NetAttest EPS
認証連携設定例

【連携機器】Riverbed Xirrus XD2-240

【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、Riverbed 社製無線アクセスポイント Xirrus XD2-240 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 Xirrus XD2-240 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。

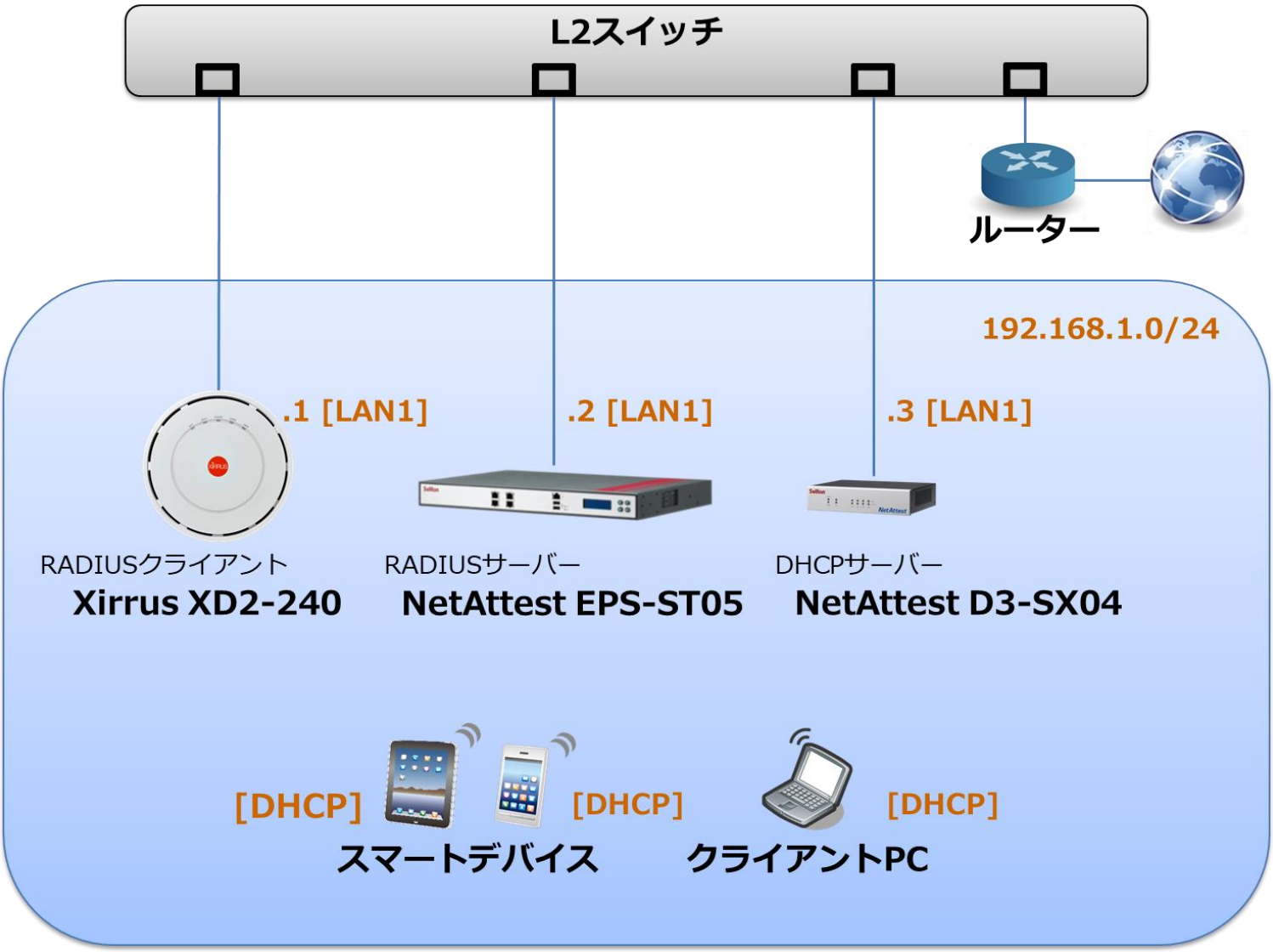
目次

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-SX04 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	4.10.3
Xirrus XD2-240	Riverbed	RADIUS クライアント (無線アクセスポイント)	AOS 8.4
Surface	Microsoft	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サプリカント
iPhone 7	Apple	802.1X クライアント (Client SmartPhone)	11.3.1
Pixel C	Google	802.1X クライアント (Client Tablet)	8.1.0
NetAttest D3-SX04	ソリトンシステムズ	DHCP/DNS サーバー	4.2.15

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
Xirrus XD2-240	192.168.1.1/24		secret
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。

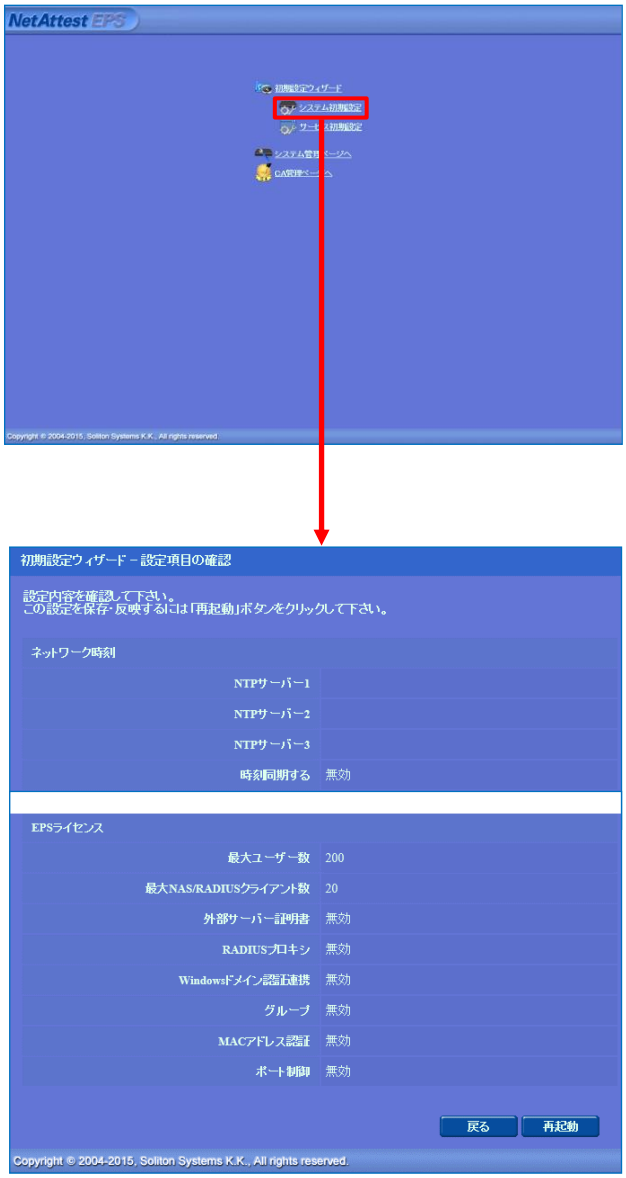
下記のような流れでセットアップを行います。

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



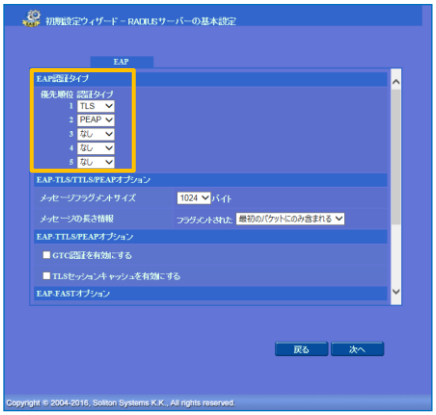
項目	値
ホスト名	naeps.example.com
IP アドレス	デフォルト
ライセンス	なし

2-3 サービス初期設定ウィザードの実行

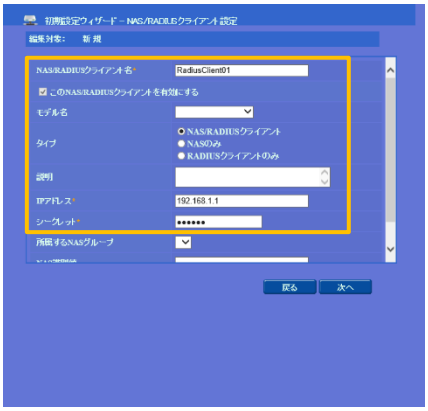
サービス初期設定ウィザードを実行します。

- 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

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	
1	TLS
2	PEAP



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

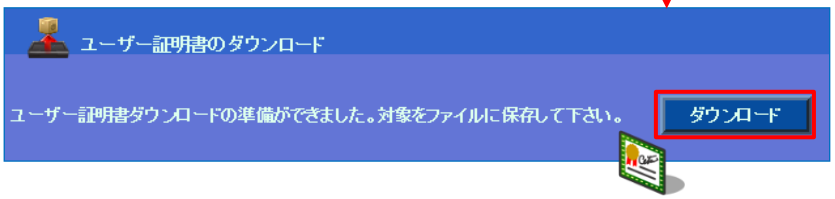
NetAttest EPS の管理画面より、認証ユーザーの登録を行います。[ユーザー]-[ユーザー一覧]から、「追加」ボタンでユーザー登録を行います。

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. NetAttest D3 の設定

Xirrus XD2-240 は、デフォルトでは DHCP にて IP アドレスを取得するよう設定されています。しかし、EPS に RADIUS クライアントとして登録するためには IP アドレスを静的に指定する必要があります。今回は Xirrus XD2-240 に静的に IP アドレスを割り当てるために、NetAttest D3 の静的割り当て機能を使用して IP アドレスを払い出すことにします。

NetAttest D3 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、Google Chrome から [http://192.168.2.1:2181/]にアクセスしてください。NetAttest D3 では以下の設定を行います。

- DHCP サーバーの起動
- スコープの設定
- IP アドレスの静的割り当て

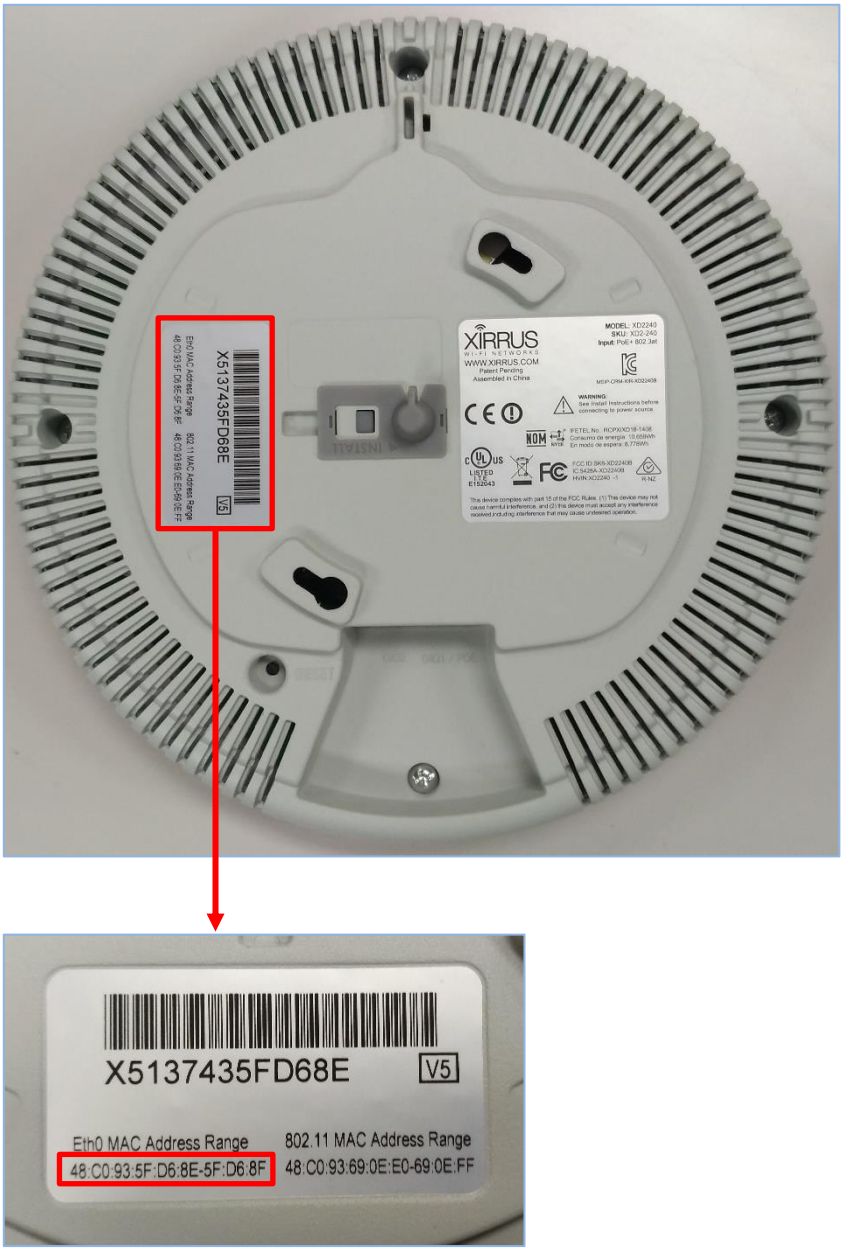
3-1 スコープの設定

[DHCP サービス]-[スコープ]から[追加]ボタンでスコープを追加します。今回は、端末に払い出す IP アドレスを[192.168.1.100-140]にするため、以下のように設定します。

項目	値
スコープの設定	
- ネットワーク	192.168.1.0
- サブネットマスク	255.255.255.0
- ルーター	192.168.1.254
- ドメイン名	solitonlab.com
- ドメインネームサーバー	192.168.1.3
レンジの設定	
- レンジ開始アドレス	192.168.1.1
- レンジ終了アドレス	192.168.1.140
- 除外レンジ開始アドレス	192.168.1.2
- 除外レンジ終了アドレス	192.168.1.99

3-2 IP アドレスの静的割り当て

Xirrus XD2-240 の MAC アドレスに IP アドレスを静的に割り当てるため、事前に Xirrus XD2-240 の MAC アドレスを確認します。Xirrus XD2-240 の MAC アドレスは本体裏面に記載されています。



[DHCP サービス]-[静的割り当て]から[追加]ボタンで IP アドレスの静的割り当てを行います。Xirrus XD2-240 の MAC アドレスと、静的に割り当てる IP アドレスを指定します。

項目	値
ホスト名	Xirrus
IP アドレス	192.168.1.1
MAC アドレス	48:c0:93:5f:d6:8e
備考 1	XD2-240 (任意)

3-3 DHCP サーバーの起動

[DHCP サービス]-[サーバー状態]にて[起動]ボタンを押し、DHCP サーバーを起動します。

4. Xirrus XD2-240 の設定

Xirrus XD2-240 は PoE 対応のスイッチにケーブルで接続すれば起動します。Xirrus XD2-240 はクラウドからの設定とローカル接続での設定の両方が可能ですが、今回はローカル接続で設定を行います。

デフォルトでは DHCP で IP アドレスが取得されるようになっているため、別途設置された DHCP サーバーから払い出された IP アドレスに対して、Firefox でアクセスします。Xirrus が DHCP で受け取った IP アドレスは、XMS-Cloud か DHCP サーバー側で確認する必要があります。

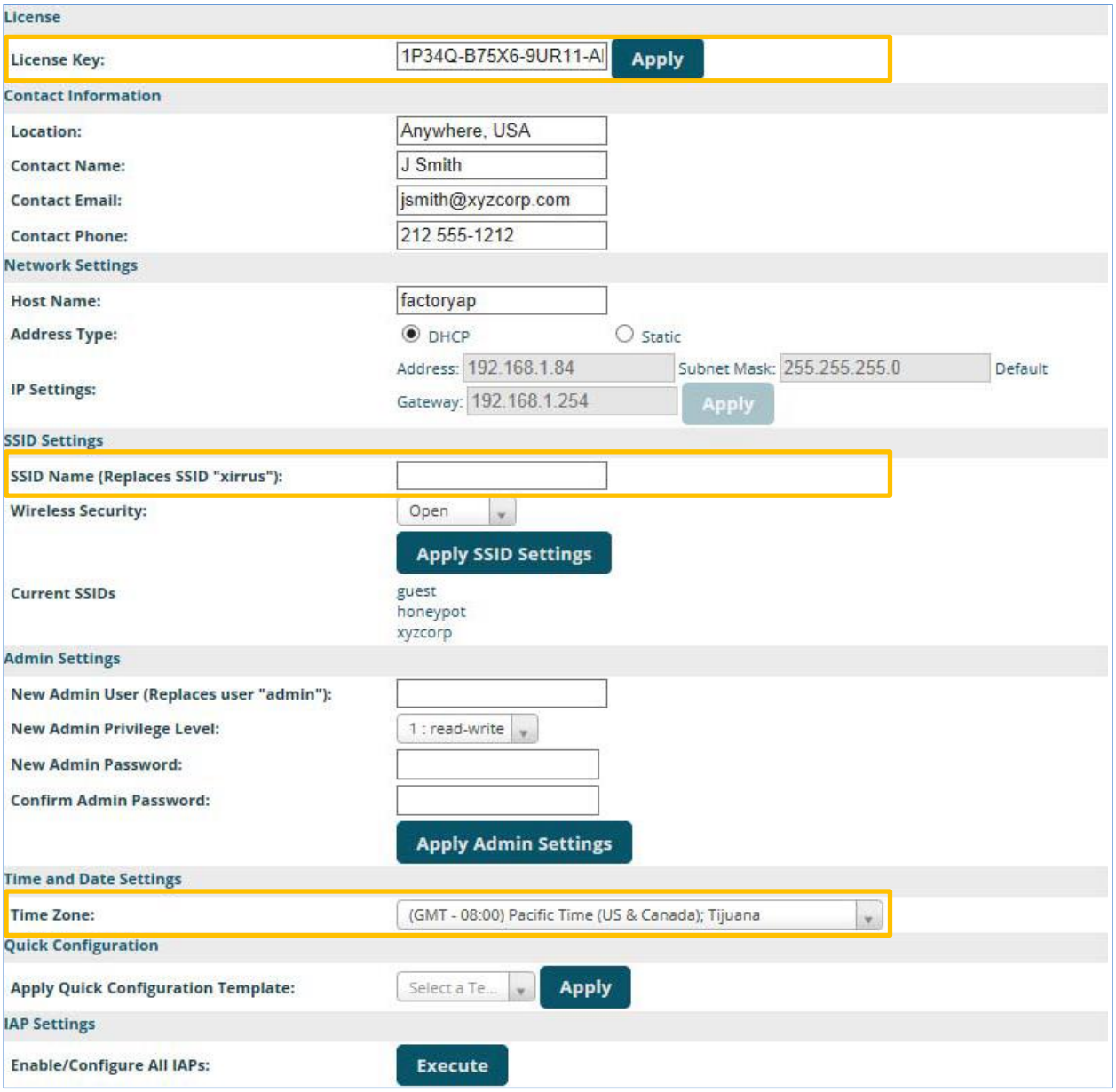
アクセスする URL は、https://<IP_ADDRESS>
証明書の例外エラーが出るため、例外登録をしたうえで続行
初期 ID/Password は、admin/admin です。

セットアップは下記の流れで行います。

1. Express setup の設定
2. External RADIUS サーバーの設定
3. 無線の設定

4-1 Express Setup

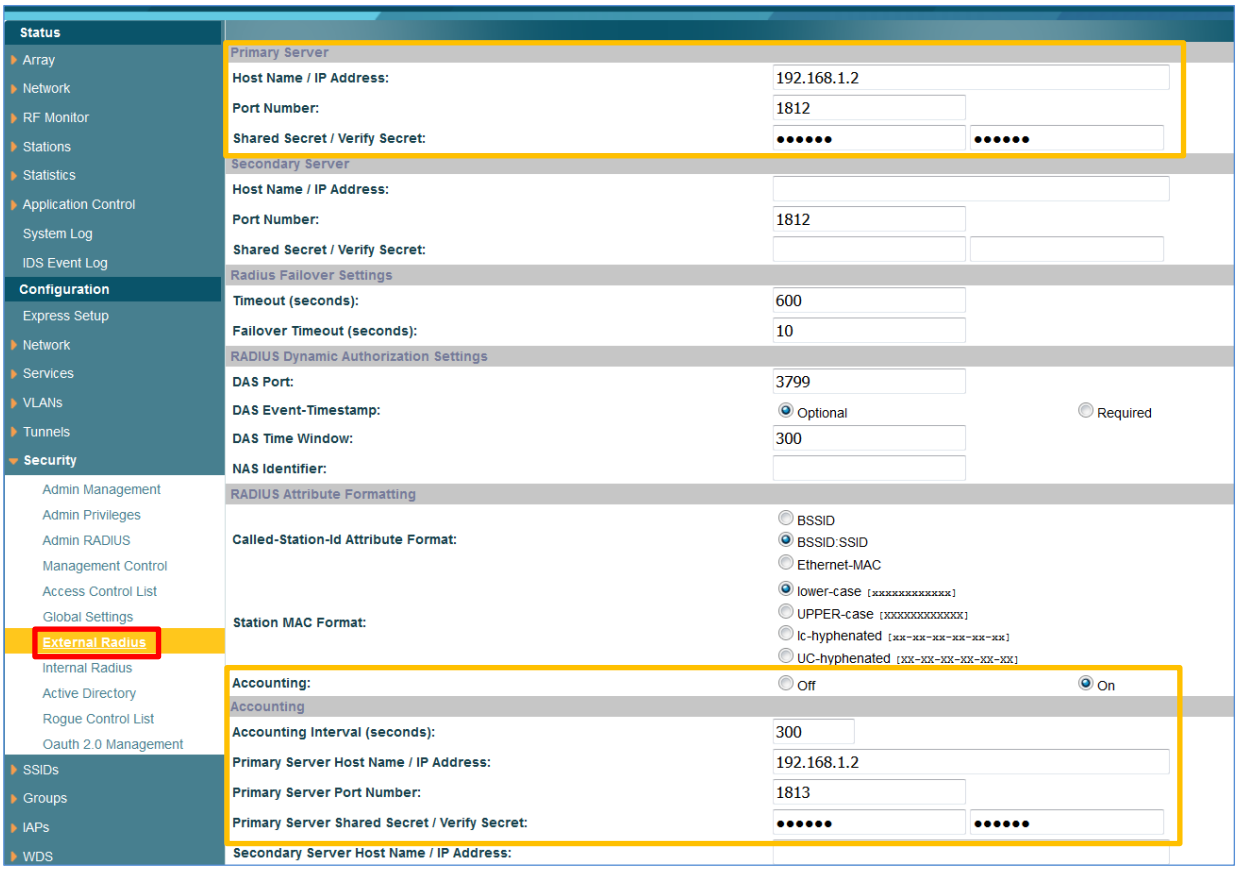
Time Zone の設定は必ず行ってください。ライセンスキーはベンダーから手に入れたものを入力してください。SSID の設定は後で変更しますが、SSID 名だけここで作成してください。



項目	値
License Key	…
SSID	SolitonLab
Timezone	GMT +09:00
admin	任意

4-2 External RADIUS サーバーの設定

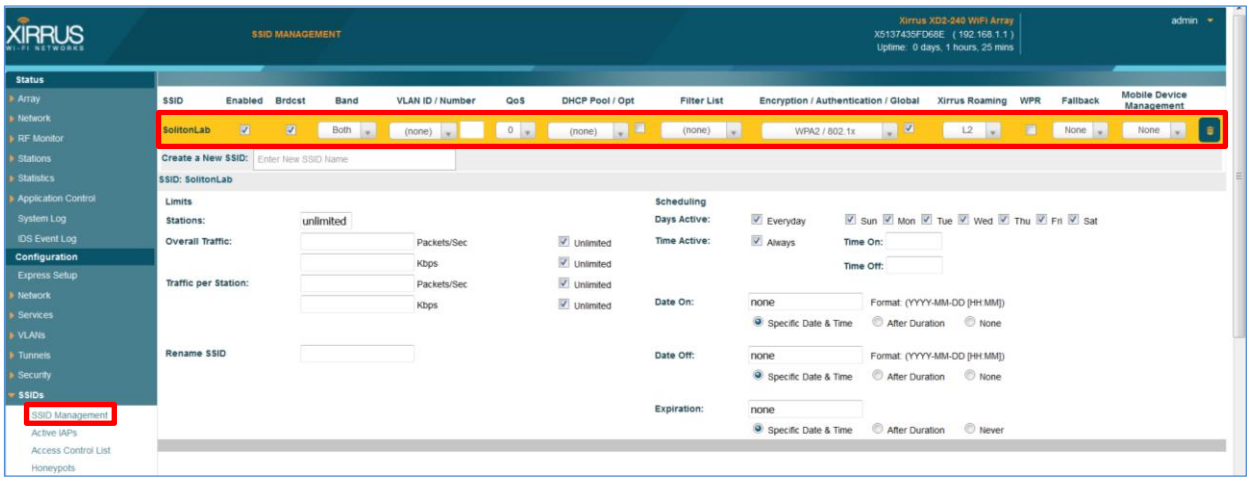
RADIUS サーバーの設定を行います。



項目	値
Host Name/IP Address	192.168.1.2
Port Number	1812
Shared Secret/Verify Secret	secret
Accounting	On
Primary Server Host Name/IP Address	192.168.1.2
Primary Server Port Number	1813
Primary Server Shared Secret/Verify Secret	secret

4-3 無線の設定

無線の設定は SSID の設定で行われます。Express setup で作成した SSID を選択して、設定を変更してください。



項目	値
SSID	SolitonLab
Enabled	Checked
Encryption/Authentication	WPA2/802.1X
Global	Checked

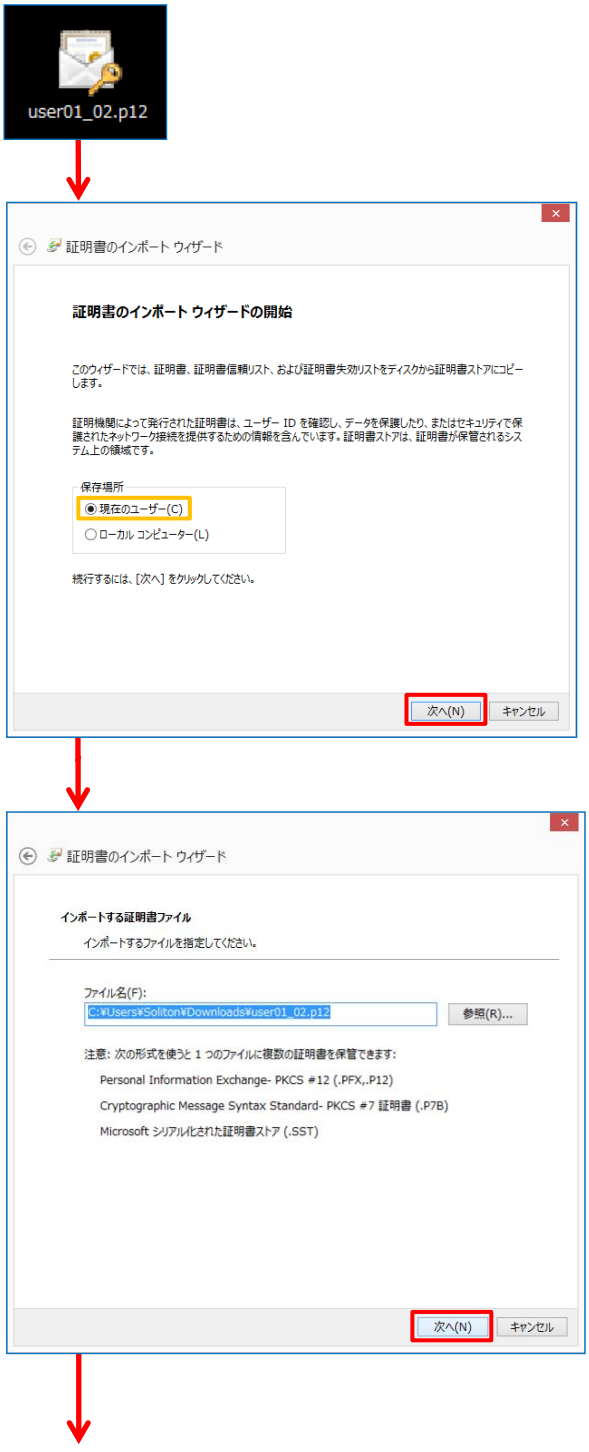
IAP Setting で IAP を Enable にします。Enable all IAPs をクリックしてください。

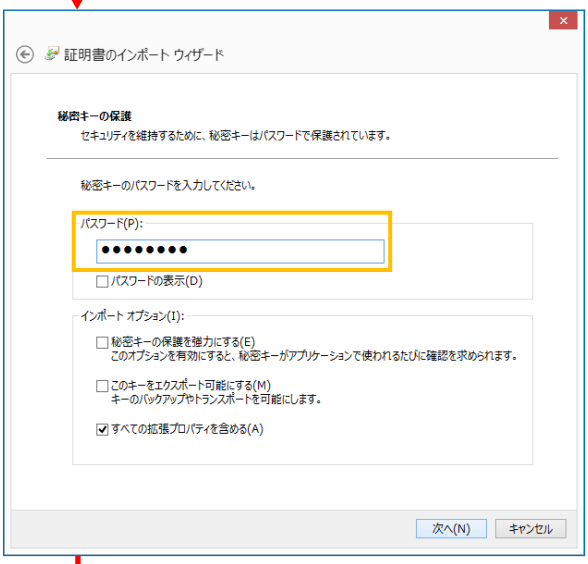
5. EAP-TLS 認証でのクライアント設定

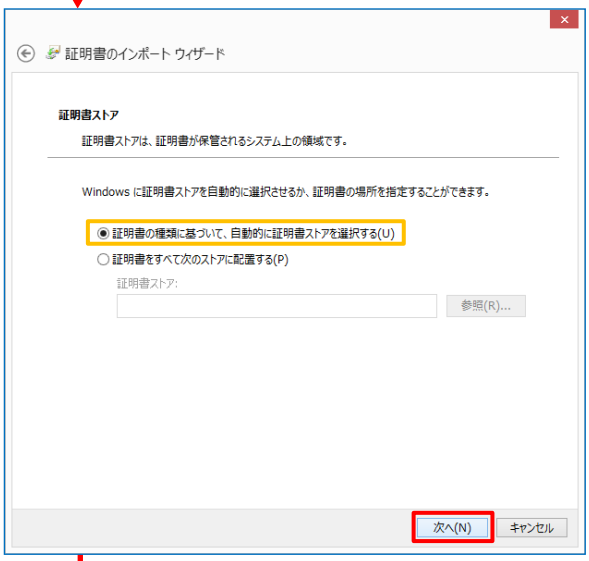
5-1 Windows 10 での EAP-TLS 認証

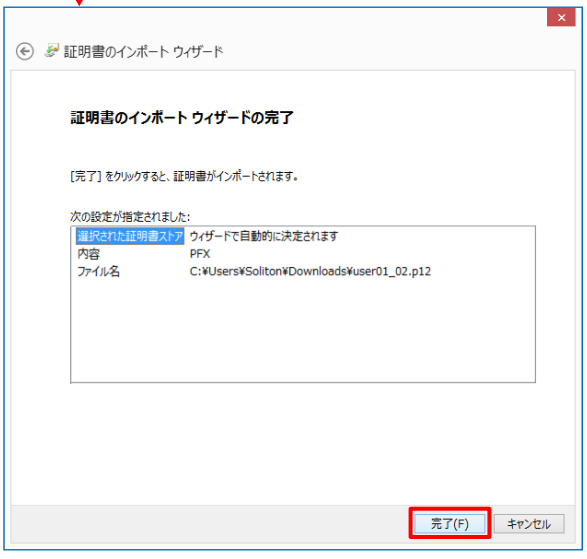
5-1-1 クライアント証明書のインポート

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。









【パスワード】

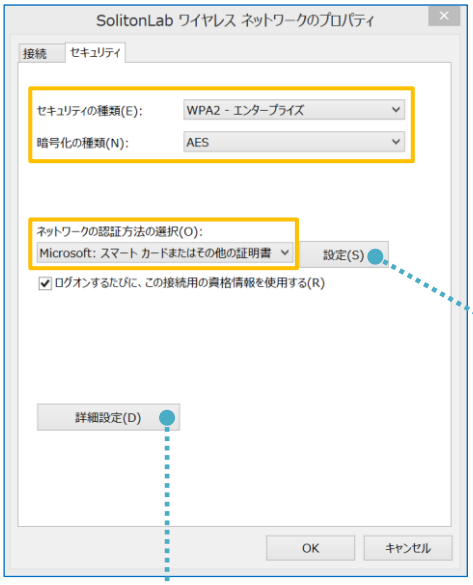
NetAttest EPS で証明書を発行した際に

設定したパスワードを入力

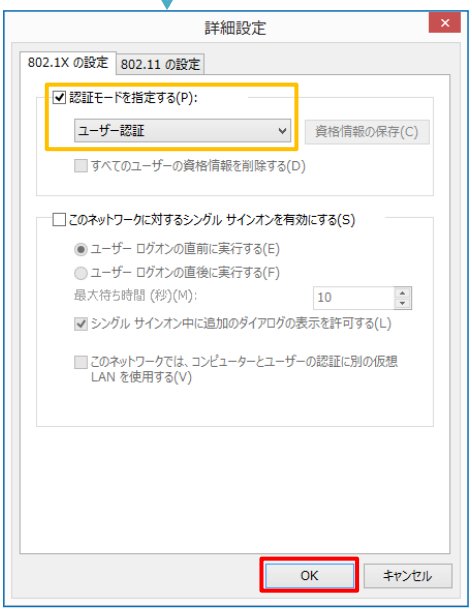
5-1-2 サプリカント設定

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

5-2 iOS での EAP-TLS 認証

5-2-1 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)

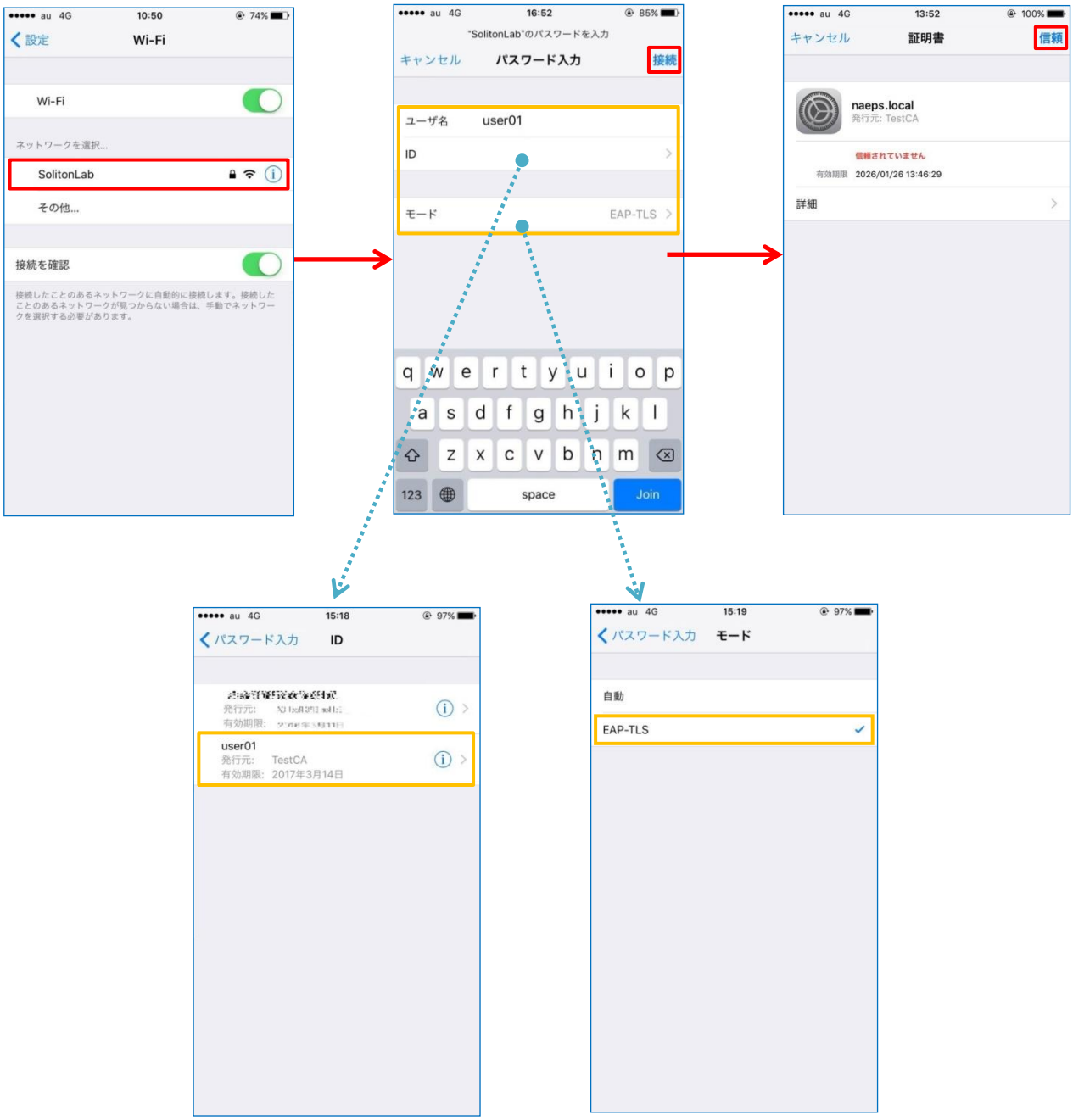
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

5-2-2 サプリカント設定

Xirrus XD2-240 で設定した SSID を選択し、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。



5-3 Android での EAP-TLS 認証

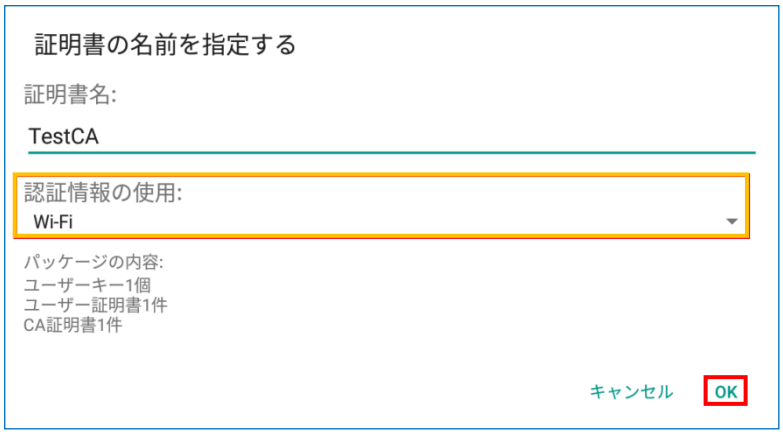
5-3-1 クライアント証明書のインポート

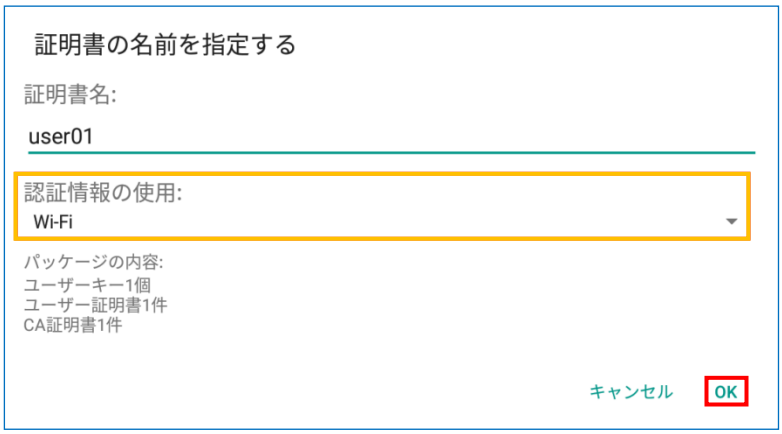
NetAttest EPS から発行したクライアント証明書を Android デバイスにインポートする方法として、下記 3 つの方法等があります。いずれかの方法で CA 証明書とクライアント証明書をインポートします。手順については、本書では割愛します。

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、メーラーにより、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。

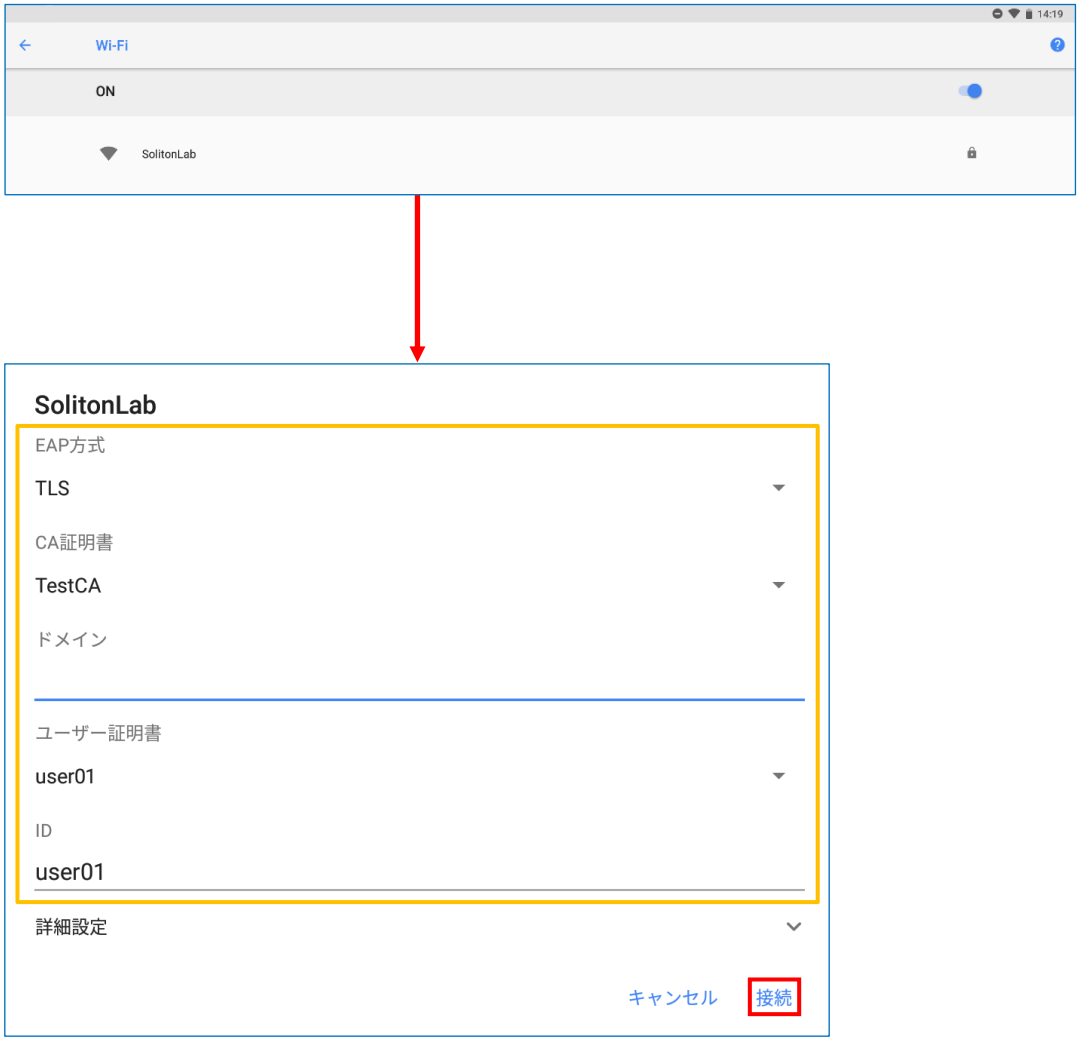




5-3-2 サプリカント設定

Xirrus XD2-240 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。



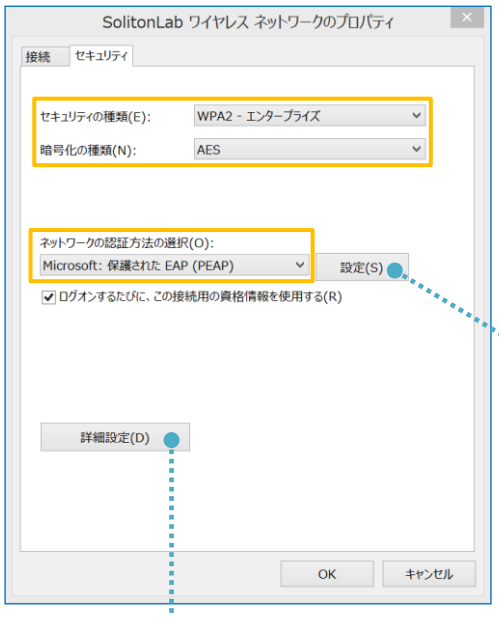
項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

6. EAP-PEAP 認証でのクライアント設定

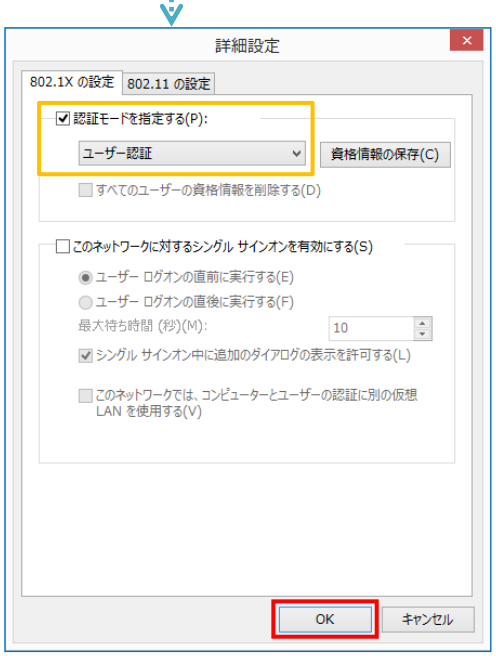
6-1 Windows 10 での EAP-PEAP 認証

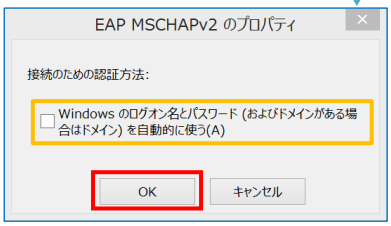
6-1-1 Windows 10 のサプリカント設定

[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

6-2 iOS での EAP-PEAP 認証

6-2-1 iOS のサプリカント設定

Xirrus XD2-240 で設定した SSID を選択し、サプリカ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。

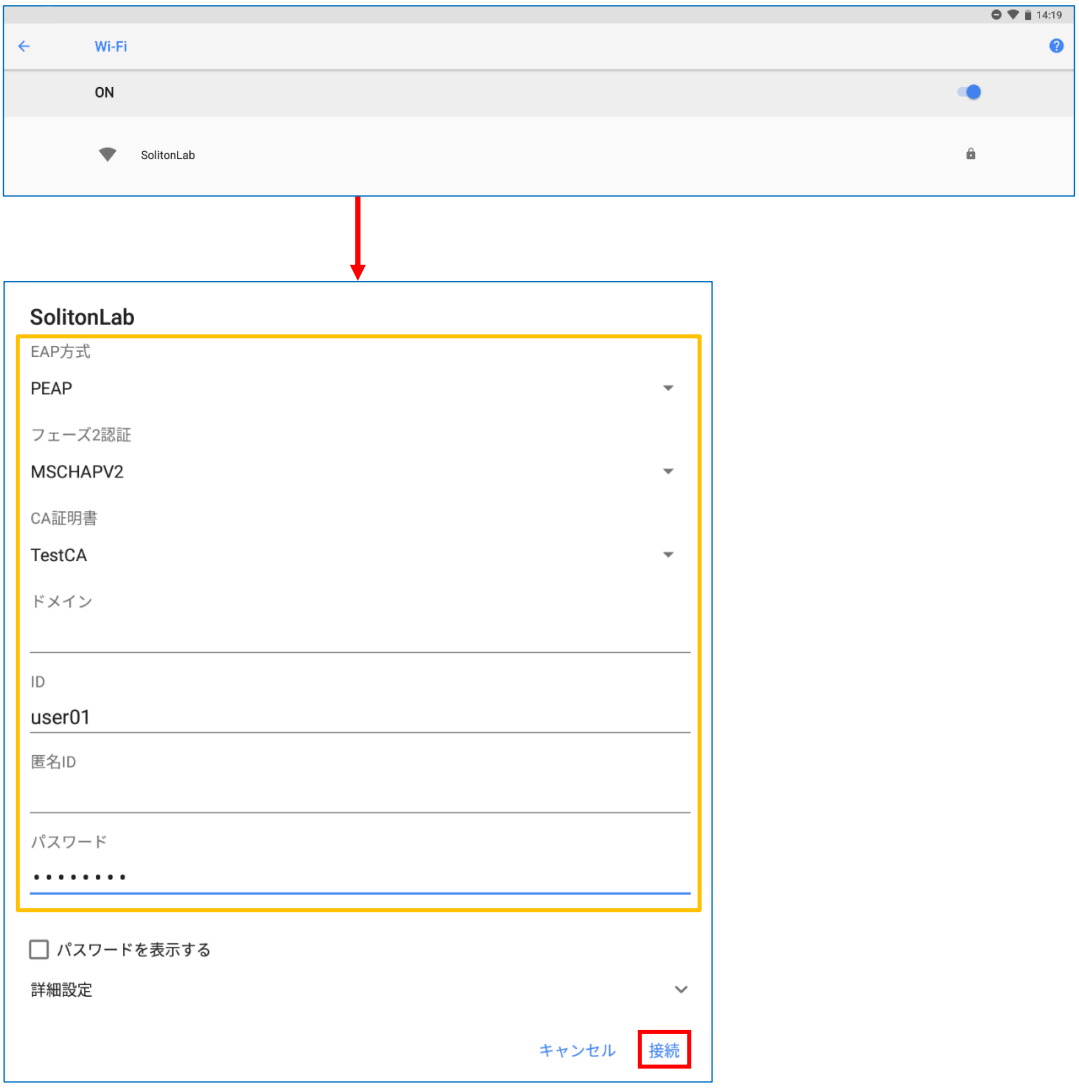
※初回接続時は「証明書が信頼されていません」と警告が出るので、「信頼」を選択し、接続します。

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

6-3 Android での EAP-PEAP 認証

6-3-1 Android のサプリカント設定

Xirrus XD2-240 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」「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

7. 動作確認結果

7-1 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	May 30 14:38:06 naeps radiusd[3094]: notice 2018/05/30 14:38:06 Login OK: [user01] (from client WirelessAP port 256 cli 40-A3-CC-32-10-A4)
Xirrus XD2-240	Station 40:a3:cc:32:10:a4 (192.168.1.106, S18205, Intel Notebook), IAP iap2: IPv4 address available, IPv4: 192.168.1.106, SSID: SolitonLab, Username: user01

7-2 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	May 30 14:53:10 naeps radiusd[3094]: notice 2018/05/30 14:53:10 Login OK: [user01] (from client WirelessAP port 256 cli 40-A3-CC-32-10-A4 via proxy to virtual server) May 30 14:53:10 naeps radiusd[3094]: notice 2018/05/30 14:53:10 Login OK: [user01] (from client WirelessAP port 256 cli 40-A3-CC-32-10-A4)
Xirrus XD2-240	Station 40:a3:cc:32:10:a4 (192.168.1.106, S18205, Intel Notebook), IAP iap2: IPv4 address available, IPv4: 192.168.1.106, SSID: SolitonLab, Username: user01

改訂履歴

日付	版	改訂内容
2018/06/13	1.0	初版作成