

NetAttest EPS

認証連携設定例

【連携機器】 ラッカスネットワークス SmartZone 124

【Case】 IEEE802.1X EAP-TLS/EAP-PEAP

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

本書はオールインワン認証アプライアンス NetAttest EPS と、ラッカスネットワークス社製無線 LAN コントローラー SmartZone 124 の IEEE802.1X EAP-TLS / EAP-PEAP 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。

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 SmartZone 124 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.....	3
1-1 構成図.....	3
1-2 環境.....	4
1-2-1 機器.....	4
1-2-2 認証方式.....	4
1-2-3 ネットワーク設定.....	4
2. NetAttest EPS の設定.....	5
2-1 初期設定ウィザードの実行.....	5
2-2 システム初期設定ウィザードの実行.....	6
2-3 サービス初期設定ウィザードの実行.....	7
2-4 ユーザーの登録.....	8
2-5 クライアント証明書の発行.....	9
3. SmartZone 124 の設定.....	10
3-1 SmartZone 124 の初期化.....	10
3-2 初期設定ウィザードの実行.....	11
3-2-1 Port Configuration.....	11
3-2-2 IP Setting.....	12
3-2-3 Cluster Information.....	13
3-2-4 Administrator.....	13
3-2-5 Confirmation.....	14
3-3 AAA 設定.....	15
3-4 WLAN 設定.....	16
3-5 WLAN Group と AP Group.....	18
3-6 AP セットアップ.....	19
4. EAP-TLS 認証でのクライアント設定.....	22
4-1 Windows 10 での EAP-TLS 認証.....	22
4-1-1 クライアント証明書のインポート.....	22
4-1-2 サブリカント設定.....	24
4-2 iOS での EAP-TLS 認証.....	25
4-2-1 クライアント証明書のインポート.....	25

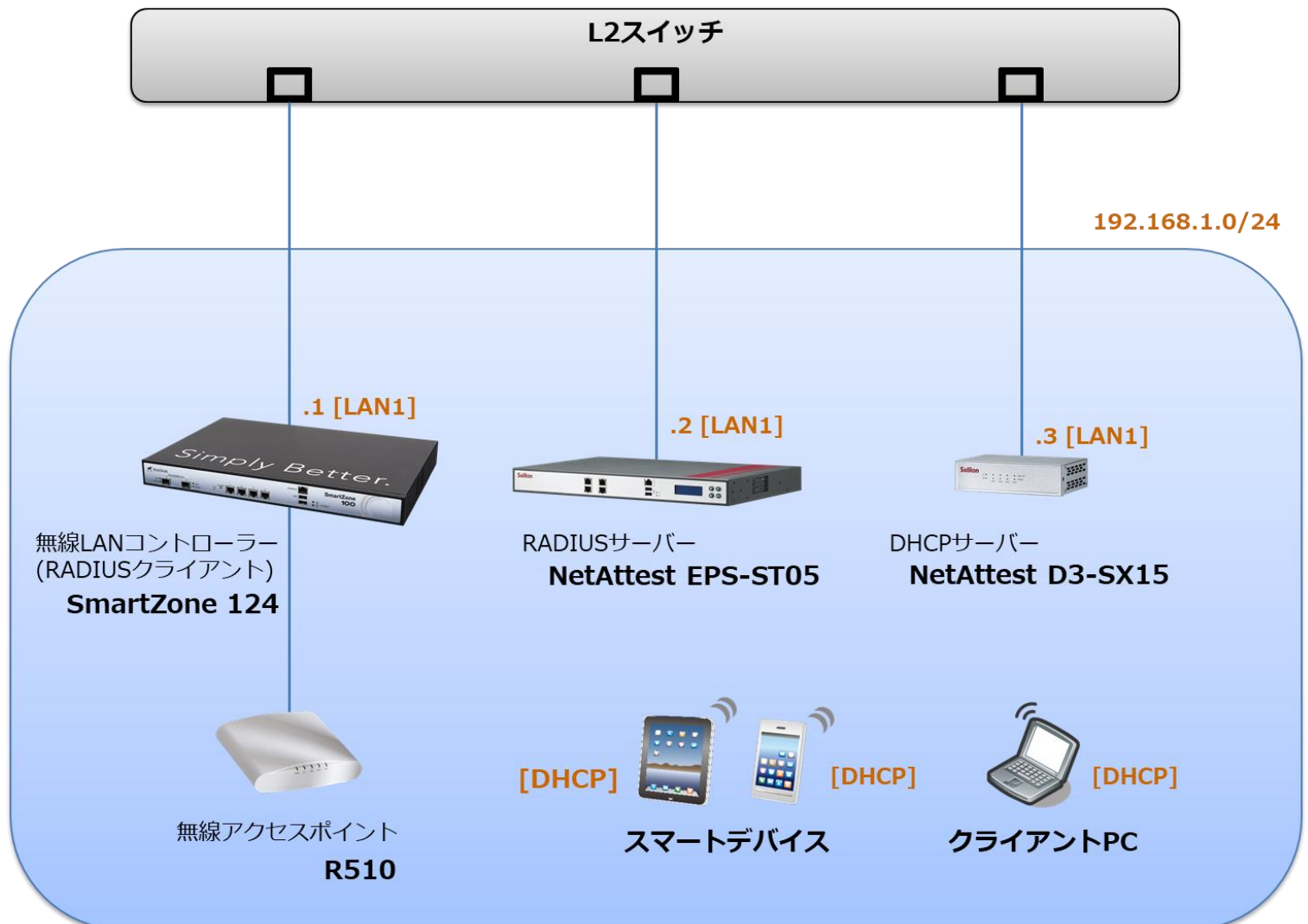
4-2-2 サプリカント設定.....	26
4-3 Android での EAP-TLS 認証.....	27
4-3-1 クライアント証明書のインポート.....	27
4-3-2 サプリカント設定.....	28
5. EAP-PEAP 認証でのクライアント設定.....	29
5-1 Windows 10 での EAP-PEAP 認証.....	29
5-1-1 Windows 10 のサプリカント設定.....	29
5-2 iOS での EAP-PEAP 認証.....	30
5-2-1 iOS のサプリカント設定.....	30
5-3 Android での EAP-PEAP 認証.....	31
5-3-1 Android のサプリカント設定.....	31
6. 動作確認結果.....	32
6-1 EAP-TLS 認証.....	32
6-2 EAP-PEAP 認証.....	32

1. 構成

1-1 構成図

以下の環境を構成します。

- 有線 LAN で接続する機器は L2 スイッチに収容
- 有線 LAN と無線 LAN は同一セグメント
- 無線 LAN で接続するクライアント PC の IP アドレスは、NetAttest D3-SX15 の DHCP サーバーから払い出す



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-ST05	ソリトンシステムズ	RADIUS/CA サーバー	4.10.4
SmartZone 124	ラッカスネットワークス	RADIUS クライアント (無線 LAN コントローラー)	ver. 5.1.0.0.496
R510	ラッカスネットワークス	無線アクセスポイント	Ver.5.1.0.0.595
VAIO Pro PB	VAIO	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サブリカント
iPhone 7	Apple	802.1X クライアント (Client SmartPhone)	iOS 12.1.4
Pixel C	Google	802.1X クライアント (Client Tablet)	Android 8.1.0
NetAttest D3-SX15	ソリトンシステムズ	DHCP/DNS サーバー	4.2.17

1-2-2 認証方式

IEEE802.1X EAP-TLS/EAP-PEAP

1-2-3 ネットワーク設定

機器	IP アドレス	RADIUS port (Authentication)	RADIUS Secret (Key)
NetAttest EPS-ST05	192.168.1.2/24	UDP 1812	secret
SmartZone 124	192.168.1.1/24		secret
R510	192.168.1.11/24	-	-
Client PC	DHCP	-	-
Client SmartPhone	DHCP	-	-
Client Tablet	DHCP	-	-

2. NetAttest EPS の設定

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

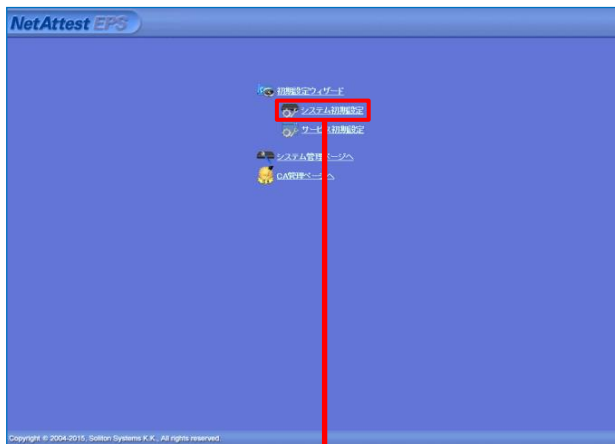
下記のような流れでセットアップを行います。

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

管理ページにアクセスしたら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
- ドメインネームサーバーの設定



初期設定ウィザード - 設定項目の確認

設定内容を確認して下さい。
この設定を保存・反映するには「再起動」ボタンをクリックして下さい。

ネットワーク時刻	
NTPサーバー1	
NTPサーバー2	
NTPサーバー3	
時刻同期する	無効

EPSライセンス	
最大ユーザー数	200
最大NAS/RADIUSクライアント数	20
外部サーバー証明書	無効
RADIUSプロキシ	無効
Windowsドメイン認証連携	無効
グループ	無効
MACアドレス認証	無効
ポート制御	無効

戻る 再起動

Copyright © 2004-2015, Soliton Systems K.K., All rights reserved.

項目	値
ホスト名	naeps.example.com
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

初期設定ウィザード - CA構築

CA種別選択
CA種別選択: ルートCA

CA秘密鍵
 内部で新しい鍵を生成する
 公開鍵方式: RSA
 鍵長: 2048
 外部HSMデバイスの鍵を使用する
 要求署名アルゴリズム: SHA256

CA情報
 CA名(必須): TestCA
 国名: 日本
 都道府県名: Tokyo
 市区町村名: Shinjuku
 会社名(組織名): Soliton Systems
 部署名:
 E-mailアドレス:
 CA署名論文:

署名アルゴリズム: SHA256

Copyright © 2004-2015, Soliton Systems K.K. All rights reserved.

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

初期設定ウィザード - RADIUSサーバーの基本設定

EAP
EAP認証タイプ
優先順位: 認証タイプ
1: TLS
2: PEAP
なし
なし
なし

EAP-TLS/TTLS/PEAPオプション
メッセージフラグメントサイズ: 1024 バイト
メッセージの長さ情報: フラグメントされた 番号の/ワットCのみ含まれる

EAP-TLS/PEAPオプション
 GTC認証を有効にする
 TLSセッションリネゴシエーションを有効にする
 EAP-FASTオプション

戻る 次へ

Copyright © 2004-2015, Soliton Systems K.K. All rights reserved.

項目	値
EAP 認証タイプ	
1	TLS
2	PEAP

初期設定ウィザード - NAS/RADIUSクライアント設定

検索対象: 新規

NAS/RADIUSクライアント名: RadiusClient01

このNAS/RADIUSクライアントを有効にする

モデル名:
タイプ:
 NAS/RADIUSクライアント
 NASのみ
 RADIUSクライアントのみ

説明:
IPアドレス: 192.168.1.1
パスワード: *****
所属するNASグループ:

戻る 次へ

項目	値
NAS/RADIUS クライアント名	RadiusClient01
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。

名前	ユーザーID	最終認証成功日時	証明書	タスク
test user	test			発行 変更 削除

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

名前	ユーザーID	最終認証成功日時	証明書	タスク
test user	test			発行 変更 削除
user01	user01			発行 変更 削除

2-5 クライアント証明書の発行

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.p12 という名前で保存)

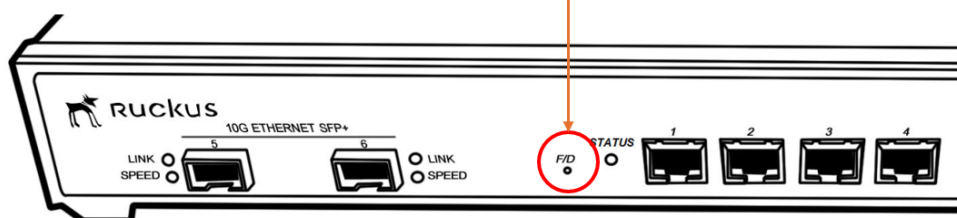
項目	値
証明書有効期限	365
PKCS#12 ファイルに証明機関の・・・	チェック有

3. SmartZone 124 の設定

3-1 SmartZone 124 の初期化

工場出荷状態の SmartZone 124 は、起動時に DHCP サーバーからアドレスを取得します。取得できない場合には、IP アドレス 192.168.2.2/24 を自身に割り当てて起動します。必要な場合は、本体起動後、筐体正面の F/D ボタンを 10 秒以上押下して工場出荷時の設定に戻してください。

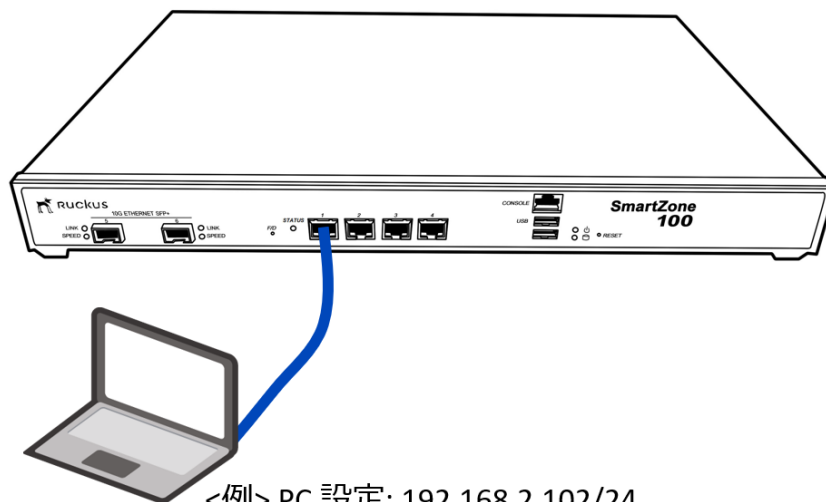
10秒間以上押下で工場出荷時設定へ



3-2 初期設定ウィザードの実行

WebUI にて Setup Wizard を開始するには、適切な IP アドレス (192.168.2.102/24 等) を設定した PC を SmartZone 124 のポート 1 へ接続し、SmartZone 124 の電源を入れます。

SmartZone 124 が起動したら、設定用 PC の Web ブラウザより、コントローラーのデフォルト IP アドレス (<https://192.168.2.2:8443>) へアクセスし、Setup Wizard を開始します。



3-2-1 Port Configuration

この例では、「One Port Group」を選択します。

Port Configuration

Please select logical interface configuration.

- One Port Group
Management and AP Tunnel Traffic combined
- Two Port Group
Port Group 1: Management & AP Control
Port Group 2: AP Tunnel Data

Next

項目	値
Port Configuration	One Port Group

3-2-2 IP Setting

コントローラーの管理 IP アドレスを設定します。各グループにアサインされた IP アドレスを設定してください。なお、設定反映後は IP の疎通がなくなりますので、PC の IP アドレスをネットワークに適したアドレスへ変更してください。

Setup Wizard - SmartZone 100 version: 5.1.0.0.496 Upgrade

Port Configuration

IP Setting

Select how you want the SmartZone 100 to obtain its IPv4 (and IPv6, if supported on your network) IP address settings. To obtain an IP address automatically using DHCP, click "DHCP" for IPv4 or "Auto Configuration" for IPv6. To specify an IP address, click "Static" and then type the IP address settings in "IP Address," "Netmask," and "Gateway." An asterisk (*) indicates required information.

Cluster Information

Administrator

Confirmation

Configuration

IP Version Support IPv4 only IPv4 and IPv6

Management/AP Tunnel Traffic

IPV4

Static DHCP

IP Address * 192.168.1.1

Netmask * 255.255.255.0

Gateway * 192.168.1.254

Primary DNS Server 192.168.1.254

Secondary DNS Server IPv4 Secondary DNS

Next Back

項目	値
IP Version Support	IPv4 only
IPv4	
- Static / DHCP	Static
- IP Address	192.168.1.1
- Netmask	255.255.255.0
- Gateway	192.168.1.254
Primary DNS Server	192.168.1.254

3-2-3 Cluster Information

再接続後、クラスタに必要な情報を入力します。

- SmartZone Cluster Setting: New Cluster を選択
- Cluster Name: クラスタ名
- Controller Name: コントローラー名
- NTP Server: 同期する NTP サーバーを指定

項目	値
SZ Cluster Setting	New Cluster
Cluster Name	soliton
Controller Name	sz100
Controller Description	sz100
Default Country Code	Japan
NTP Server	ntp.ruckuswireless.com
AP Convention	Convert ZoneDirector APs ...

3-2-4 Administrator

システムの管理パスワードを設定してください。

3-2-5 Confirmation

設定内容の確認画面が表示され、「Finish」をクリックすることでシステムセットアップが開始されます。セットアップ完了までの目安は 20 分程度です。セットアップ完了後、先に設定した管理者パスワードを用いてログインして下さい。

The screenshot shows the 'Setup Wizard - SmartZone 100' interface. The left sidebar contains navigation options: Port Configuration, IP Setting, Cluster Information, Administrator, Confirmation (highlighted), and Configuration. The main content area is titled 'Confirmation' and contains the following text:

Please review the following settings. If changes need to be made, click Back to edit your settings. If the settings are ready for use, click Finish.

Cluster Name soliton
Protocol Type TCP
AP IP Mode IPV4
Management IP Management/AP Tunnel Traffic: Manual 192.168.1.1
Default Country Code JP
System time will be automatically set.
System Time Your current system time is (2019-03-04 09:58:21 Epoch : 1551661101)
System Time Zone (GMT +09:00) Asia/Tokyo
The field is only for UTC time calculation. Not SZ timezone settings

* After completing the setup wizard, please check the Ruckus Wireless Support Web site for the latest software updates.

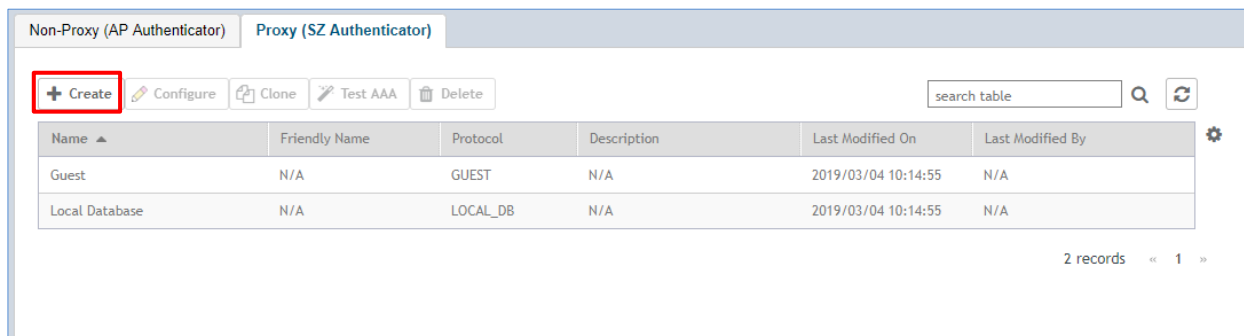
Restore from Config Backup: 選択されていません

At the bottom right, there are two buttons: 'Finish' (highlighted with a red box) and 'Back'.

The screenshot shows the 'Ruckus Wireless SmartZone 100' login screen. It features the Ruckus logo and a Wi-Fi symbol. Below the logo, there are two input fields: the first contains the username 'admin', and the second contains masked characters '.....'. At the bottom, there is a large orange button labeled 'ログイン' (Login).

3-3 AAA 設定

802.1x 認証を行うために、NetAttest EPS (RADIUS サーバー) の登録を行います。
WebUI より、[Services & Profiles]-[Authentication]を選択し、「Proxy (SZ Authenticator)」
タブにて「Create」をクリックします。

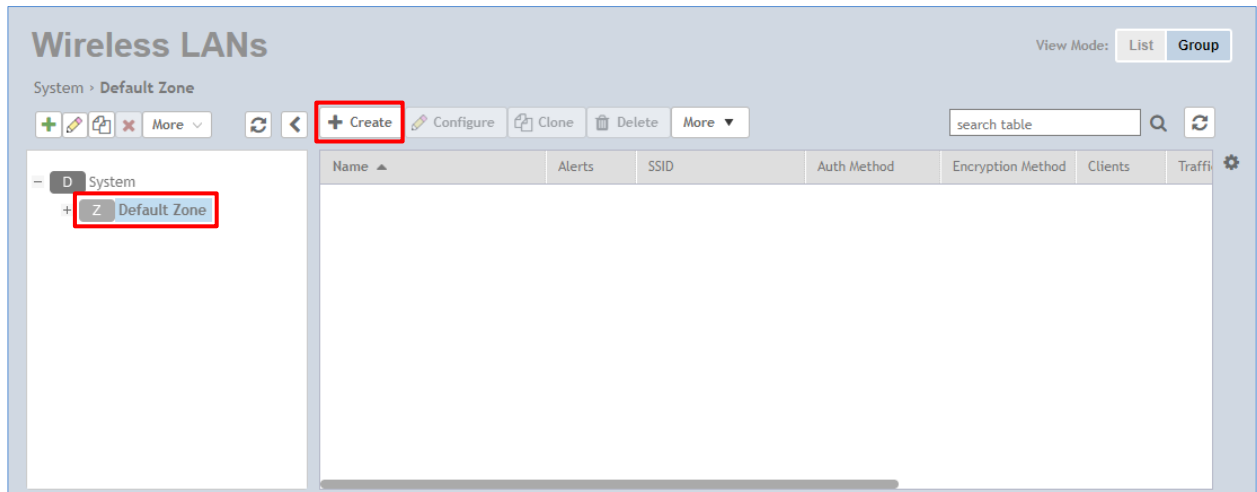


新規作成画面にて、RADIUS サーバー名、認証方式、RADIUS サーバーの IP Address と共有シークレットを入力し、「OK」をクリックします。

項目	値
Name	RADIUS
Service Protocol	RADIUS
Primary Server	
- IP Address	192.168.1.2
- Port	1812
- Shared Secret / Confirm Secret	secret

3-4 WLAN 設定

WLAN 設定では、「SolitonLab」という WPA2-EAP-AES の SSID を新規作成します。
WebUI より、Wireless LANs を選択した後、「Default Zone」を選択し、「+Create」をクリックして WLAN の新規作成を行います。



項目	値
General Options	
- Name	SolitonLab
- SSID	SolitonLab
Authentication Option	
- Authentication Type	Standard usage
- Method	802.1X EAP

Encryption Options ▼

* Method: WPA2 WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None

* Algorithm: AES AUTO

802.11r Fast Roaming: ON OFF

* 802.11w MFP: Disabled Capable Required

Data Plane Options ▼

[?] Access Network: ON OFF Tunnel WLAN traffic through Ruckus GRE

Authentication & Accounting Server ▼

* Authentication Server: ON Use the Controller as Proxy
 +

OFF RFC 5580 Location Delivery Support: Requires that Authentication Service be set to 'Use the controller as a proxy'

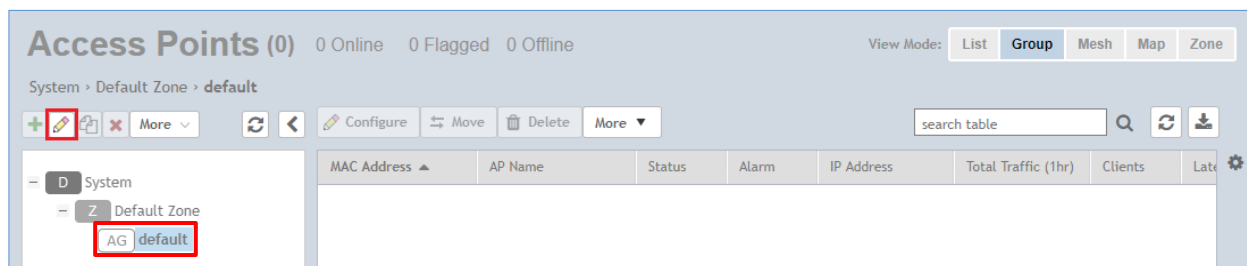
Accounting Server: ON Use the Controller as Proxy
 +

項目	値
Encryption Options	
- Method	WPA2
- Algorithm	AES
Authentication & Accounting Server	
- Authentication Server	Use the Controller as Proxy
	RADIUS

3-5 WLAN Group と AP Group

先に作成した WLAN グループ (Default) を、AP グループに割当てます。工場出荷時の設定では、Default の AP グループが準備されており、この例では Default のグループを利用するため、手動での割り当ては不要です。但し、チャンネル化設定は 20MHz を設定します。

WebUI より「Access Points」を選択し、[AG] default を選択し、鉛筆マークより編集を行います。



2.4GHz/5GHz 共に Channelization を ON にし、Override に 20 を指定します。

Configuration

Radio b/g/n (2.4 GHz)

Channelization: ON OFF Override: 20

Channel: ON OFF Override: Auto

Auto Cell Sizing: OFF OFF Enable

TX Power: OFF OFF Override: Full

WLAN Group: OFF OFF Override: default

Radio a/n/ac (5 GHz)

Channelization: ON OFF Override: 20

Channel: Indoor: ON OFF Override: Auto

 Outdoor: ON OFF Override: Auto

Auto Cell Sizing: OFF OFF Enable

TX Power: OFF OFF Override: Full

WLAN Group: OFF OFF Override: default

項目	値
Radio 2.4GHz/5GHz	
- Channelization	ON
- Override	20

3-6 AP セットアップ

Ruckus AP が SmartZone コントローラーを発見するには以下の方法があり、一般的には「IP subnet broadcast」又は「AP Static Configuration」のいずれかが用いられることが多いです。

- IP subnet broadcast
- DHCP Option 43 sub-option 3
- DHCPv6 Option 17 sub-option 3
- DHCPv6 Option 52
- DNS entry named "zonedirector.<local domain>"
- AP Static Configuration

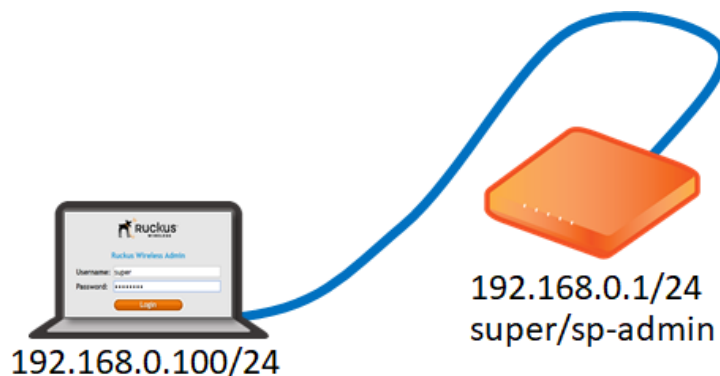
「IP subnet broadcast」は、Ruckus Standalone AP を SmartZone コントローラーと同じセグメントに接続すると、セグメント内の SmartZone コントローラーを自動的にディスカバリし、同じバージョンへアップグレードされ、SmartZone コントローラーの管理下となる方法です。

このドキュメントでは、「AP Static Configuration」の方法にて進めます。

Standalone AP の工場出荷時は管理 IP を DHCP で取得しますが、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 を自身に割り当てて起動します。

設定を行う PC に適切な IP アドレスを設定(例: 192.168.0.100/24)し、Web ブラウザを起動し、192.168.0.1 へ接続します。ログインユーザーID/パスワードは下記の通りです。

- User Name: super
- Password: sp-admin



WebUI より[Administration]-[Management]を選択し、コントローラーを指定します。各パラメータは以下を参考にし、「Update Settings」をクリックしてください。

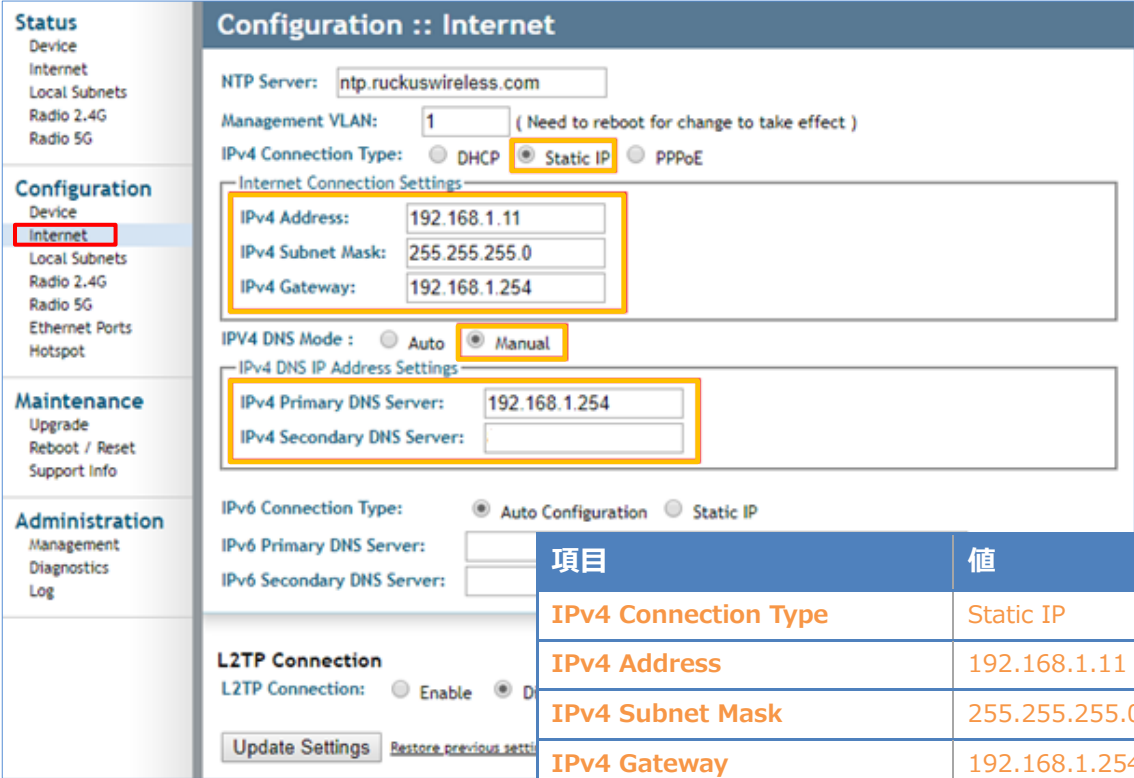
The screenshot shows the 'Administration :: Management' page in the Soliton WebUI. The left sidebar contains navigation menus for Status, Configuration, Maintenance, and Administration. The 'Administration' menu is expanded, and 'Management' is selected. The main content area displays the following settings:

- Network Profile: 4bss
- Telnet Access? Enabled Disabled
- Telnet Port: 23
- SSH Access? Enabled Disabled
- SSH Port: 22
- HTTP Access? Enabled Disabled
- HTTP Port: 80
- HTTPS Access? Enabled Disabled
- HTTPS Port: 443
- Certificate Verification: PASSED
- Controller Discovery Agent (LWAPP)? Enabled Disabled
- SmartCellGateway Agent? Enabled Disabled
- Cloud Discovery Agent (FQDN) Enabled Disabled
- Set Controller Address (Reboot to take effect) Enabled Disabled
- Primary Controller Addr: 192.168.1.1
- Secondary Controller Addr: [Empty field]
- TR069 / SNMP Management Choice:
 - Auto (SNMP and TR069 will work together.)
 - SNMP only
 - FlexMaster only
 - None

At the bottom of the page, there are two buttons: 'Update Settings' and 'Restore previous settings'.

項目	値
Set Controller Address (Reboot to take effect)	Enable
Primary Controller Addr	192.168.1.1

AP の管理 IP Address を設定するには、WebUI より、[Configuration]-[Internet]を選択し、IP 情報を指定します。設定後に「Update Settings」をクリックしてください。クリック後すぐに反映されるので、AP を AP セグメントに接続してください。



項目	値
IPv4 Connection Type	Static IP
IPv4 Address	192.168.1.11
IPv4 Subnet Mask	255.255.255.0
IPv4 Gateway	192.168.1.254
IPv4 DNS Mode	Manual
IPv4 Primary DNS Server	192.168.1.254

なお、設定 PC から Standalone AP へ SSH 接続し、CLI にて設定することも可能です。

```
rkscli: set director ip 192.168.1.1
** Please reboot for this change to take effect
OK
rkscli: reboot
OK
Rkscli:
```

AP の管理 IP Address を Static で指定するには、以下のコマンドで IP Address、mask、IP Gateway を設定します。

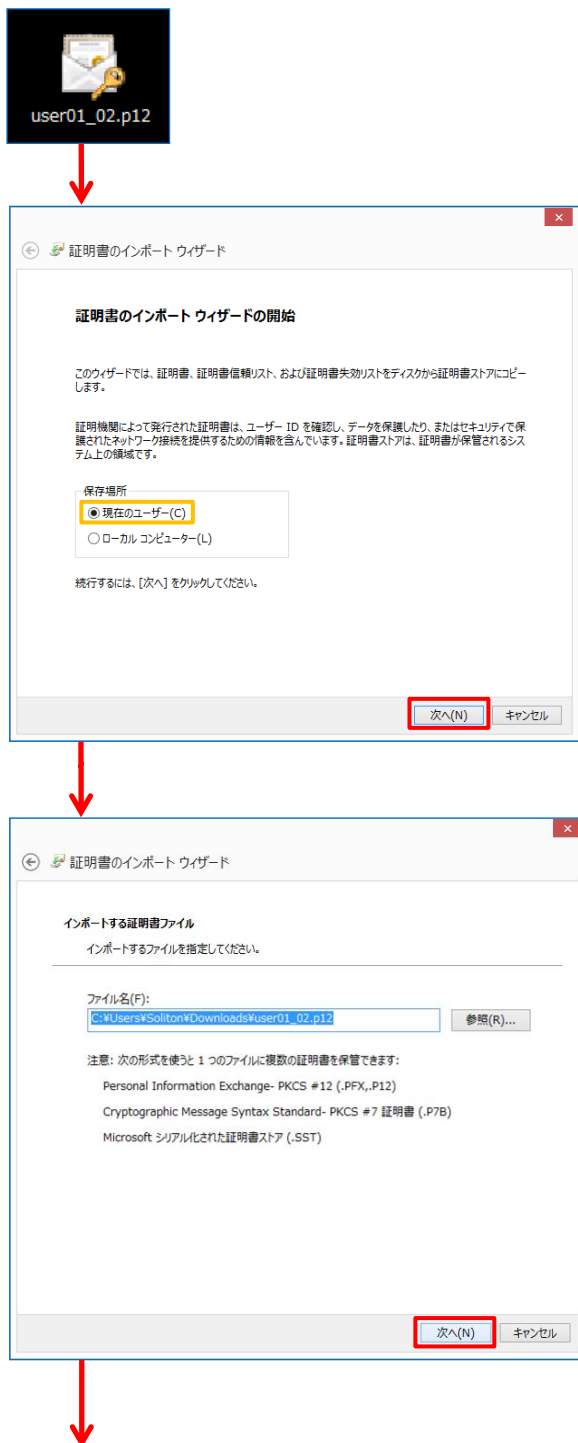
```
rkscli:
rkscli: set ipaddr wan 192.168.1.11 255.255.255.0 192.168.1.254
```


4. EAP-TLS 認証でのクライアント設定

4-1 Windows 10 での EAP-TLS 認証

4-1-1 クライアント証明書のインポート

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。



証明書インポート ウィザード

秘密キーの保護
セキュリティを維持するために、秘密キーはパスワードで保護されています。

秘密キーのパスワードを入力してください。

パスワード(P):
●●●●●●

パスワードの表示(D)

インポート オプション(O):

秘密キーの保護を強化にする(E)
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。

このキーをエクスポート可能にする(M)
キーのバックアップやトランスポートを可能にします。

すべての拡張プロパティを含める(A)

次へ(N) キャンセル

【パスワード】

「2-4 ユーザーの登録」で設定したパスワードを入力

証明書インポート ウィザード

証明書ストア
証明書ストアは、証明書が保管されるシステム上の領域です。

Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。

証明書の種類に基づいて、自動的に証明書ストアを選択する(U)

証明書をすべて次のストアに配置する(P)

証明書ストア:
参照(R)...

次へ(N) キャンセル

証明書インポート ウィザード

証明書のインポート ウィザードの完了

【完了】をクリックすると、証明書がインポートされます。

次の設定が指定されました:

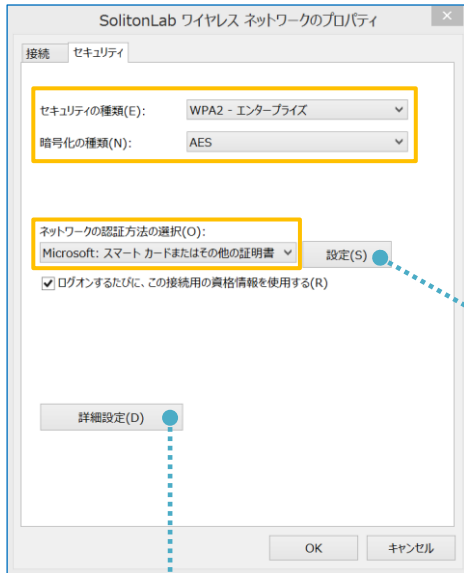
選択された証明書ストア	ウィザードで自動的に決定されます
内容	PFX
ファイル名	C:\Users\Soliton\Downloads\User01_02.p12

完了(F) キャンセル

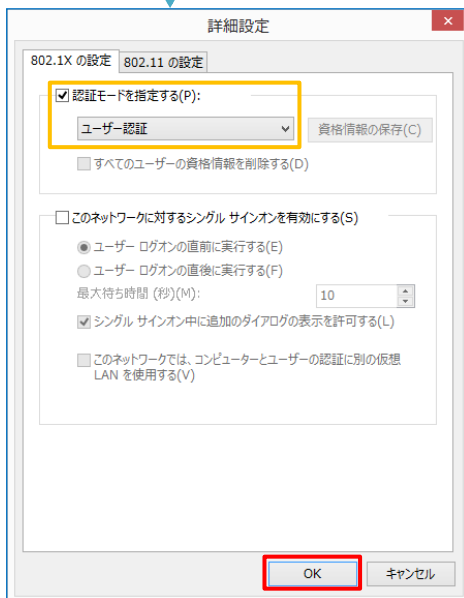
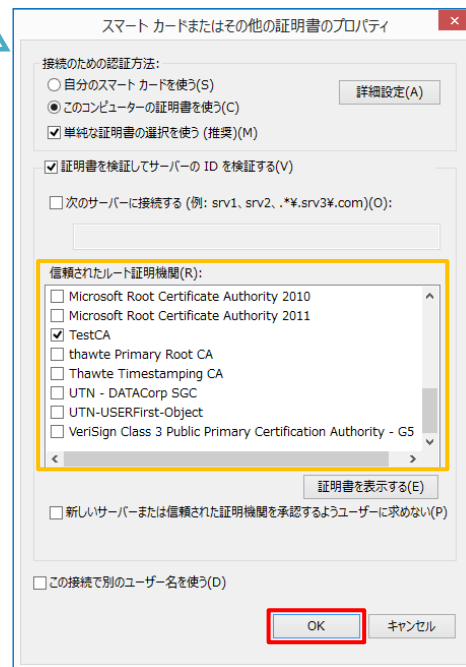
4-1-2 サプリカント設定

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
ネットワークの認証・・・	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証明書を・・・	On
- 単純な証明書の選択を使う (推奨)	On
証明書を検証してサーバーの ID を・・・	On
信頼されたルート証明機関	TestCA

4-2 iOS での EAP-TLS 認証

4-2-1 クライアント証明書のインポート

NetAttest EPS から発行したクライアント証明書を iOS デバイスにインポートする方法には下記などがあります。

- 1) Mac OS を利用して Apple Configurator を使う方法
- 2) クライアント証明書をメールに添付し iOS デバイスに送り、インポートする方法
- 3) SCEP で取得する方法(NetAttest EPS-ap を利用できます)

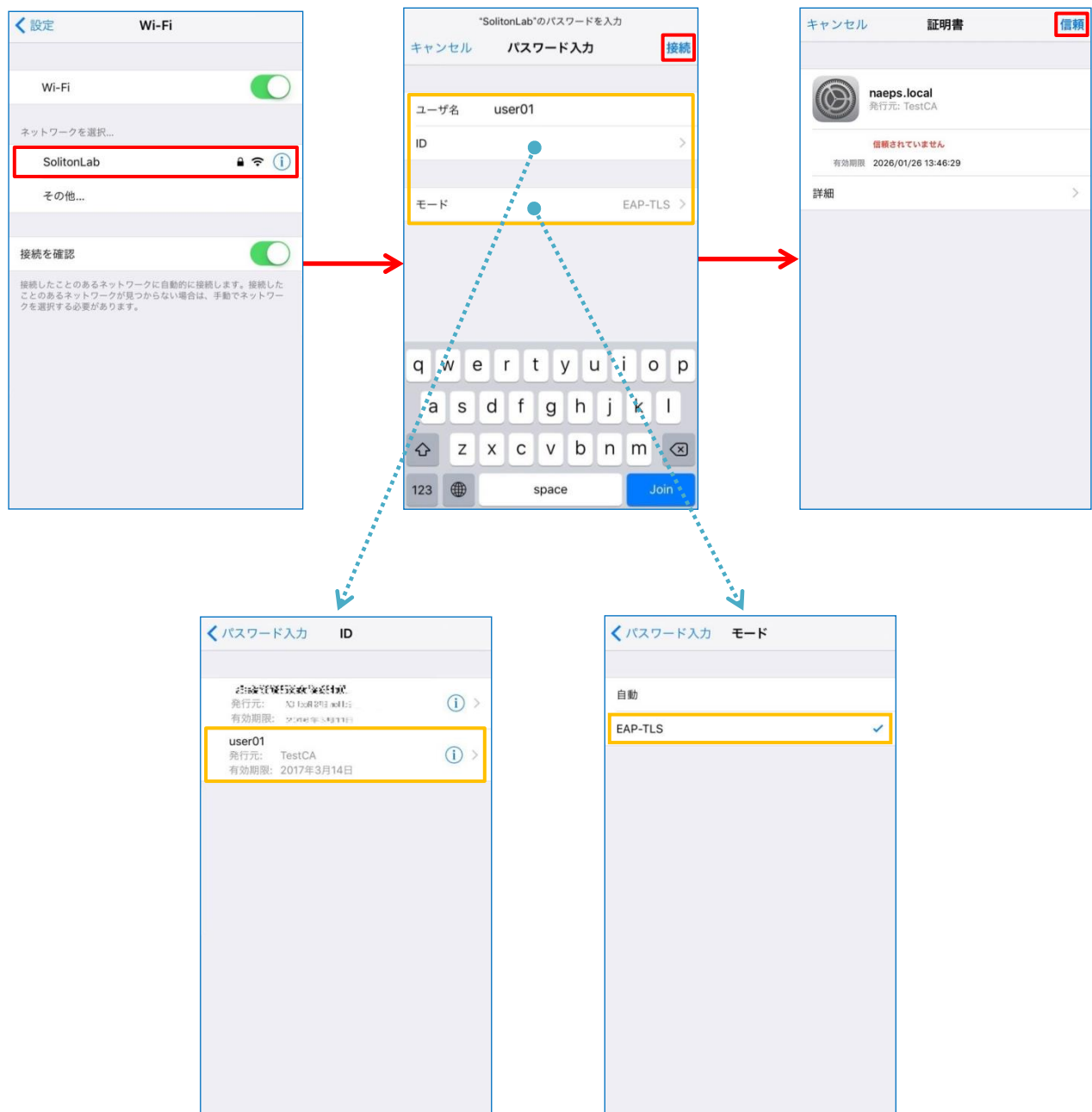
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

4-2-2 サプリカント設定

SmartZone 124 で設定した SSID を選択し、サブ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のユーザー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」よりインポートされたクライアント証明書をを選択します。

※初回接続時は「信頼されていません」と警告が出るので、「信頼」を選択し、接続します。



4-3 Android での EAP-TLS 認証

4-3-1 クライアント証明書のインポート

NetAttest EPS から発行したクライアント証明書を Android デバイスにインポートする方法として、下記 3 つの方法等があります。いずれかの方法で CA 証明書とクライアント証明書をインポートします。手順については、本書では割愛します。

- 1) SD カードにクライアント証明書を保存し、インポートする方法※1
- 2) クライアント証明書をメールに添付し Android デバイスに送り、インポートする方法※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、インポート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、インポート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、Soliton KeyManager 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。

Android 8.1.0 では証明書インポート時に用途別に証明書ストアが選択できますが、本書では無線 LAN への接続を行うため「Wi-Fi」を選択しています。

証明書の名前を指定する

証明書名:
TestCA

認証情報の使用:
Wi-Fi

パッケージの内容:
ユーザーキー1個
ユーザー証明書1件
CA証明書1件

キャンセル

証明書の名前を指定する

証明書名:
user01

認証情報の使用:
Wi-Fi

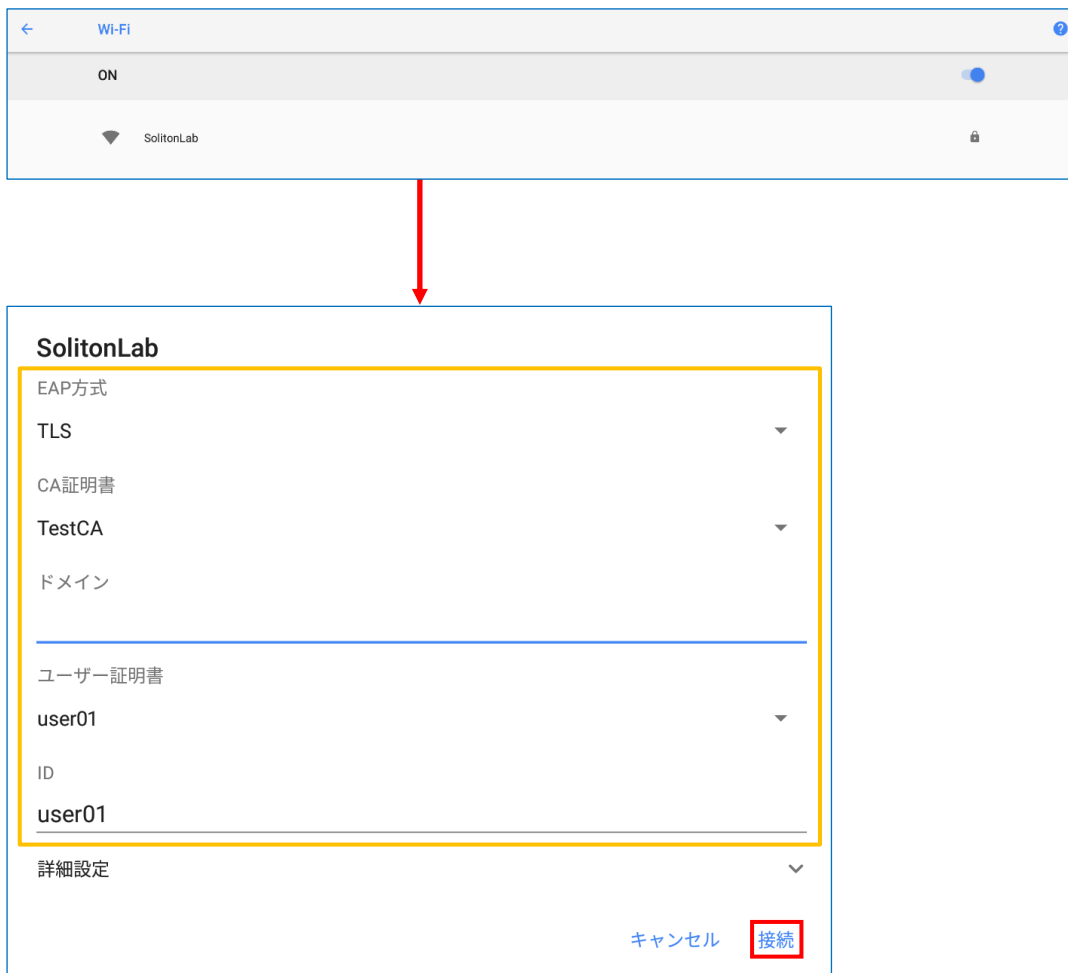
パッケージの内容:
ユーザーキー1個
ユーザー証明書1件
CA証明書1件

キャンセル

4-3-2 サプリカント設定

SmartZone 124 で設定した SSID を選択し、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のユーザーID を入力します。CA 証明書とユーザー証明書はインポートした証明書を選択して下さい。



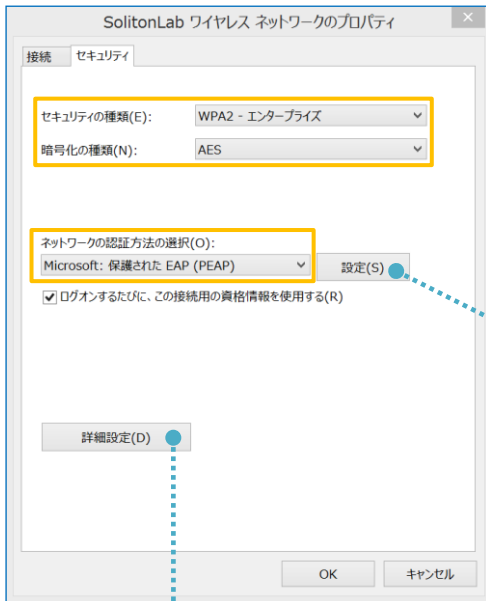
項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

5. EAP-PEAP 認証でのクライアント設定

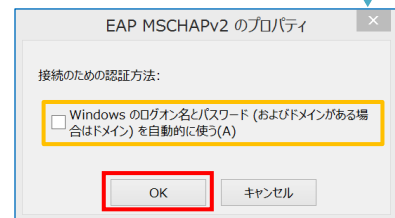
5-1 Windows 10 での EAP-PEAP 認証

5-1-1 Windows 10 のサブクライアント設定

[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
ネットワークの認証・・・	Microsoft: 保護された EAP



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	
- サーバー証明書の検証をする	On
- 信頼されたルート認証機関	TestCA
- Windows のログオン名と・・・	Off

5-2 iOS での EAP-PEAP 認証

5-2-1 iOS のサブクライアント設定

SmartZone 124 で設定した SSID を選択し、サブクライアントの設定を行います。「ユーザ名」、「パスワード」には「2-4 ユーザー登録」で設定したユーザーID、パスワードを入力してください。

※初回接続時は「証明書が信頼されていません」と警告が出るので、「信頼」を選択し、接続します。

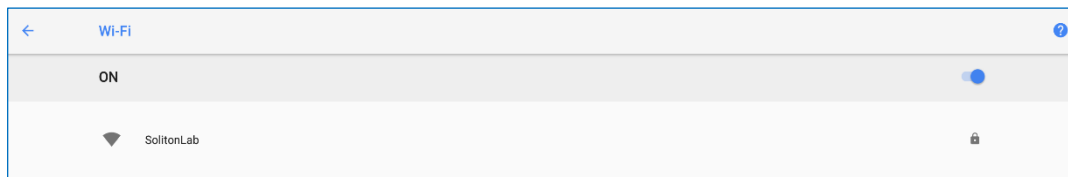


項目	値
ユーザ名	user01
パスワード	password
モード	自動

5-3 Android での EAP-PEAP 認証

5-3-1 Android のサブリカント設定

SmartZone 124 で設定した SSID を選択し、サブリカントの設定を行います。「ID」「パスワード」には「2-4 ユーザー登録」で設定したユーザーID、パスワードを入力してください。「CA 証明書」にインポートした CA 証明書を選択してください。



項目	値
EAP 方式	PEAP
フェーズ 2 認証	MSCHAPV2
CA 証明書	TestCA
ID	user01
パスワード	password

6. 動作確認結果

6-1 EAP-TLS 認証

EAP-TLS 認証が成功した場合のログ表示例

製品名	ログ表示例
NetAttest EPS	Login OK: [user01] (from client RadiusClient01 port 14 cli 40-A3-CC-32-10-A4)
SmartZone 124	以下のログが表示されます。

Date and Time	Code	Type	Severity	Activity
2019/02/14 11:43:35	204	Client disconnected	Informational	Client [user01] disconnected from WLAN [SolitonLab] on AP [Ruckus-SZ-AP@EC:8C:A2
2019/02/14 11:43:31	206	Client authorization success...	Informational	Client [user01] of WLAN [SolitonLab] from AP [Ruckus-SZ-AP@EC:8C:A2:16:36:80] was
2019/02/14 11:43:31	202	Client joined	Informational	Client [user01] joined WLAN [SolitonLab] from AP [Ruckus-SZ-AP@EC:8C:A2:16:36:80]
2019/02/14 11:42:50	204	Client disconnected	Informational	Client [user01] disconnected from WLAN [S
2019/02/14 11:42:35	206	Client authorization success...	Informational	Client [user01] of WLAN [SolitonLab] from
2019/02/14 11:42:35	202	Client joined	Informational	Client [user01] joined WLAN [SolitonLab] fr
2019/02/14 11:40:41	204	Client disconnected	Informational	Client [user01] disconnected from WLAN [SolitonLab] on AP [Ruckus-SZ-AP@EC:8C:A2
2019/02/14 11:40:24	206	Client authorization success...	Informational	Client [user01] of WLAN [SolitonLab] from AP [Ruckus-SZ-AP@EC:8C:A2:16:36:80] was

6-2 EAP-PEAP 認証

EAP-PEAP 認証が成功した場合のログ表示例

製品名	ログ表示例
NetAttest EPS	Login OK: [user01] (from client RadiusClient01 port 14 cli 40-A3-CC-32-10-A4 via proxy to virtual server) Login OK: [user01] (from client RadiusClient01 port 14 cli 40-A3-CC-32-10-A4)
SmartZone 124	上記と同様です。

