1812
 Accounting port: 1813
 Retry interval: 10 seconds
 Retry
 timeout: 60 seconds
 Authentication method: MSCHAPv2
 NAS ID: Z004-00043
 Always try primary server first
 Use message authenticator
 Force NAS-Port to ingress VLAN ID
 Override NAS ID when acting as a RADIUS proxy

Primary RADIUS server
 Server address: 192.168.1.2
 Secret: *****
 Confirm secret: *****

Secondary RADIUS server (optional)
 Server address:
 Secret:
 Confirm secret:

Authentication realm
 Changing the realm configuration will logout all authenticated users.
 Associated realms:
 Support regular expressions in realm names
 New realm:
 Remove Add

Cancel Save

項目	値
Profile name	NetAttest EPS
Authentication method	PAP
Server address	192.168.1.2
Secret	secret



6-2-5 VSC の作成

「Network Tree」の[Controller]-[VSCs]より、今回はデフォルト VSCである「HP」をクリックします。

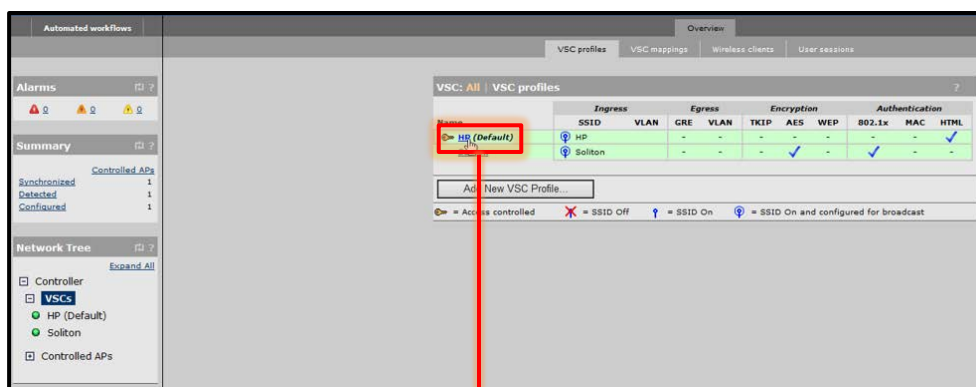
「Use Controller for」の「Authentication」、「Access Control」のチェックを入れます。

「Wireless Protection」にチェックを入れ、「WPA」を選択します。「Mode」に「WPA2」を選択し、「Key source」は「Preshared Key」を選択します。

「Client data tunnel」の「Always tunnel client traffic」にチェックを入れ、「HTML-based user logins」にチェックを入れます。

「Authentication」で「Remote」をチェックし、[6-1-4]で作成したプロファイルを選択します。

「Save」をクリックします。

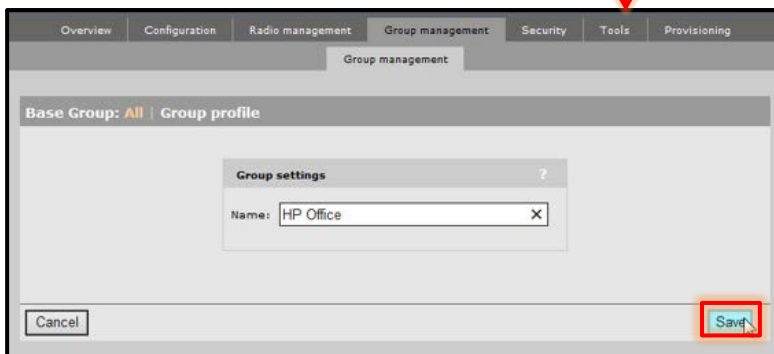
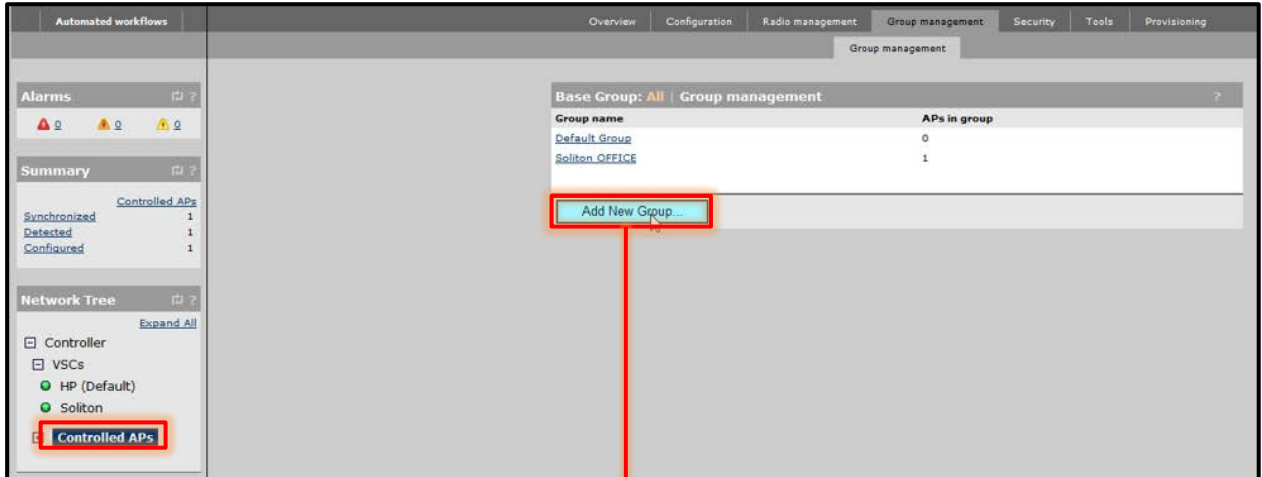


項目	値
Profile name	HP
Name(SSID)	HP
Wireless Protection	WPA
Mode	WPA2
Key source	Preshared Key
Authentication	NetAttes EPS

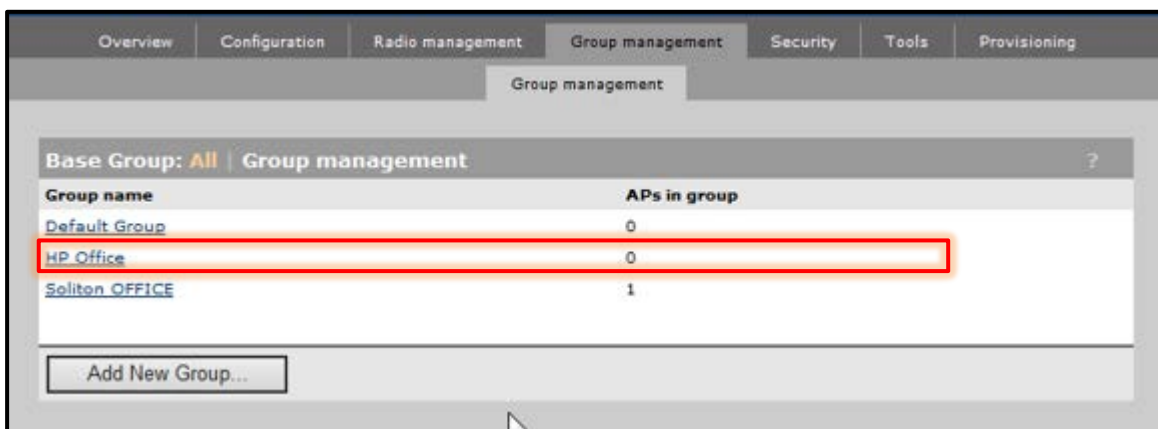
6-2-6 AP グループの追加

「Network Tree」の[Controller]-[Controlled APs]より、[Group management]の「Add New Group」をクリックします。

「Group settings」に任意のグループ名を入力します。「Save」をクリックします。



項目	値
Name	HP OFFICE



6-2-7 AP 名、グループの変更

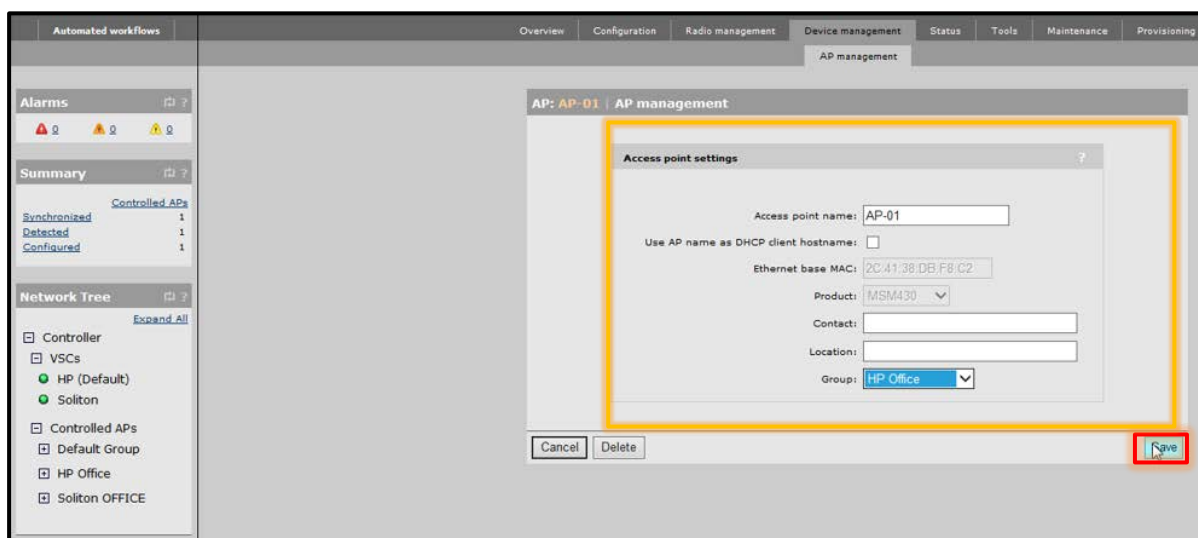
「Network Tree」の[Controller]-[Controlled APs]-[Default Group]に表示されているアクセスポイントをクリックします。

※デフォルトはシリアルナンバーがアクセスポイント名となっています。

[Device management]-[AP management]の「Access point name」を変更し、「Group」は[6-1-6]で追加したグループを選択します。「Save」をクリックします。

「Save」をクリックすると、[Network Tree]の[Controller]-[Controlled APs]の[Default Group]から作成したグループへアクセスポイントが移動します。

インジケータは黄色になり、「Summary」では「Unsynchronized」となります。



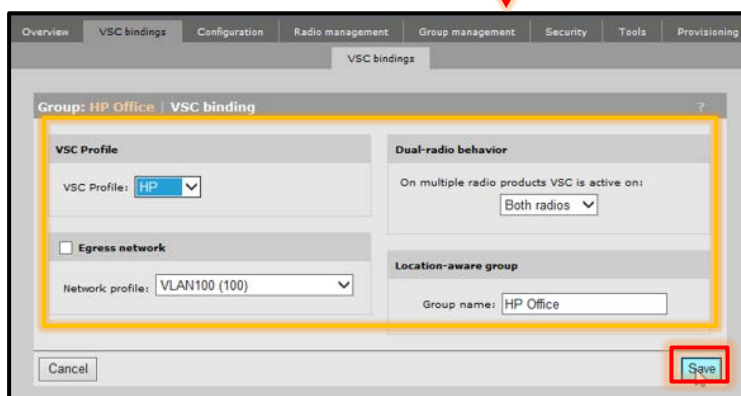
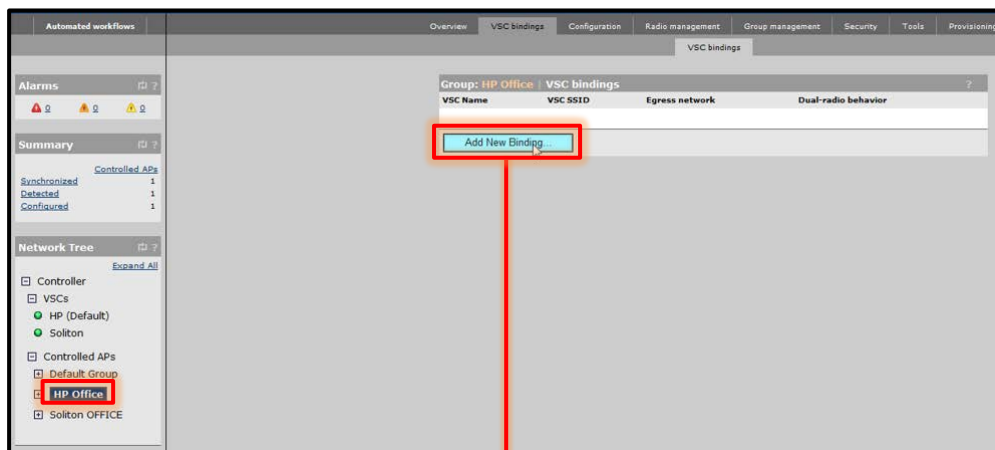
項目	値
Access point name	AP-01
Group	HP OFFICE

6-2-8 グループと VSC の紐付け

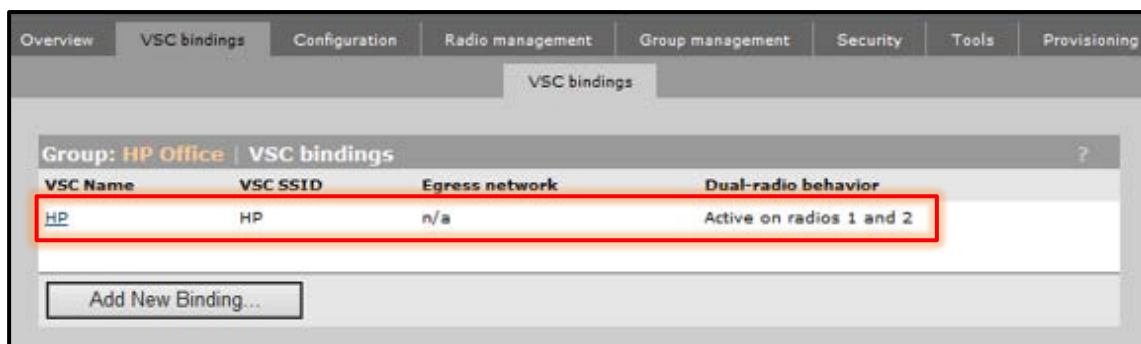
作成したグループは何も SSID を出力していない状態です。VSC を紐付けることで、SSID を出力します。

「Network Tree」の[Controller]-[Controlled APs]の作成したグループより[VSC bindings]の「Add New Binding」をクリックします。

「VSC Profile」にて[6-1-5]で作成した VSC を選択します。「Save」をクリックします。

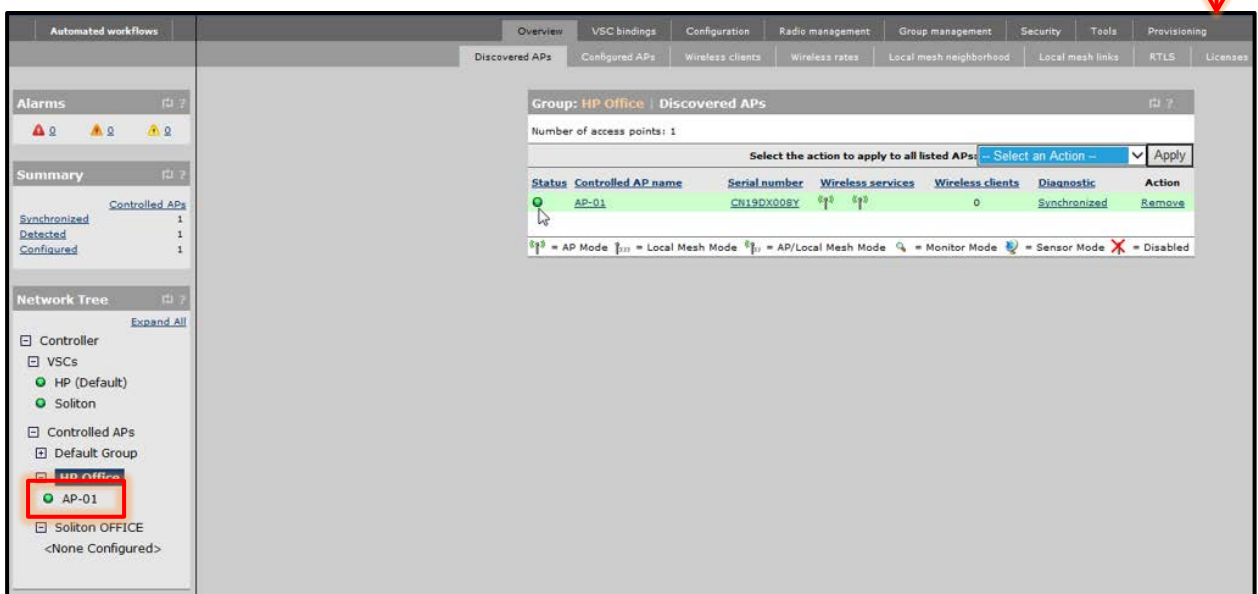
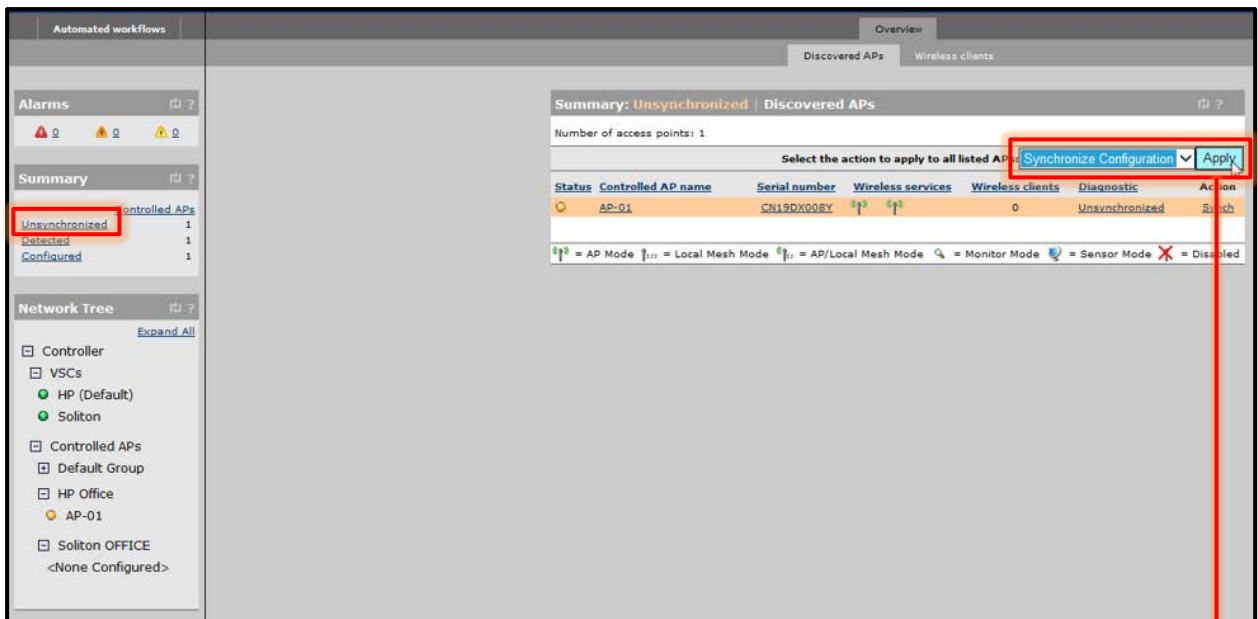


項目	値
VSC Profile	HP



6-2-9 コンフィグの同期

ここまでは、アクセスポイントのコンフィグの作成を行いました。コントローラーとアクセスポイントを同期させることによって、アクセスポイントから設定した SSID が出力できるようになります。[Summary]の「Unsynchronized」をクリックし、「Select the action to all listed APs」で「Synchronize Configuration」を選択し、「Apply」をクリックします。[Summary]にて「Synchronized」となり、アクセスポイントのインジケータが緑に表示されれば、同期が完了となります。



6-3 iOS (iPad)

iPadにてSSID「HP」をタップするとWEBページにリダイレクトされます。

「Username」、「Password」を求められますので、今回は「Password」部分に弊社で取り扱っている、VASCO社製のワンタイムパスワードを入力します。

※ワンタイムパスワードである「DIGIPASS」はハードウェアタイプ、ソフトウェアタイプ(Windows、iOS、Android)をご用意しております。ソフトウェアタイプの各OSでのアクティベーション方法などは割愛させていただきます。詳しくは、「ワンタイムパスワード 利用者向け簡易設定手順書」をご参照ください。



項目	値
Username	User01
Password	ワンタイムパスワード

7. 証明書配布ソリューション連携について

EAP-TLS 認証に必要なクライアントへの証明書配布について、マルチデバイス対応の証明書配布ソリューション「NetAttest EPS-ap」との連携も可能です。コントローラーのキャプティブポータル機能と連携し、未登録端末は証明書発行申請ページへ誘導させることができます。

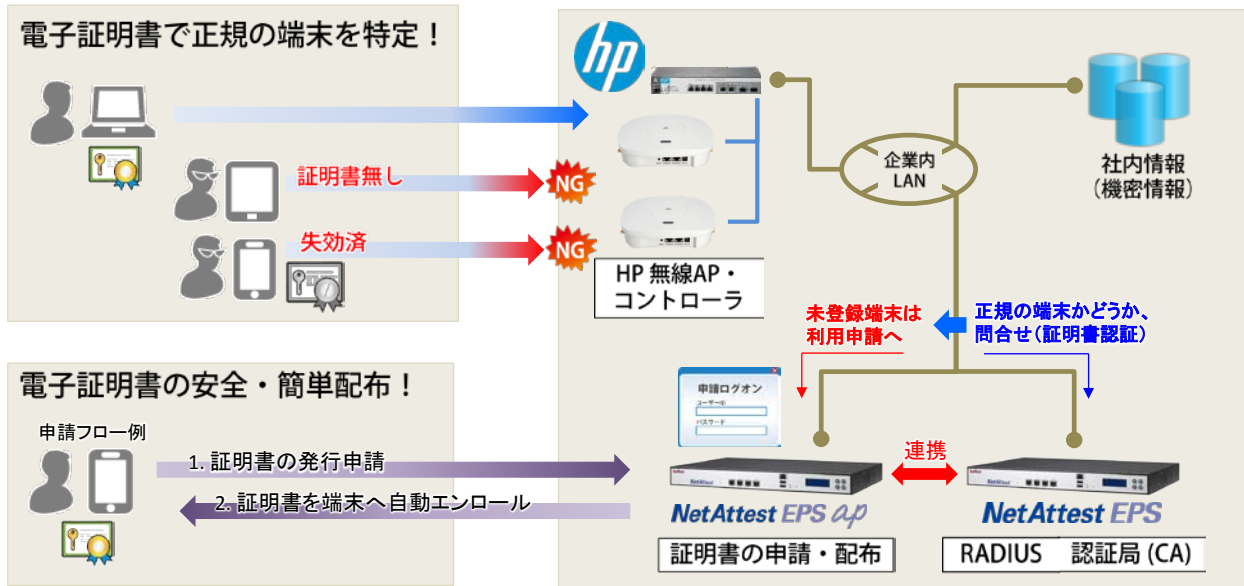


図 証明書配布ソリューションとの連携イメージ

