

NetAttest EPS

認証連携設定例

【連携機器】 RUCKUS ZoneDirector3000

【Case】 IEEE802.1x EAP-TLS 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 RUCKUS 社製 無線 LAN コントローラー ZoneDirector 3000 の IEEE802.1x EAP-TLS 環境での接続について、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 ZoneDirector 3000 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

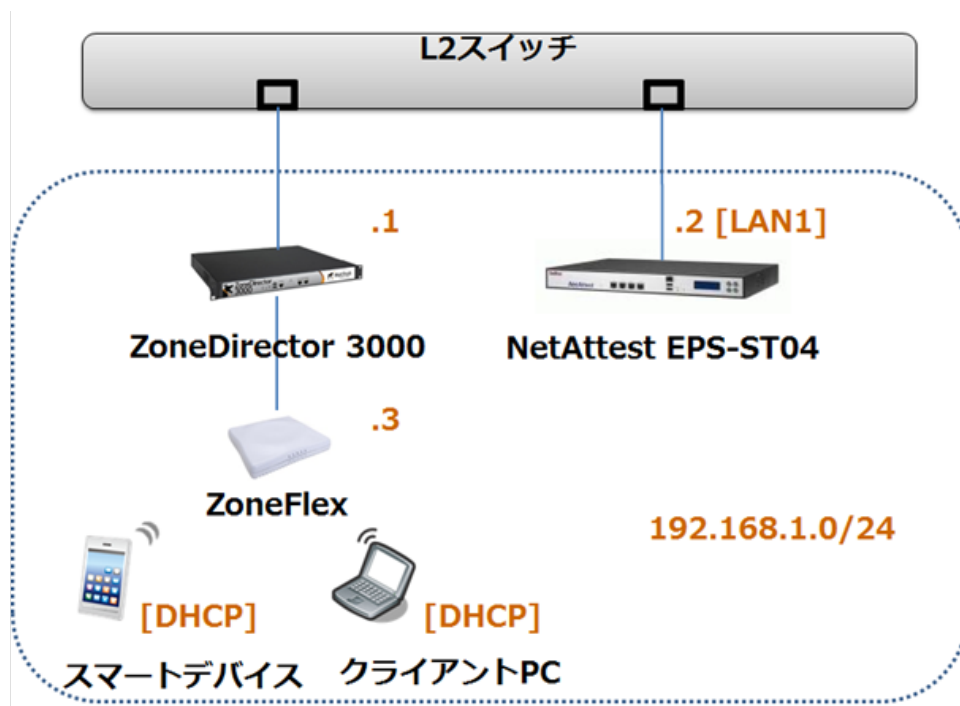
1. 構成.....	6
1-1 構成図.....	6
1-2 環境.....	7
1-2-1 機器.....	7
1-2-2 認証方式.....	7
1-2-3 ネットワーク設定.....	7
2. NetAttest EPS の設定.....	9
2-1 システム初期設定ウィザードの実行.....	9
2-2 システム初期設定ウィザードの実行.....	10
2-3 サービス初期設定ウィザードの実行.....	11
2-4 ユーザーの登録.....	12
2-5 クライアント証明書の発行.....	13
3. RUCKUS ZoneDirector 3000 の設定.....	14
3-1 ZoneDirector IP アドレス設定.....	14
3-2 セットアップウィザード.....	16
3-3 AAA(RADIUS)の設定.....	19
3-4 WLAN 設定.....	20
3-5 WLAN Group 設定.....	21
3-6 Access Point Group へ WLAN の割り当て.....	22
3-7 ZoneFlex IP アドレス設定.....	23
3-8 ZoneDirector と ZoneFlex との接続確認.....	25
4. 無線 LAN クライアントの設定.....	26
4-1 Windows7.....	26
4-1-1 Windows7 へのデジタル証明書のインストール.....	26
4-1-2 サブリカントの設定.....	28
4-2 iOS (iPad).....	29
4-2-1 iOS へのデジタル証明書のインストール.....	29
4-2-2 サブリカントの設定.....	30
4-3 Android (Nexus7).....	31
4-3-1 Android へのデジタル証明書のインストール.....	31

4-3-2 サプリカントの設定.....	32
5. 無線 LAN クライアントの設定.....	33

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)	Ver. 4.4.4
ZoneDirector 3000	RUCKUS	Authenticator (認証機器)	Ver. 9.6.0.0
ZoneFlex	RUCKUS	無線 AP	Ver. 9.6.0.0
Let's note CF-SX2	Panasonic	Client PC (802.1x クライアント)	Windows 7 64bit Windows 標準サブリカント
iPad(第3世代)	Apple	Client Tablet① (802.1x クライアント)	Ver. 5.1.1
Nexus 7	Google	Client Tablet② (802.1x クライアント)	Ver. 4.2.2

1-2-2認証方式

IEEE802.1x EAP-TLS 認証

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
ZoneDirector 3000	192.168.1.1/24		secret
ZoneFlex	192.168.1.3/24	-	-
Client PC	DHCP	-	-
Client Tablet①	DHCP	-	-
Client Tablet②	DHCP	-	-

2. NetAttest EPS の設定

2-1 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ーから「<http://192.168.2.1:2181/>」にアクセスしてください。

下記のような流れでセットアップを行います。

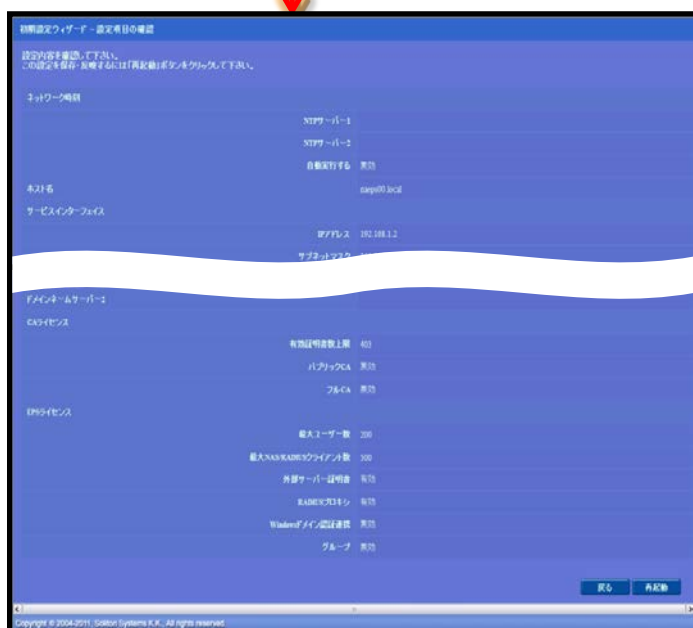
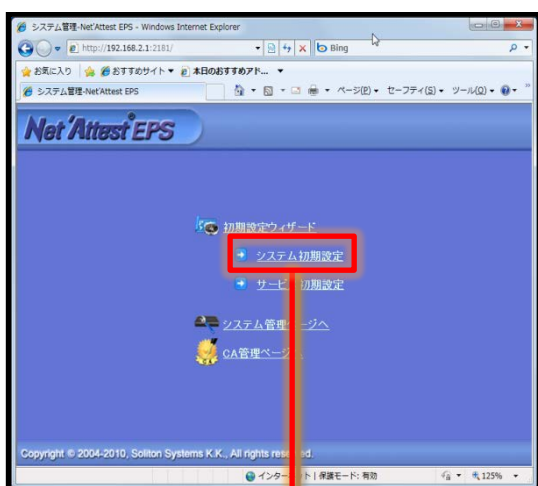
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

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ーから「http://192.168.2.1:2181/」にアクセスしてください。

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。

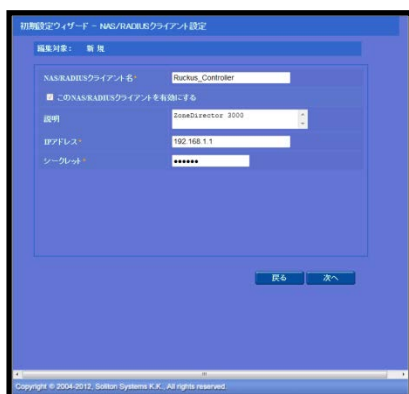
- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定 (全般)
- RADIUS サーバーの基本設定 (EAP)
- RADIUS サーバーの基本設定 (証明書検証)
- NAS/RADIUS クライアント設定



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



項目	値
EAP 認証タイプ	TLS



項目	値
NAS/RADIUS クライアント名	RUCKUS_Controller
IP アドレス	192.168.1.1
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。

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

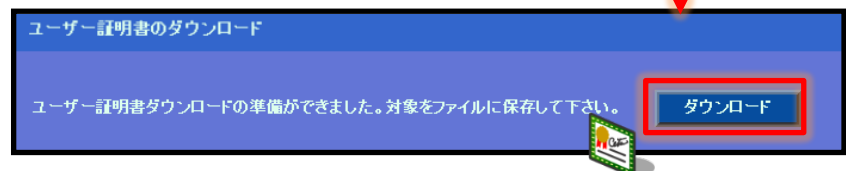
2-5クライアント証明書発行

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)



項目	値
証明書有効期限	365
PKCS#12 ファイルに証明機関の・・・	チェック有



3. RUCKUS ZoneDirector 3000 の設定

3-1 ZoneDirector IP アドレス設定

工場出荷状態の ZoneDirector は、起動時に DHCP サーバーからアドレスを取得します。取得できなかった場合には、自動的に IP アドレス 192.168.0.2/24 を自身に割り当てます。設定を行う PC に適切な IP アドレスを設定した後、Web ブラウザを起動し、ZoneDirector に Web 接続してセットアップウィザードを開始します。なお、ZoneDirector に任意の IP アドレスを割り当てて設定したい場合には、一度 CLI から ZoneDirector の IP アドレスを設定する必要があります。

コンソールを接続し、PC 上のターミナルソフトウェアを起動し接続します。

【ターミナルソフトウェアの設定】

ボーレート	データビット	パリティ	ストップビット	フロー制御
115200	8 bit	none	1 bit	none

コンソール接続後、ログインし、Enable モードに入ります。

```
Please login: admin
Password: [admin(default)]
Welcome to the RUCKUS Wireless ZoneDirector 3000 Command Line Interface
RUCKUS> enable
RUCKUS#
```

ログイン後、「config mode」に入り、以下の手順で IP Static mode, IP Gateway, IP Addressを設定します。CLIで設定した内容は、「exit」コマンド実施後にフラッシュメモリへ保存されます。必ず設定後は、「exit」コマンドを実行してください。

IP アドレスの設定が完了したら、設定を行う PC に適切な IP アドレスを設定した後、ZoneDirector に Web 接続してセットアップウィザードを開始します。

```
RUCKUS# config
RUCKUS(config)# system
RUCKUS(config-sys)# interface
RUCKUS(config-sys-if)# ip mode static
The command was executed successfully. To save the changes, type 'end' or 'exit'.
RUCKUS(config-sys-if)# ip route gateway 192.168.1.2 254
The command was executed successfully. To save the changes, type 'end' or 'exit'.
RUCKUS(config-sys-if)# ip addr 192.168.1.1 255.255.255.0
The command was executed successfully. To save the changes, type 'end' or 'exit'.
RUCKUS(config-sys-if)# exit
The device IP settings has been updated.
Your changes have been saved.
RUCKUS(config-sys)# exit
Your changes have been saved.
RUCKUS(config)# exit
Your changes have been saved.
RUCKUS# exit
Exit RUCKUS CLI.
```

3-2 セットアップウィザード

Language の選択を行います。このガイドでは、日本語で進めます。「次へ」をクリックします。

RUCKUS WIRELESS セットアップ ウィザード

言語

全般

管理 IP

ワイヤレス LAN

管理者

確認

完了

言語 Japanese (日本語)

< 戻る 次へ >

項目	値
言語	Japanese(日本語)

システム名を入力し、国コード Japan を選択し、「次へ」をクリックします。

RUCKUS WIRELESS セットアップ ウィザード

言語

全般

管理 IP

ワイヤレス LAN

管理者

確認

完了

システム名 ruckus

国コード Japan

ZD では、メッシュ機能を利用することができます。ZD でメッシュを有効にするには、それぞれの ZD に、バックボーントラフィックのメッシュ WLAN に一意の名前 (SSID) を指定する必要があります。

メッシュを有効にする

< 戻る 次へ >

項目	値
システム名	RUCKUS
国コード	Japan

IP 情報を入力し、「次へ」をクリックします。

管理 IP

ネットワークアドレス指定モードを [手動] と [DHCP] のいずれかから選択してください。[DHCP] を選択した場合、他の情報は必要ありません。[手動] を選択した場合は、関連するアドレス指定情報を入力してください (アスタリスク (*) の付いていないフィールドは省略可能です)。

IPv4 IPv6 IPv4 and IPv6

手動 DHCP

IP Address * 192.168.1.1

Netmask * 255.255.255.0

Gateway * 192.168.1.254

プライマリ DNS サーバー

セカンダリ DNS サーバー

項目	値
IP Address	192.168.1.1
Netmask	255.255.255.0
Gateway	192.168.1.254

ワイヤレス LAN 情報を入力します。ここでは SSID を 1 つだけ設定することができます。複数の SSID を設定する場合にはセットアップウィザード終了後に追加することが可能です。ESSID 名を入力し、「次へ」をクリックします。

ワイヤレス LAN

既定の設定を変更しない場合は、オープン認証を使用する既定の WLAN である "Wireless 1" が作成されます。WPA_PSK 認証を選択しパスワードを設定することによって、WLAN のセキュリティを高めることができます。またオプションとして、一時的なゲスト アクセス用の "Guest" WLAN を作成することができます (使用制限付きの WLAN を後から追加することもできます)。

Wireless 1 -- 最初のワイヤレス LAN を作成します

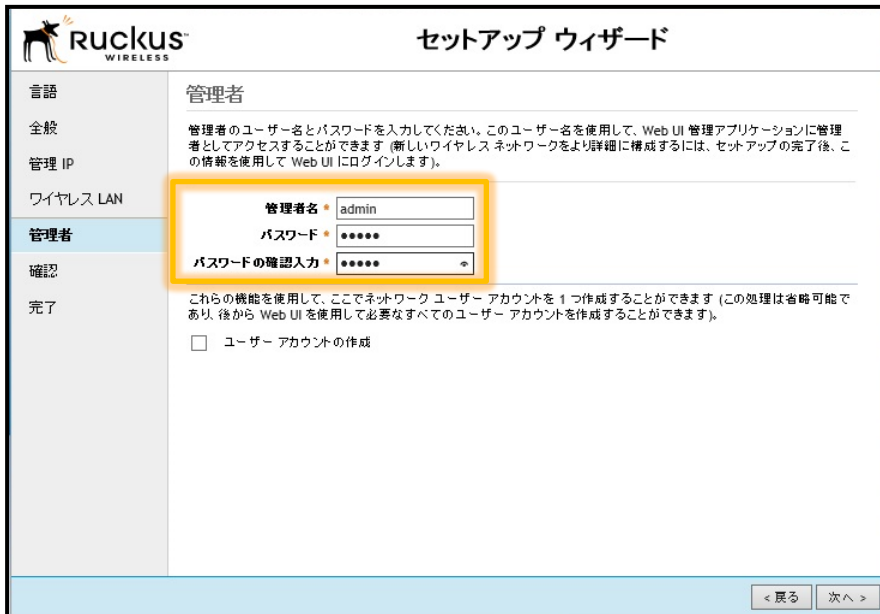
名前 (ESSID) * Ruckus-Wireless-1

認証 オープン WPA_PSK

Guest WLAN -- 訪問者用の一時的なアクセス。

項目	値
名前	RUCKUS-Wireless-1
認証	オープン

ZoneDirector の管理者(admin) のパスワードを変更し、「次へ」をクリックします。



RUCKUS WIRELESS セットアップ ウィザード

言語 管理者

全般 管理者のユーザー名とパスワードを入力してください。このユーザー名を使用して、Web UI 管理アプリケーションに管理者としてアクセスすることができます (新しいワイヤレス ネットワークをより詳細に構成するには、セットアップの完了後、この情報を使用して Web UI にログインします)。

管理 IP

ワイヤレス LAN

管理者

確認

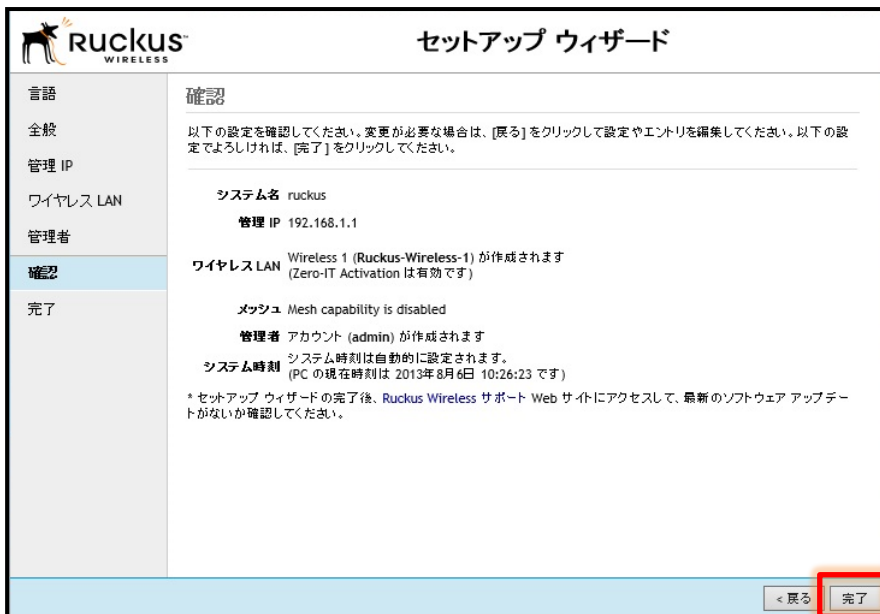
完了

これらの機能を使用して、ここでネットワーク ユーザー アカウントを 1 つ作成することができます (この処理は省時可能であり、後から Web UI を使用して必要なすべてのユーザー アカウントを作成することができます)。

ユーザー アカウントの作成

< 戻る 次へ >

実施したセットアップウィザードの内容を確認します。よければ「完了」をクリックします。



RUCKUS WIRELESS セットアップ ウィザード

言語 確認

全般 以下の設定を確認してください。変更が必要な場合は、[戻る] をクリックして設定やエントリを編集してください。以下の設定でよろしければ、[完了] をクリックしてください。

管理 IP

ワイヤレス LAN

管理者

確認

完了

システム名 ruckus

管理 IP 192.168.1.1

ワイヤレス LAN Wireless 1 (Ruckus-Wireless-1) が作成されます (Zero-IT Activation は有効です)

メッシュ Mesh capability is disabled

管理者 アカウント (admin) が作成されます

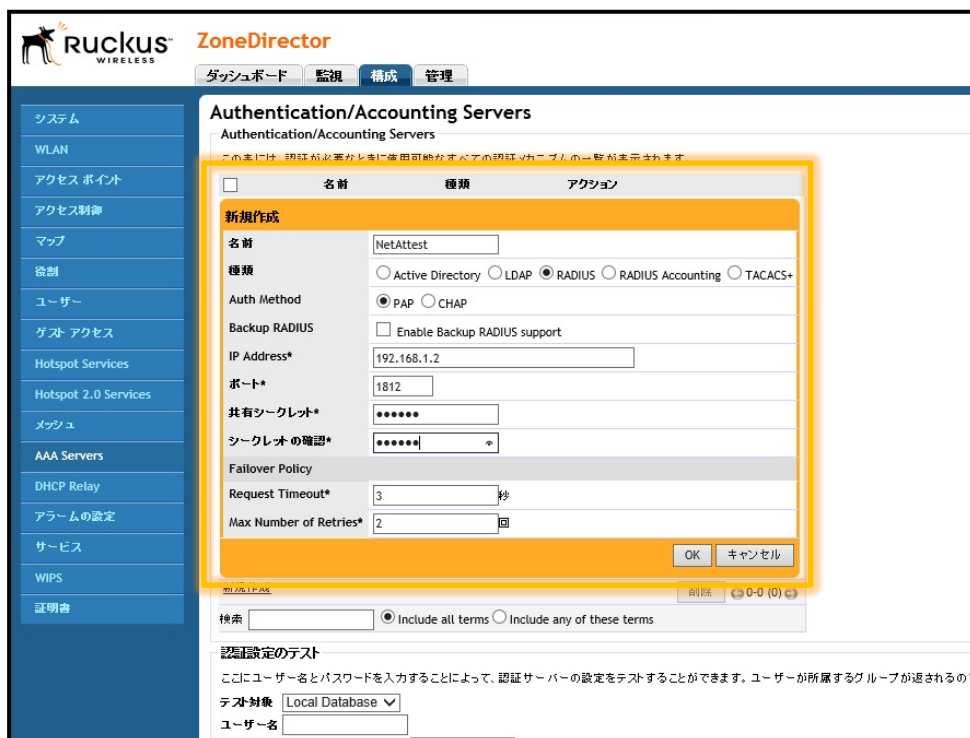
システム時刻 システム時刻は自動的に設定されます。 (PC の現在時刻は 2013年8月6日 10:26:23 です)

* セットアップ ウィザードの完了後、Ruckus Wireless サポート Web サイトにアクセスして、最新のソフトウェア アップデートがないか確認してください。

< 戻る 完了

3-3AAA(RADIUS)の設定

RADIUS サーバーの登録を行います。[構成]-[AAA Server]より、「新規作成」をクリックします。RADIUS サーバー名を入力し、認証の種類では RADIUS を、Auth Method では RADIUS の認証方式に合致するものを選択します。IP Address、RADIUS サーバーとの共通シークレットを入力し、「OK」をクリックします。



項目	値
名前	NetAttest
種類	RADIUS
Auth Method	PAP
IP Address	192.168.1.2
ポート	1812
共通シークレット	secret

3-4WLAN 設定

先のセットアップウィザードで行った WLAN 設定の編集を行います。新たな WLAN(SSID)を作成したい場合には「新規作成」をクリックします。



認証オプションは以下の通りに設定し、先に作成した認証サーバーを選択します。

Zero IT Activation は無効にしてください。完了したら「OK」をクリックします。なお、SSID を変更する場合には、「ESSID」を編集します。



項目	値
認証オプション	802.1x EAP
暗号化オプション	WPA2 AES
Zero IT Activation	無効

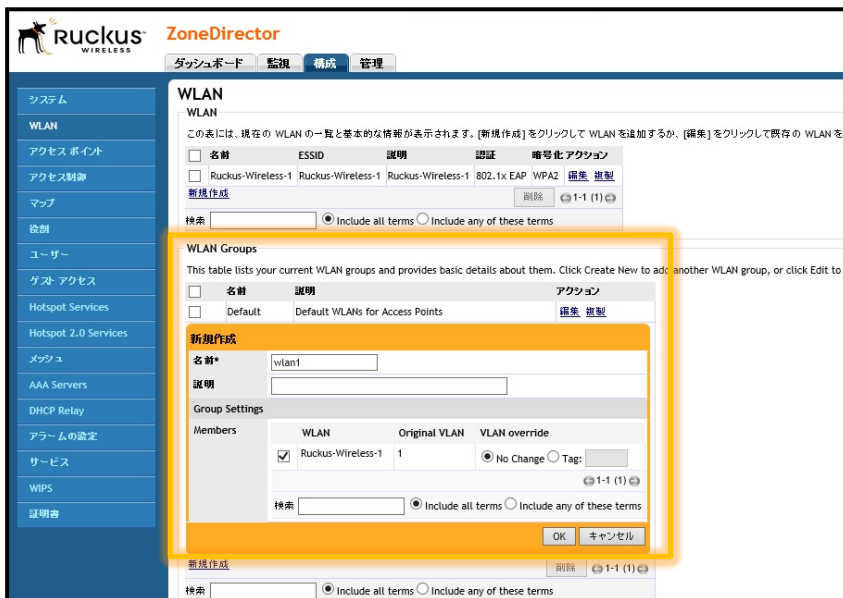
3-5WLAN Group 設定

WLAN グループは、複数の WLAN 設定をグループ化し、それを AP に割り当てることで 1 台の AP に複数の WLAN 設定(SSID)をアサインすることができます。

WLAN Groups より「新規作成」をクリックしてください。



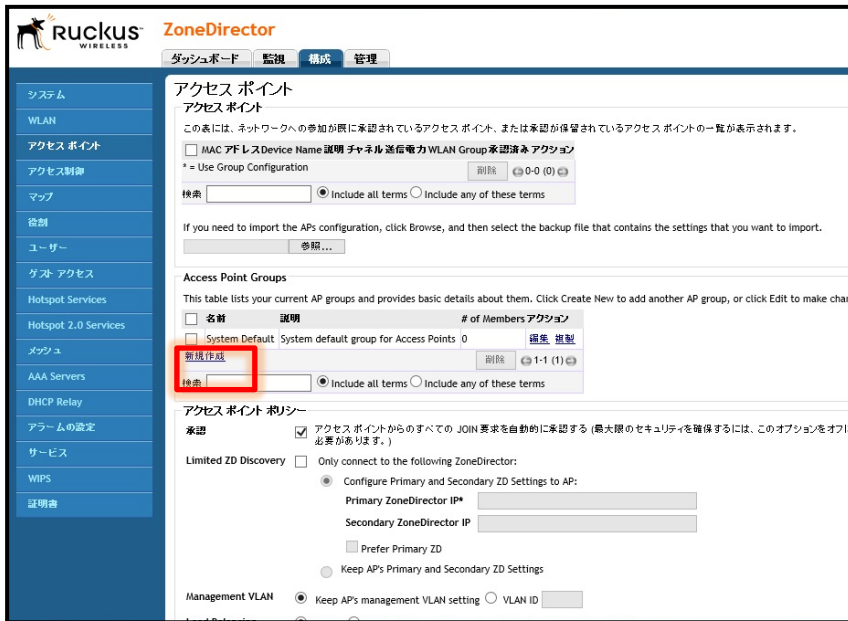
作成した WLAN をグループに含めてください。



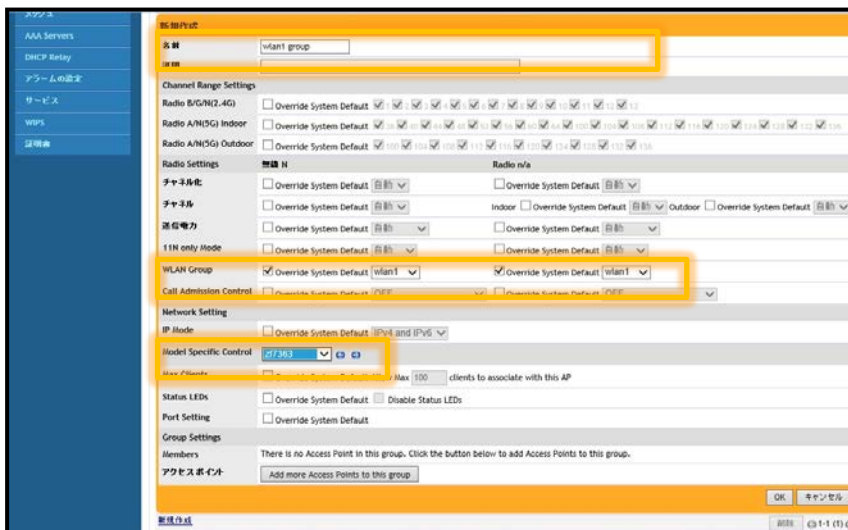
項目	値
名前	802.1x EAP
Members	RUCKUS-Wireless-1

3-6 Access Point Group へ WLAN の割り当て

[3-5]で作成した WLAN 設定を、グループ化した AP に割り当てます。[構成]-[アクセスポイント]-[Access Point Group]より「新規作成」をクリックし新たな Access Point Group を作成します。



Access Point Group の「名前」を入力し、先に作成した WLAN Group を選択します。異なる ZoneFlex のモデルを、同じ Access Point Group にアサインし、それぞれのモデル特有の LED や物理ポートなどに関する設定を行うには Model specific Control で ZoneFlex のモデル名を選択し、設定します。特に指定しない場合には設定する必要はありません。

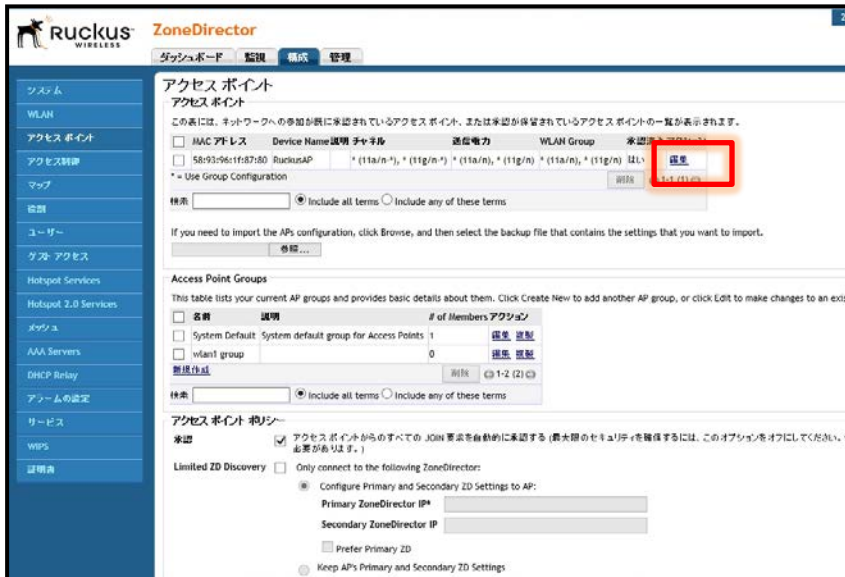


項目	値
名前	wlan1group
Radio Settings	
- 無線 N	wlan1
- Radio n/a	wlan1
Model Specific Control	Zf7363

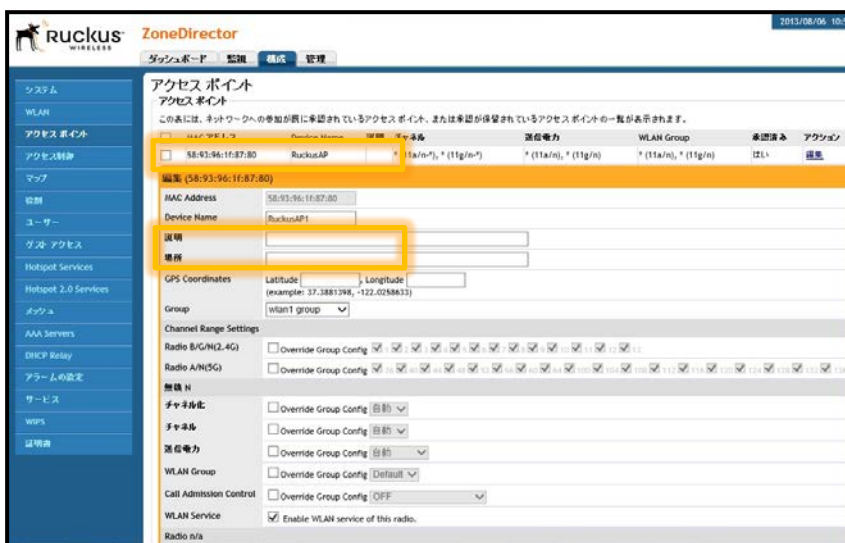
3-7ZoneFlex IP アドレス設定

工場出荷状態の ZoneFlex は、DHCP サーバーからアドレスを取得します。取得できなかった場合には、自動的に IP アドレス 192.168.0.1/24 を自身に割り当てます。

本書では、AP(ZoneFlex)の IP アドレスは DHCP で取得し、同一セグメント内にある ZoneDirector から Discover します。[アクセスポイント]より Discover されたアクセスポイントの「編集」をクリックしてください。

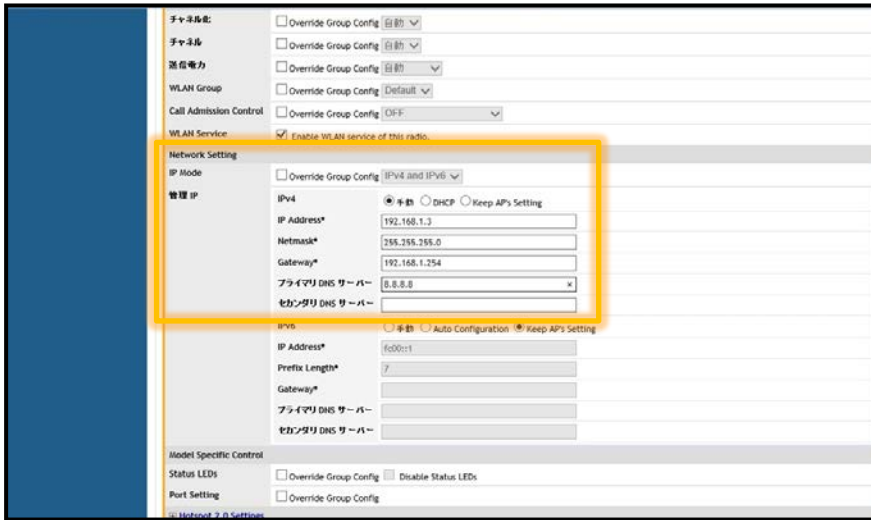


「Device Name」を編集し、「Group」に先ほど作成した AP Group の「wlan1 group」を選択してください。



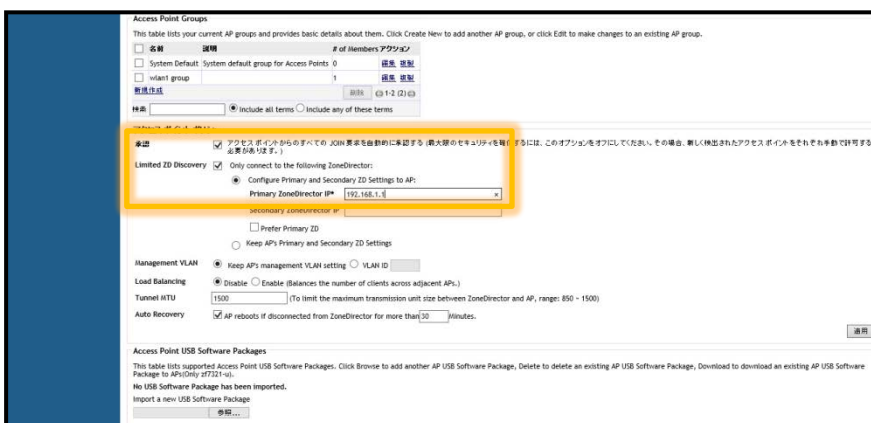
項目	値
Device Names	RUCKUSAP1
Group	wlan1group

画面下の方にスクロールし、管理 IP アドレスで IPv4 を手動に指定し、IP Address, Netmask, Gateway, DNS を指定します。



項目	値
IPv4	手動
IP Address	192.168.1.3
Netmask	255.255.255.0
Gateway	192.168.1.254
プライマリ DNS サーバー	8.8.8.8

さらにスクロールし、アクセスポイントポリシーにて「Primary ZoneDirector IP」を指定します。これを指定することによって、スタティックに ZoneDirector の IP アドレスを割り当て、異なるセグメントでも ZoneDirector から Discover できます。



項目	値
Primary ZoneDirector IP	192.168.1.1

3-8ZoneDirectorとZoneFlexとの接続確認

[監視]-[アクセスポイント]より、ZoneFlexのステータスが「接続」となっていることを確認します。

The screenshot shows the Ruckus ZoneDirector web interface. The left sidebar contains navigation options like 'アクセスポイント', 'マップビュー', 'WLAN', etc. The main content area is titled 'アクセスポイント' and shows a table of '現在管理されているアクセスポイント' (Currently managed access points). A green box highlights the first row of this table, which shows an access point with MAC address 58:93:96:1f:87:80, device name RuckusAP1, and status '接続' (Connected).

MACアドレス	Device Name	説明	場所	モデル	ステータス	Mesh	Mode	IP Address	External IP:Port	VLAN	チャネル	クライアント	アクション
58:93:96:1f:87:80	RuckusAP1			z7363	接続		Disabled	192.168.1.3	192.168.1.3:12223	1	100 (11a/n-40), 6 (11g/n-20)	0	

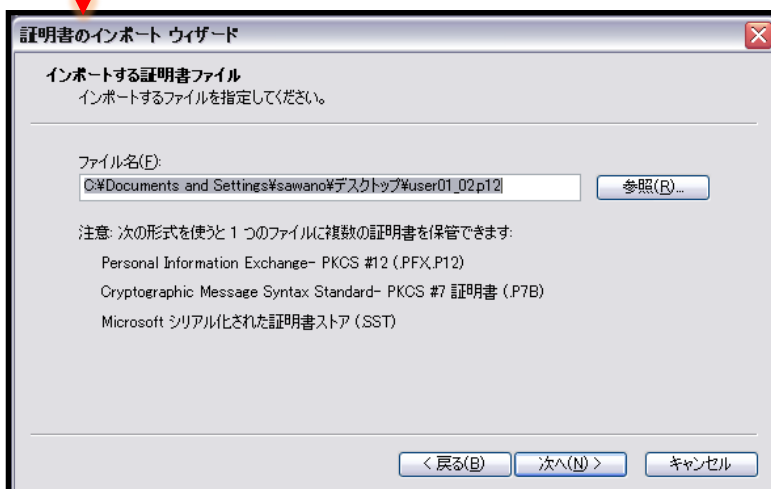
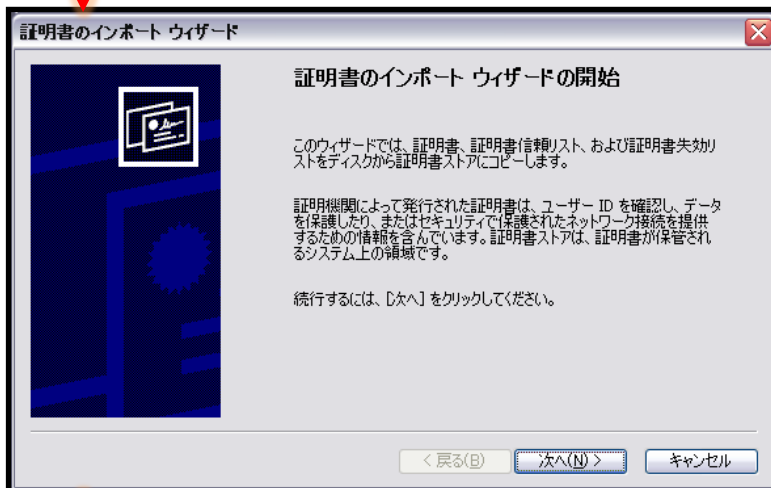
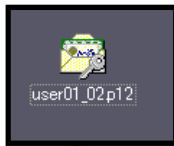
Below the table, there is a section for 'Currently managed AP Groups' with a table showing 'System Default' and 'wlan1 group'. At the bottom, there is an 'イベント/アクティビティ' (Event/Activity) log showing various system events and warnings.

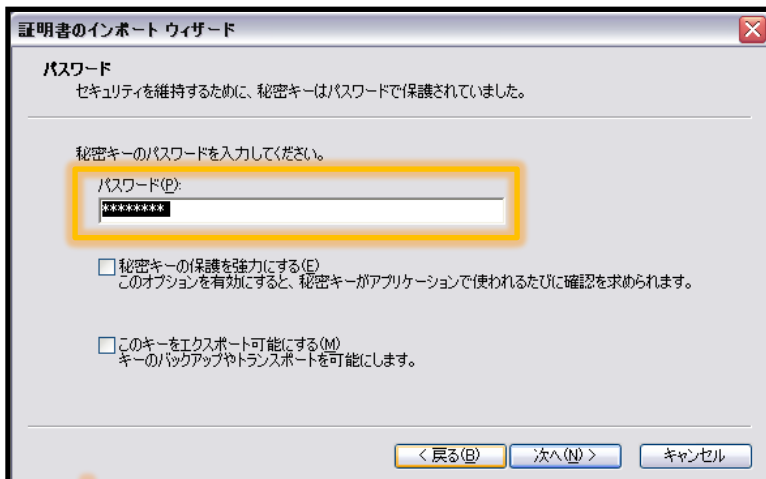
4. 無線 LAN クライアントの設定

4-1Windows7

4-1-1Windows7 へのデジタル証明書のインストール

PC にクライアント証明書をインポートします。ダウンロードしておいたクライアント証明書 (user01_02.p12) をダブルクリックすると、証明書インポートウィザードが実行されます。



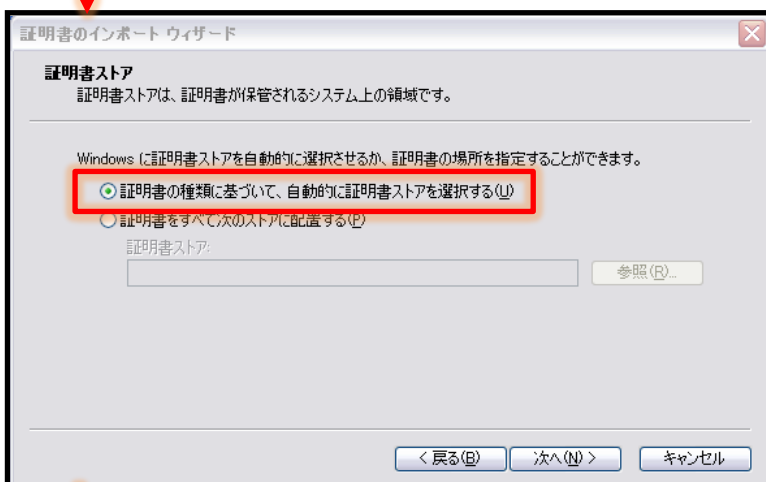


【パスワード】

NetAttest EPS で証明書を
発行した際に設定したパスワードを入力



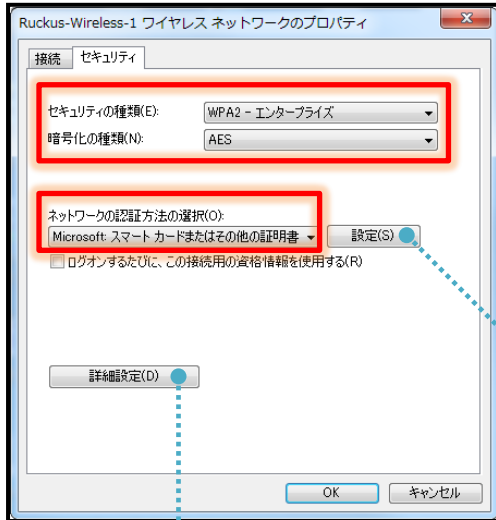
iPhone 構成ユーティリティを利用し iOS デバイスにデジタル証明書をインストールする場合は、【このキーをエクスポート可能にする】チェックを入れる必要があります。



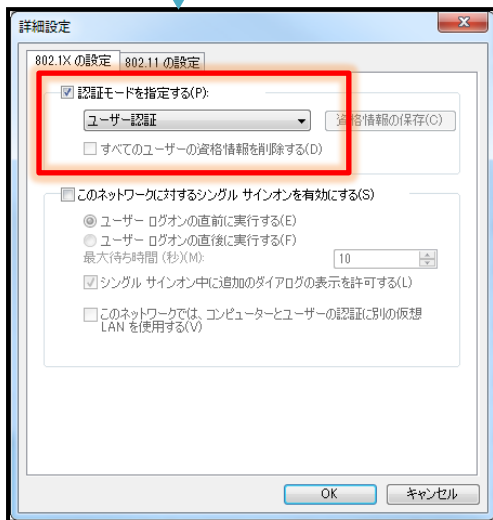
4-1-2 サプリカントの設定

Windows 標準サプリカントで TLS の設定を行います。

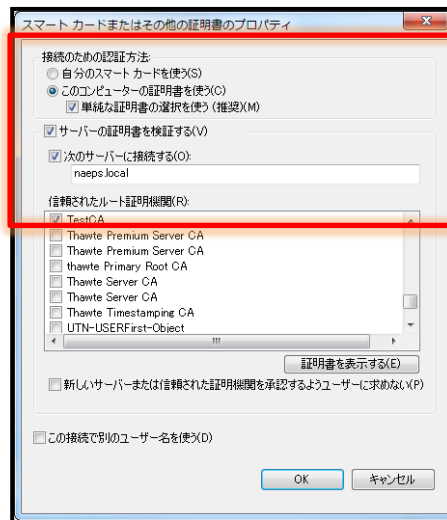
[ワイヤレスネットワークのプロパティ]の「セキュリティ」タブから以下の設定を行います。



項目	値
セキュリティの種類	WPA2-エンタープライズ
暗号化の種類	AES
ネットワーク認証の・・・	Microsoft スマートカード・・・



項目	値
認証モードを指定する	ユーザー認証



項目	値
接続のための認証方法	
- このコンピューターの・・・	On
- 単純な証明書の選択・・・	On
サーバー証明書の検証をする	On
次のサーバーに接続する	naeps.local
信頼されたルート証明機関	TestCA

4-2iOS (iPad)

4-2-1iOS 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。

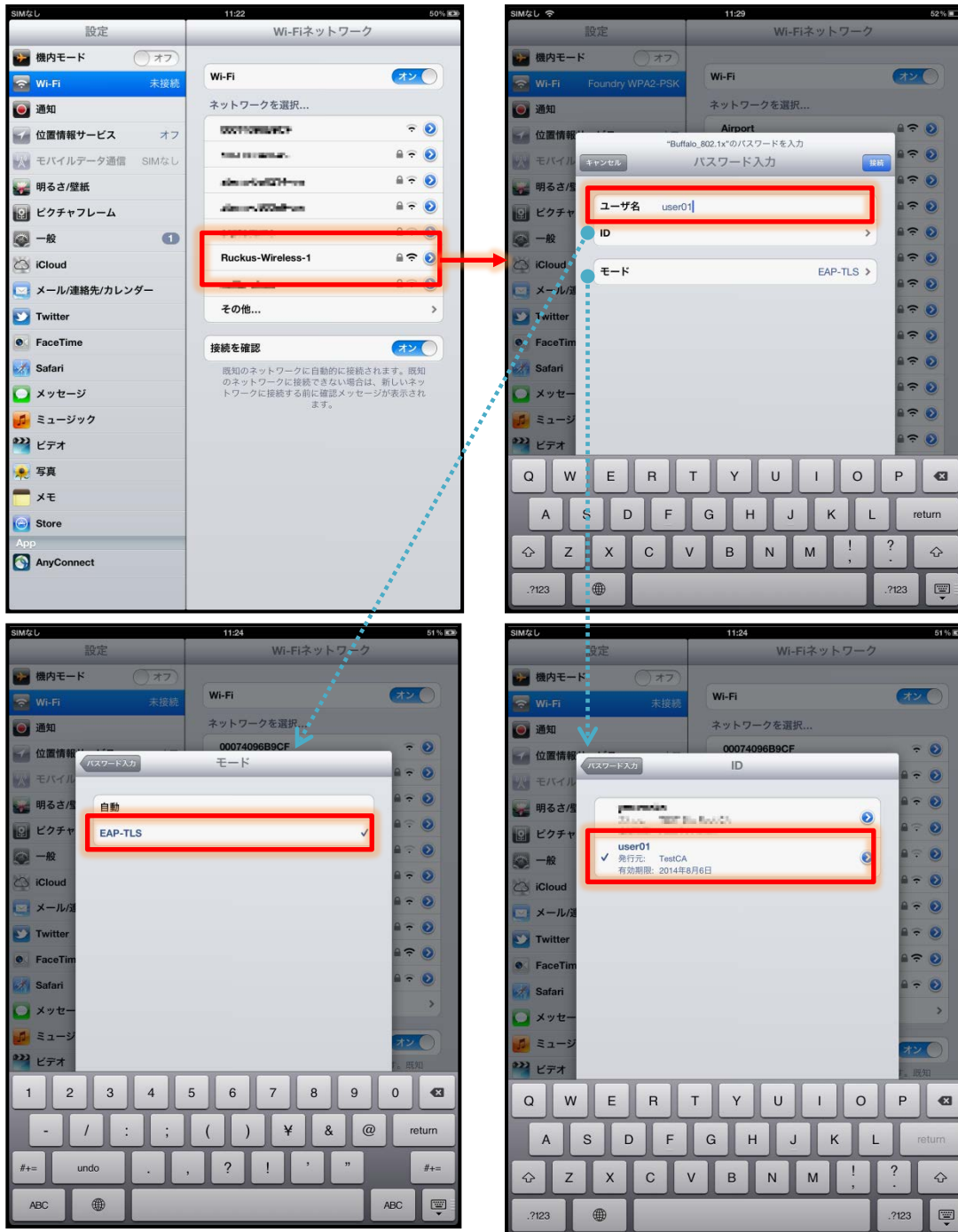
- 1) iPhone 構成ユーティリティ（構成プロファイル）を使う方法
- 2) デジタル証明書をメールに添付し iOS デバイスに送り、インストールする方法
- 3) SCEP で取得する方法(NetAttest EPS-ap を利用できます)

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。

4-2-2 サプリカントの設定

ZoneFlex 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を選択します。



4-3Android (Nexus7)

4-3-1 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。

4-3-2 サプリカントの設定

BZoneFlex で設定した SSID をタップし、サブ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。

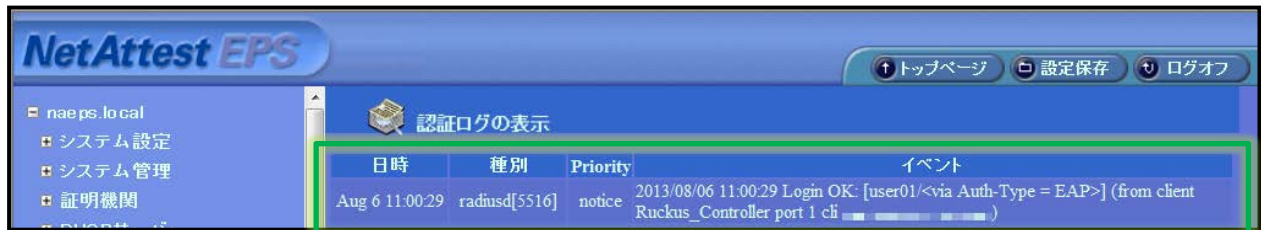
CA 証明書を個別にインストールした場合は、その CA 証明書を選択してください。



項目	値
ネットワーク SSID	RUCKUS-Wireless
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

5. 無線 LAN クライアントの設定

PC から無線 LAN 「RUCKUS-wireless-1」 に接続します。認証が成功すると NetAttest EPS 側に以下のような認証ログが出力されます。



また、ZoneDirector では「監視」-[現在アクティブなクライアント]より、接続中の無線 LAN クライアントを確認することができます。

