

NetAttest EPS

認証連携設定例

【連携機器】 バッファロー WAPM-AX8R

【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、バッファロー社製無線アクセスポイント WAPM-AX8R 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 WAPM-AX8R 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 サービス管理ページへのログオン | 5 |
| 2-2 初期設定ウィザード (システム、システム-2)の実行 | 6 |
| 2-3 初期設定ウィザード (サービス)の実行 | 9 |
| 2-4 https サービスの再起動 | 13 |
| 2-5 RADIUS クライアントの登録..... | 14 |
| 2-6 利用者の登録 | 15 |
| 2-7 クライアント証明書の発行 | 16 |
| 3. WAPM-AX8R の設定 | 17 |
| 3-1 WAPM-AX8R へログイン | 18 |
| 3-2 WAPM-AX8R へ LAN 側 IP アドレスを設定..... | 19 |
| 3-3 WAPM-AX8R へ RADIUS を設定 | 20 |
| 3-4 WAPM-AX8R へ SSID を設定 | 21 |
| 4. EAP-TLS 認証でのクライアント設定 | 23 |
| 4-1 Windows 10 での EAP-TLS 認証..... | 23 |
| 4-1-1 クライアント証明書のインポート..... | 23 |
| 4-1-2 サプリカント設定 | 25 |
| 4-2 Mac での EAP-TLS 認証 | 26 |
| 4-2-1 クライアント証明書のインポート..... | 26 |
| 4-2-2 サプリカント設定 | 28 |
| 4-3 iOS での EAP-TLS 認証 | 30 |
| 4-3-1 クライアント証明書のインポート..... | 30 |
| 4-3-2 サプリカント設定 | 31 |
| 4-4 Android での EAP-TLS 認証 | 32 |

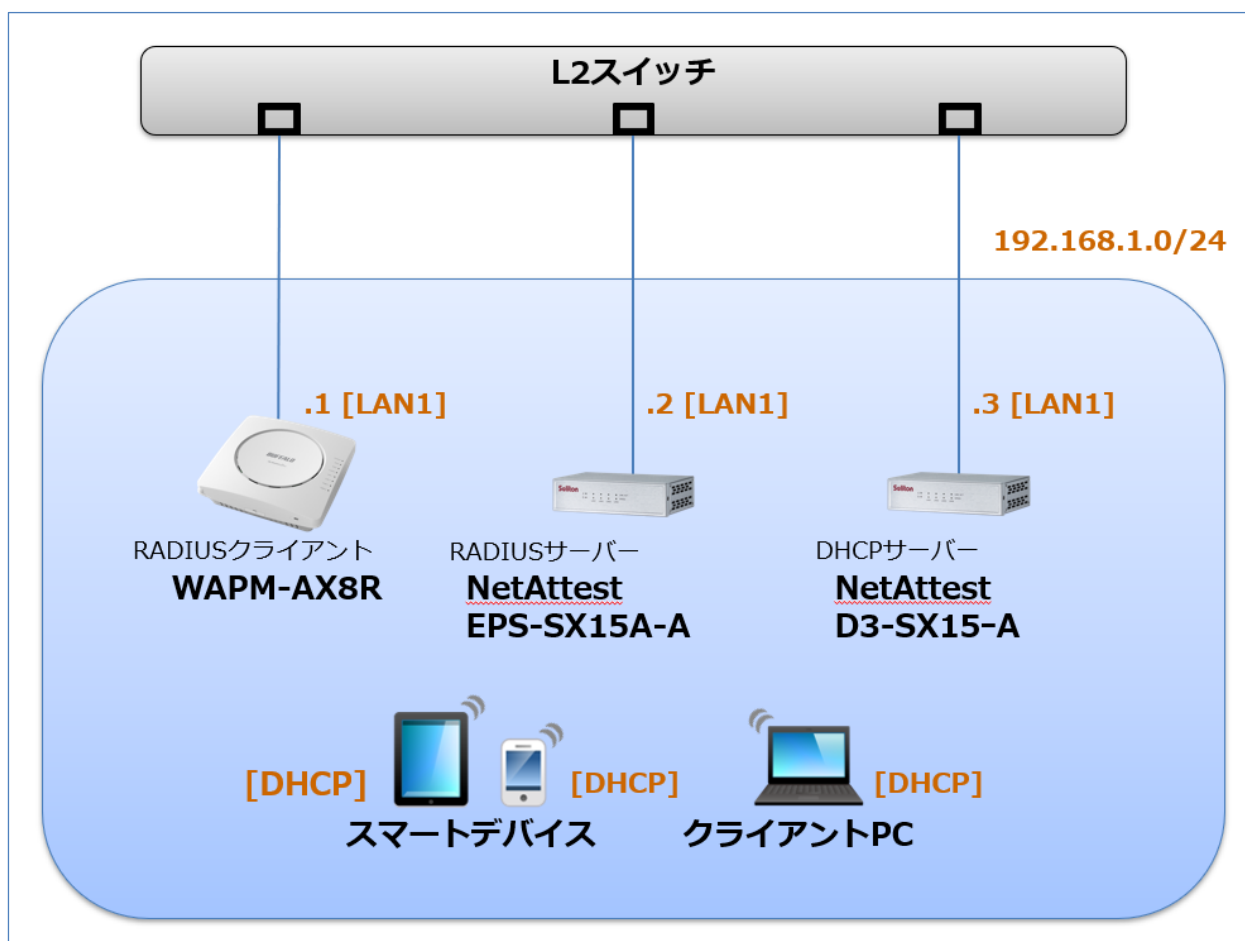
| | |
|--------------------------------------|-----------|
| 4-4-1 クライアント証明書のインポート..... | 32 |
| 4-4-2 サプリカント設定..... | 33 |
| 5. EAP-PEAP 認証でのクライアント設定..... | 34 |
| 5-1 Windows 10 での EAP-PEAP 認証..... | 34 |
| 5-1-1 Windows 10 のサプリカント設定 | 34 |
| 5-2 Mac での EAP-PEAP 認証 | 35 |
| 5-2-1 Mac のサプリカント設定 | 35 |
| 5-3 iOS での EAP-PEAP 認証..... | 36 |
| 5-3-1 iOS のサプリカント設定..... | 36 |
| 5-4 Android での EAP-PEAP 認証 | 37 |
| 5-4-1 Android のサプリカント設定..... | 37 |
| 6. 動作確認..... | 38 |
| 6-1 RADIUS 認証ログの確認(EPS) | 38 |
| 6-2 認証ログの確認(WAPM-AX8R) | 39 |

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 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-SX15A-A | ソリトンシステムズ | RADIUS/CA サーバー | 5.0.4 |
| WAPM-AX8R | バッファロー | RADIUS クライアント (無線アクセスポイント) | 1.01 |
| NetAttest D3-SX15-A | ソリトンシステムズ | DHCP サーバー | 5.2.10 |
| Lenovo X390 | Lenovo | 802.1X クライアント (Client PC) | Windows 10 64bit Windows 標準サブリカント |
| MacBook Pro | Apple | 802.1X クライアント (Client PC) | 13.0.1 (macOS Ventura) |
| iPhone SE (2nd generation) | Apple | 802.1X クライアント (Client SmartPhone) | 16.1.1 |
| Pixel 5 | Google | 802.1X クライアント (Client SmartPhone) | 13 |

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-SX15A-A | 192.168.1.2/24 | UDP 1812 | secret |
| WAPM-AX8R | 192.168.1.1/24 | | secret |
| NetAttest D3-SX15-A | 192.168.1.3/24 | | |
| Client PC | DHCP | - | - |
| Client SmartPhone | DHCP | - | - |


2. NetAttest EPS の設定

NetAttest EPS のセットアップを下記の流れで行います。

1. サービス管理ページへのログイン
2. 初期設定ウィザード (システム、システム-2)の実行
3. 初期設定ウィザード (サービス)の実行
4. https サービスの再起動
5. RADIUS クライアントの登録
6. 利用者の登録
7. クライアント証明書の発行

2-1 サービス管理ページへのログイン

NetAttest EPS の初期設定は LAN1 から行います。初期の IP アドレスは「192.168.1.2/24」です。管理端末に適切な IP アドレスを設定し、Google Chrome もしくは Microsoft Edge から「https://192.168.1.2:2181」にアクセスしてください。



| 項目 | 値 |
|-------|------|
| ログイン名 | root |
| パスワード | root |

2-2 初期設定ウィザード（システム、システム-2）の実行

サービス管理ページにログイン後、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。

- 管理者アカウントの設定
- 日付と時刻の設定
- ホスト名の設定
- ネットワークの設定
- DNS の設定
- インターネット時刻サーバーの設定
- ライセンスの設定

ログイン後に表示される画面より、「セットアップをはじめる」→「すすめる」→「はじめる」と進み、初期設定ウィザードの「システム」に関する設定を行います。

管理者アカウント

管理者アカウントのパスワード

アカウント名（アカウント名は変更できません） ⓘ

root

新規パスワード* ⓘ ■■■■■ 弱い

新規パスワードの確認*

| 項目 | 値 |
|---------|------|
| 新規パスワード | root |

日付と時刻

日付と時刻*

自動的に日付と時刻を設定 ⓘ ☒

手動で日付と時刻を設定 ⓘ

2022/08/04 13:18:05 ⓘ

タイムゾーン*

現在の設定

Asia/Tokyo 変更するとシステムの再起動が必要となります。

自動的にタイムゾーンを設定 ⓘ ☒

手動でタイムゾーンを選択 ⓘ

Asia/Tokyo ▼

| 項目 | 値 |
|---------------|----|
| 自動的に日付と時刻を設定 | ON |
| 自動的にタイムゾーンを設定 | ON |

ON とした場合、管理用 PC の情報をこの EPS に設定します。手動で設定する場合は OFF とします。

ホスト名

ホスト名
完全修飾ドメイン名 (FQDN) * ②
EPSの識別名として管理ページやログ上に表示されます。
また、EPSが発行するサーバー証明書や、EPSが発行する各証明書のCRL配布ポイントなどに記載されます。

naeps.example.com 変更するとシステムの再起動が必要となります。

ニックネーム ②
ニックネームには、設置先や用途などを自由に入力できます。
ホスト名の補助情報として、管理ページ上に表示されます。最大文字数は32文字です。
例：○○支店向け認証サーバー、無線LAN認証用サーバー

認証用サーバー (最大文字数3)

ネットワーク

LAN1
☒ 有効
IPアドレス ② 192.168.1.2 サブネットマスク ② 255.255.255.0

LAN2
☐ 有効
IPアドレス ② 192.168.2.2 サブネットマスク ② 255.255.255.0

LAN2を使用しない場合は無効化してください。LAN3～LAN4を有効化することもできます。
LAN3～LAN4を設定する・・・

デフォルトゲートウェイ ②
192.168.1.254

DNS

DNSサーバー
プライマリDNSサーバー ②
192.168.0.1
セカンダリDNSサーバー ②
192.168.0.2

設定の確認

管理者アカウント 変更する
パスワード


日付と時刻 変更する
日時 2022/08/04 13:35:26
タイムゾーン Asia/Tokyo

ホスト名 変更する
完全修飾ドメイン名 (FQDN) naeps.example.com
ニックネーム


ネットワーク 変更する
LAN1 192.168.1.2/255.255.255.0

もどる 確定

| 項目 | 値 |
|--------|-------------------|
| ホスト名 | naeps.example.com |
| ニックネーム | (任意) |

 ニックネームは、この EPS の設置先や用途など、任意の情報を入力できます。ホスト名の補助情報としてサービス管理ページ上に表示されます。

| 項目 | 値 |
|--------------|---------------|
| LAN1 IP アドレス | 192.168.1.2 |
| サブネットマスク | 255.255.255.0 |
| LAN2 | 無効 |
| デフォルトゲートウェイ | - |

 今回の環境では LAN2 は利用しないため無効としています。なお、LAN2 は V5.0.4 以降でデフォルト有効となっています。

| 項目 | 値 |
|----------------|---|
| プライマリ DNS サーバー | - |
| セカンダリ DNS サーバー | - |

ここからは、システム初期セットアップウィザードの「システム-2」に関する設定を行います。

インターネット時刻サーバー

インターネット時刻サーバー

現在の日時 2022/08/04 13:37:13

| | |
|----------|--|
| NTPサーバー1 | <input type="text" value="ntp.nict.jp"/> |
| NTPサーバー2 | <input type="text" value="ntp.nict.jp"/> |
| NTPサーバー3 | <input type="text" value="ntp.nict.jp"/> |

自動的にインターネット時刻サーバーと同期する 

☐ OFF

NTPの状態

[更新](#)

An illustration showing the completion of system initial setup. At the top, the text 'システムの初期設定が完了しました。' (System initial setup is complete.) is displayed. Below it, a central message reads 'おつかれさまでした。' (Thank you for your hard work.) followed by 'システムの初期設定が完了しました！' (System initial setup is complete!). A paragraph explains that the IP address and default gateway settings have been updated. It then instructs the user to click a button labeled '変更後の設定を有効にするには【変更後のネットワーク設定を有効にする】をクリックしてください。' (To enable the settings after change, please click [Enable the network settings after change].) to activate the changes. A red button with the text 'システムを再起動する' (Restart system) is shown. The final instruction is 'システム設定の変更を反映するにはシステムのリブートが必要ですよ。' (To reflect the system settings change, you need to reboot the system.). The background features a stylized cityscape with a large gear icon and a green bar at the bottom with the text 'サーバーの初期設定にすむ' (Complete server initial setup).

システム初期設定ウィザード

システムを再起動します。よろしいですか？


キャンセル 再起動

システムの再起動

システムの再起動を実行しました。しばらく待ってから再度ログインしてください。

OK

| 項目 | 値 |
|------------------------|-----|
| NTP サーバー1 | - |
| NTP サーバー2 | - |
| NTP サーバー3 | - |
| 自動的にインターネット時刻サーバーと同期する | OFF |

 今回の環境では NTP サーバーがないため設定をしていませんが、証明書の有効期間や、ログの時刻を正確なものにするために、実際の環境では NTP サーバーを利用いただくことを強く推奨します。

2-3 初期設定ウィザード (サービス)の実行

OS 再起動が完了後、再度サービス管理ページにアクセス及びログインし、サービス初期設定ウィザードを使用して、以下の項目を設定します。

- 認証の用途の設定
- 認証の方式の設定
- 利用者情報リポジトリの設定
- CA 構築
- サーバー証明書発行

NetAttest EPS へようこそ

早速、セットアップを進めていきましょう。

「セットアップをはじめる」ボタンから、初期設定を開始します。

はじめて使用する場合

セットアップをはじめる

その他

- ・ 前回のつづきをはじめる
- ・ バックアップからリストア
- ・ ファームウェアの変更(インストール済み 5.0.4 (build: 20220719151347))
- ・ EPS V4.10 バックアップデータの移行

☐ 次回以降、表示しない

サービスの初期設定

つぎに、サービスの初期設定をすすめていきましょう。

RADIUS認証や証明書の発行を行うための設定をお手伝いします。

クイック設定

簡単な質問に答えてセットアップをすすめていきます。

一般的な構成では、クイック設定で構築を完了することができます。

詳細な項目は自動的に設定されます。

クイック設定の結果で現在の設定が上書きされます。

カスタム設定

環境や用途に応じて、高度な設定を行う場合に適しています。

RADIUS、CA、LDAP等の詳細な項目を手動で設定します。

例：下位CAとして構築、RADIUSサービスを利用しない

レプリカとして構成

冗長構成のレプリカとして設定します。

クイック設定をはじめる

利用用途についての質問に答えて、サービスの設定をすすめていきましょう。

設定終了時に、利用開始までのステップをご案内します。

キャンセル

はじめる

認証の用途

どのような用途で認証を利用しますか？

複数選択可能

☒ 無線LAN(Wi-Fi)や、有線LANの認証

☐ VPNの認証

それ以外の用途の場合はこちら

認証の方式（無線/有線LAN）

無線LAN(Wi-Fi)や有線LANでどの認証方式を使用しますか？
使用する認証方式を選択してください。
複数の認証方式をEPSで受け付ける場合は、それぞれを選択します。②

1つ以上の方式をお選び下さい。複数選択が可能です

☒ 証明書で認証 (EAP-TLS) ②

☒ このEPSに登録したID・パスワードで認証 (EAP-PEAP) ②

☐ Active Directoryに登録したID・パスワードで認証 (EAP-PEAP) ②

☐ MACアドレス認証 (PAP) ②

その他の認証方式の場合はこちら

利用者情報リポジトリ

どこに格納された利用者情報で認証しますか？
利用者情報は、EPS内部のデータベースへ登録するか、外部データベースを参照するかを選択できます。
MACアドレスの情報はMACアドレスデータベースに登録します。

複数選択可能

☒ ローカル利用者データベース ②

☐ ローカルMACアドレスデータベース ②

☐ その他のLDAPサーバー/他のEPS ②

CA

CAの情報

ここで入力した情報は、EPSが発行する各種証明書に記録されます。
この値を後で変更するには、CAの再構築が必要となります。

CA名* ②
TestCA

国名 ②
日本

都道府県名 ②
Tokyo-to

市区町村名 ②
Shinjuku-ku

会社名(組織名) ②
Soliton Systems

部署名 ②
R&D

メールアドレス ②
ca.admin@example.com

有効期限

有効日数* ②
3650

| 項目 | 値 |
|----------|-----------------|
| CA 名 | TestCA |
| 国名 | 日本 |
| 都道府県名 | Tokyo-to |
| 市区町村名 | Shinjuku-ku |
| 会社名(組織名) | Soliton Systems |
| 部署名 | - |
| メールアドレス | - |
| 有効日数 | 3650 |

サーバー証明書

この値を後で変更するには、サーバー証明書の再発行が必要となります。

サーバー名*

naeps.example.com

国名 都道府県名 市区町村名

日本 Tokyo-to Shinjuku-ku

会社名(組織名) 部署名

Your Company Name RDD

DNS名

☒ 自身のホスト名

IPアドレス

☒ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4

任意設定

DNS.naca.example.com/IP:15

有効期限

有効日数*

730

鍵と署名ハッシュアルゴリズム

公開鍵方式 鍵長

RSA 2048bits

署名ハッシュアルゴリズム

SHA256

| 項目 | 値 |
|--------------|--------------|
| 国名 | 日本 |
| 都道府県名 | Tokyo-to |
| 市区町村名 | Shinjuku-ku |
| 会社名(組織名) | - |
| 部署名 | - |
| DNS 名 | 自身のホスト名 : 有効 |
| IP アドレス | LAN1 のみ有効 |
| 任意設定 | - |
| 有効日数 | 730 |
| 公開鍵方式 | RSA |
| 鍵長 | 2048bits |
| 署名ハッシュアルゴリズム | SHA256 |



「有効日数」の設定箇所は、証明書の更新運用も考慮してください。クライアント OS や RADIUS クライアントによっては、サーバー証明書の最長有効日数に制限がある場合があります。一例として、iOS 13 以降では最長でも 825 日(EPS の設定値は 824 日)とすることをお勧めいたします。

設定の確認

認証の用途 変更する

無線(LAN/Wi-Fi)や、有線LANの認証

認証方式 変更する

証明書認証(EAP-TLS)

利用者情報リポジトリ 変更する

ローカル利用者データベース

LDAPデータベース

もどる 確定

サービスの構築

- ✓ LDAPデータベースの構築が完了しました
- ✓ CAを構築しました
- ✓ サーバー証明書を更新しました
- ✓ RADIUSサーバーを設定しました
- ✓ LDAPサービスを起動しました
- ✓ RADIUSサービスを起動しました
- ✓ 利用者ページサービスを起動しました

[次へ](#)

サービスの初期設定が完了しました

おつかれさまでした。サービスの初期設定が完了しました。
詳細な設定項目は、管理ページから設定・変更できます。

続けて、環境別の利用の準備にすすみましょう。
いよいよ、ファイナルステップです。

[設定完了](#)

利用の準備

ご利用にあたり、以下の設定・登録が必要です。
一つひとつ、準備をしていきましょう。
スキップした場合は、管理ページのヘッダーから再開できます。

未
未

- > RADIUSクライアントの登録
- > 利用者の登録

[スキップしてダッシュボードへ進む](#)

2-4 https サービスの再起動

画面上部に「https サービスを再起動する」ボタンを選択し、https サービスの再起動を行います。https サービスを再起動するとページの再読み込みを求められるため、ページの再読み込みを行います。



サーバー証明書が更新されました。https サービスの再起動が必要です。再起動中は数秒間、利用者ページ、サービス管理ページ、システム管理ページにアクセスできなくなります。再起動後、ブラウザによるページ再読み込みが必要となる場合があります。

https サービスを再起動する



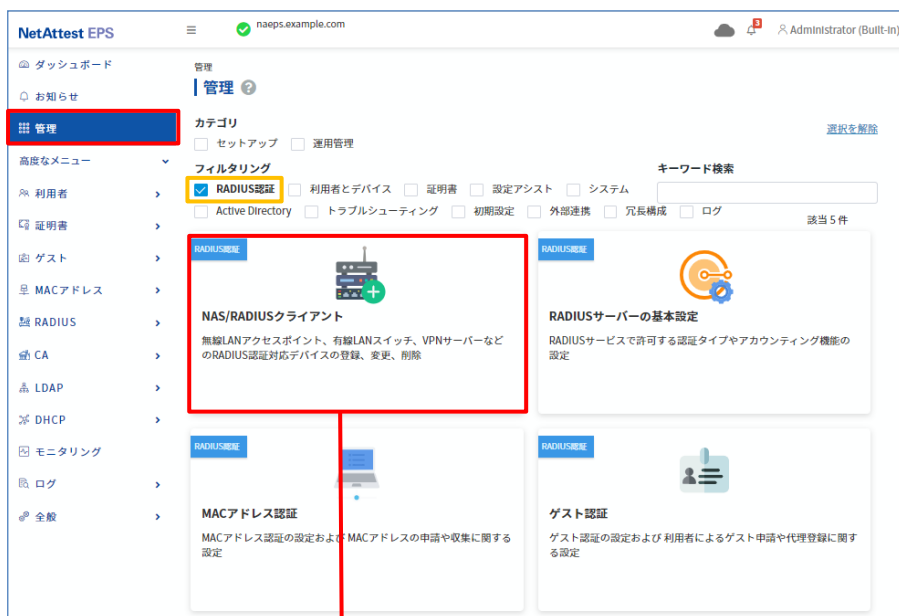
HTTPSサービス

サーバー証明書が更新されたために再読み込みが必要である可能性があります。

再読み込み

2-5 RADIUS クライアントの登録

サービス管理画面の「管理」メニューにて「RADIUS 認証」でフィルタリングし、「NAS/RADIUS クライアント」を選択します。表示された画面で「新規登録」ボタンを選択し、RADIUS クライアントの登録を行います。



NAS/RADIUSクライアント設定

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

シークレット

.....

NASグループ

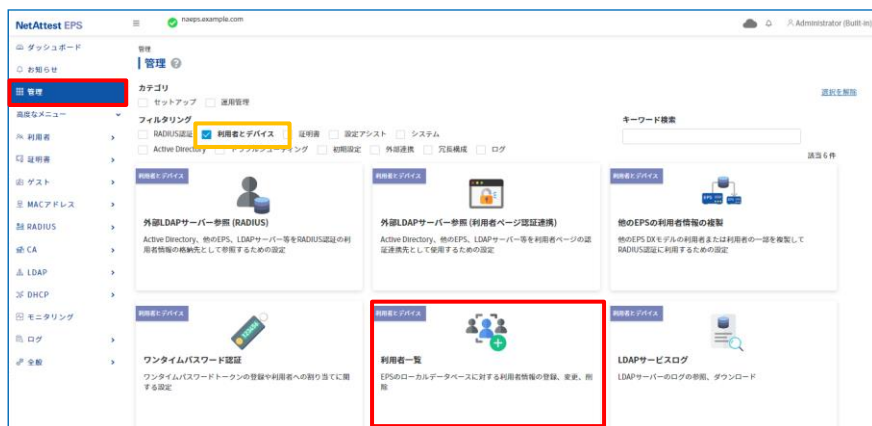
NAS識別値

キャンセル 実行

| | 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 |

2-6 利用者の登録

サービス管理画面の「管理」メニューにて「利用者とデバイス」でフィルタリングし、「利用者一覧」を選択します。表示された画面で「新規登録」ボタンを選択し、利用者登録を行います。



利用者設定

利用情報 チェックアイテム リプライアイテム OTP

利用者情報

基本情報

名前* user01 氏名

名前(フリガナ)

セイ

メールアドレス user01@example.test

役割

認証情報

ログイン名* user01

パスワード* 強い

パスワード (確認) *

利用ページ

ロール

キャンセル 登録

| 項目 | 値 |
|-------|----------|
| 名前 | user01 |
| ログイン名 | user01 |
| パスワード | password |



2-7 クライアント証明書の発行

サービス管理画面より、クライアント証明書の発行を行います。[利用者一覧]ページから該当する利用者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)

NetAttest EPS

naeps.example.com

利用の準備

Administrator (Built-in)

ダッシュボード

お知らせ

管理

高度なメニュー

利用者

利用者一覧

利用者パスワードポリシー

利用者 > 利用者一覧

利用者一覧 ?

検索キーワードを入力してください。

検索条件

条件をクリア

新規登録 インポート エクスポート

1-1/1 10 件/ページ

| 名前 | ログイン名 | 状態 | 証明書 |
|---------------------------------|--------|----|-----------------------|
| <input type="checkbox"/> user01 | user01 | | 証明書発行 |

利用者証明書発行 ?

基本情報

名前

user01

メールアドレス

詳細情報

ロール

証明書申請管理

認証情報

ログイン名

user01

有効期限

☒ 日数 365 日

☐ 日付 2022/08/04 23:59:59 まで

証明書ファイルオプション

パスワード

パスワード (確認)

※パスワードが空欄の場合は、利用者のパスワードを使用します。

☒ PKCS#12ファイルに証明機関の証明書を含める

キャンセル 発行

| 項目 | 値 |
|--------------------------|-----|
| 有効期限 | 365 |
| PKCS#12 ファイルに証明機関の . . . | 有効 |

3. WAPM-AX8R の設定

下記の手順で WAPM-AX8R の設定を行います。

1. WAPM-AX8R へログイン
2. WAPM-AX8R へ LAN 側 IP アドレスを設定
3. WAPM-AX8R へ RADIUS を設定
4. WAPM-AX8R へ SSID を設定

尚、設定の際には PC を WAPM-AX8R と LAN ケーブルで直結して WEB ブラウザから行います。

3-1～3-4 の項目の設定が完了次第、WAPM-AX8R を L2 スイッチに接続します。

既に L2 スイッチに接続済みの場合には、L2 スイッチから切り離し、AP を再起動して下さい。

※設定用 PC のネットワーク設定は IP アドレス : 192.168.11.1/24 とします。

3-1 WAPM-AX8R ヘログイン

WEB ブラウザから[http://192.168.11.100]へアクセスし、WAPM-AX8R ヘログインします。
下記のようなログイン画面が表示されますので、各項目に値を入力しログインします。



The login screen for the Buffalo AirStation Pro WAPM-AX8R. It features the Buffalo logo at the top, followed by the product name and version (WAPM-AX8R Version 1.01). Below this are two input fields: 'ユーザー名' (Username) with the value 'admin' and 'パスワード' (Password) with masked characters. A 'ログイン' (Login) button is at the bottom.

| 項目 | 値 |
|-------|----------|
| ユーザー名 | admin |
| パスワード | password |



The configuration page for the Buffalo AirStation Pro WAPM-AX8R. A red arrow points from the login button to this page. The page has a navigation bar with 'Home', '詳細設定' (Detailed Settings), 'システム情報' (System Information), and 'ログアウト'. The '詳細設定' tab is selected. The main content area is divided into several sections: '機能設定' (Function Settings) with sub-sections for '無線' (Wireless), 'その他' (Others), and '緊急時モード' (Emergency Mode); 'ファームウェア情報' (Firmware Information); '無線情報' (Wireless Information) showing 2.4GHz and 5GHz settings; and 'Language' with a dropdown set to 'Japanese' and a 'Change Language' button. The footer contains the copyright notice: 'Copyright © 2021 Buffalo Inc.'.

3-2 WAPM-AX8R へ LAN 側 IP アドレスを設定

ログイン後に「詳細設定」をクリックし、LAN 側 IP アドレスを設定します。

「LAN 設定」 - 「IP アドレス」より、下記の通り設定します。

| 項目 | 値 |
|----------------|---------------|
| IP アドレス | - |
| - IP アドレスの取得方法 | 手動設定 |
| - IP アドレス | 192.168.1.1 |
| - サブネットマスク | 255.255.255.0 |
| - デフォルトゲートウェイ | 192.168.1.254 |
| DNS サーバー | - |
| - プライマリー | 8.8.8.8(任意) |
| - セカンダリー | 8.8.4.4(任意) |
| DHCP サーバー | - |
| - DHCP サーバー機能 | 使用しない |

値入力後、「設定」をクリックすると、以下確認画面が表示されますので、再度「設定」をクリックして設定内容を反映します。

設定が完了しました。再スタートしています。

あと約 43 秒、お待ちください。

その後、設定を続ける場合は、次の手順を行ってください。

1. WEBブラウザを全て終了してください。
2. お使いのパソコンとエアステーションが通信できる設定になっている事を確認してください。
3. 設定ユーティリティからWEBブラウザを起動してエアステーションのWEB設定を行ってください。

設定ユーティリティのインストール方法・使い方につきましては、マニュアルを参照してください。

設定反映後、WEB ブラウザを終了し、PC 側のネットワーク設定を WAPM-AX8R に設定した IP アドレス(192.168.1.1)に接続できるように設定し、再度ログインします。

3-3 WAPM-AX8R へ RADIUS を設定

再ログイン後に「詳細設定」をクリックし、RADIUS を設定します。

「ネットワーク設定」 - 「RADIUS」 - 「RADIUS 設定」より、下記の通り設定します。

RADIUS設定

RADIUSサーバー

プライマリ-RADIUSサーバー

| | |
|-----------------|--|
| サーバー | <input type="radio"/> 内蔵 <input checked="" type="radio"/> 外部 |
| サーバー名 | 192.168.1.2 |
| 認証ポート | 1812 |
| Accounting | <input checked="" type="checkbox"/> 使用する |
| Accountingポート | 1813 |
| Shared Secret | ***** |
| Session-Timeout | 3600 秒 |

セカンダリ-RADIUSサーバー

| | |
|-----------------|--|
| サーバー | <input type="radio"/> 内蔵 <input checked="" type="radio"/> 外部 |
| サーバー名 | |
| 認証ポート | 1812 |
| Accounting | <input checked="" type="checkbox"/> 使用する |
| Accountingポート | 1813 |
| Shared Secret | |
| Session-Timeout | 3600 秒 |

Calling-Station-Id ""(区切りなし, 小文字)
Called-Station-Id ""(区切りなし, 小文字)

設定

| 項目 | 値 |
|------------------|-------------|
| プライマリ-RADIUSサーバー | - |
| - サーバー | 外部 |
| - サーバー名 | 192.168.1.2 |
| - 認証ポート | 1812 |
| - Shared Secret | secret |

値入力後、「設定」をクリックして設定内容を反映します。

設定が完了しました。再スタートしています。

あと約 17 秒、お待ちください。

17 秒後、画面が切り換わらない時は [ここ](#) をクリックしてください。

3-4 WAPM-AX8R へ SSID を設定

続いて「詳細設定」の項目から、SSID を設定します。

「無線設定」 - 「無線基本」 - 「SSID 設定」より、SSID 編集の「新規追加」をクリックします。

下記の通り設定を行い、「編集を終了して前の画面へ戻る」をクリック。

| 項目 | 値 |
|--------|----------------------------------|
| 無線 LAN | 有効 |
| SSID | SolitonLab(任意) |
| 使用デバイス | 2.4GHz/5GHz 共にチェック |
| 無線の認証 | WPA2 Enterprise |
| 暗号化方式 | AES |
| RADIUS | ネットワーク設定内の RADIUS サーバー設定を使用する |

以下確認画面が表示されますので、「設定」をクリックして設定内容を反映します。

SSID設定
内容:SSIDを変更します。パソコン側の無線LAN設定も再設定してください。

設定を行う場合は「設定」ボタンを押してください。

その後、設定を続ける場合は、次の手順を行ってください。

1. WEBブラウザを全て終了してください。
2. お使いのパソコンとエアステーションが通信できる設定になっている事を確認してください。
3. 設定ユーティリティからWEBブラウザを起動してエアステーションのWEB設定を行ってください。

設定ユーティリティのインストール方法・使い方につきましては、マニュアルを参照してください。

設定 設定中止

設定が完了しました。再スタートしています。

あと約 17 秒、お待ちください。

その後、設定を続ける場合は、次の手順を行ってください。

1. WEBブラウザを全て終了してください。
2. お使いのパソコンとエアステーションが通信できる設定になっている事を確認してください。
3. 設定ユーティリティからWEBブラウザを起動してエアステーションのWEB設定を行ってください。

設定ユーティリティのインストール方法・使い方につきましては、マニュアルを参照してください。

設定した SSID が有効になっている事を確認します。

SSID設定 - SSIDの編集

ステアリング ポリシー設定

ステアリング ポリシー

設定

SSID編集

| Index | 状態 | SSID | VLAN ID | 2.4GHz | 5GHz | ステアリング | 無線の認証 | 暗号化 |
|-------|----|-------------|---------|-----------------------|-----------------------|--------|---------------------|---|
| 1 | 有効 | SolitonLab1 | | <input type="radio"/> | <input type="radio"/> | 無効 | WPA2 Enterprise AES | <input type="button" value="編集"/> <input type="button" value="削除"/> |

また、Home 画面の無線情報で SSID が有効になっているか確認します。

BUFFALO WAPM-AX8R Intelligent Wireless LAN Access Point **AirStation Pro**

Home 詳細設定 システム情報 ログアウト

機能設定

無線

無線LANのSSIDと暗号化を設定する(WEP/TKIP/AES)

無線LANのチャンネルを設定する

その他

エアステーションのファームウェアを更新する

エアステーションの設定を初期化する

緊急時モード

緊急時モード

ファームウェア情報

WAPM-AX8R Version 1.01

無線情報

2.4GHz

無線モード 11b/g/n/ax

チャンネル Auto(1~11)
Ch 11 / 20MHz

SSID 1 個のSSIDが有効です

5GHz

無線モード 11a/n/ac/ax

チャンネル Auto(W52)
Ch 36 / 80MHz

SSID 1 個のSSIDが有効です

Language

Japanese

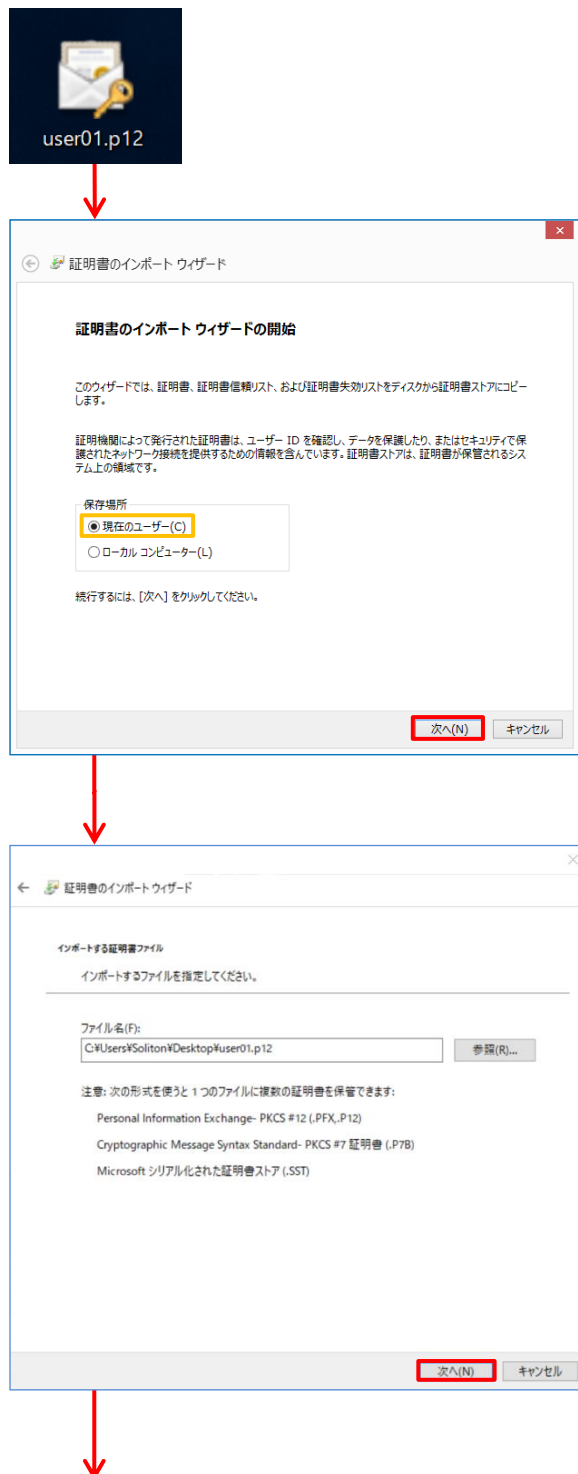
以上で WAPM-AX8R の設定は完了です。

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。



証明書のインポート 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(I):

☐ 秘密キーの保護を有効にする(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】

「2-6 利用者の登録」で設定したパスワードを入力

証明書のインポート 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)

☐ 証明書をすべて既定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

証明書のインポート 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:

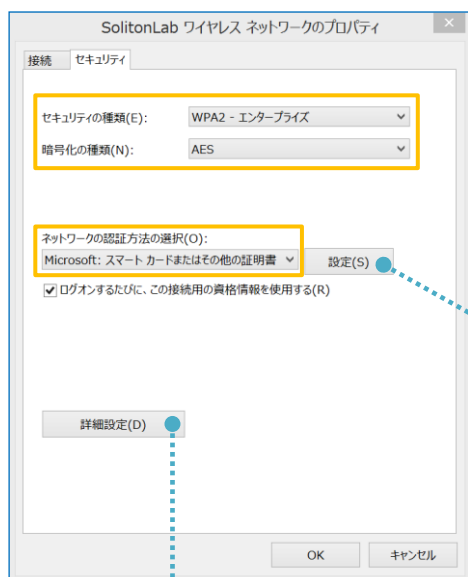
| | |
|-------------|--|
| 選択された証明書ストア | ウィザードで自動的に決定されます |
| 内容 | PFX |
| ファイル名 | C:\Users\Soliton\Downloads\User01_02.p12 |

完了(F) キャンセル

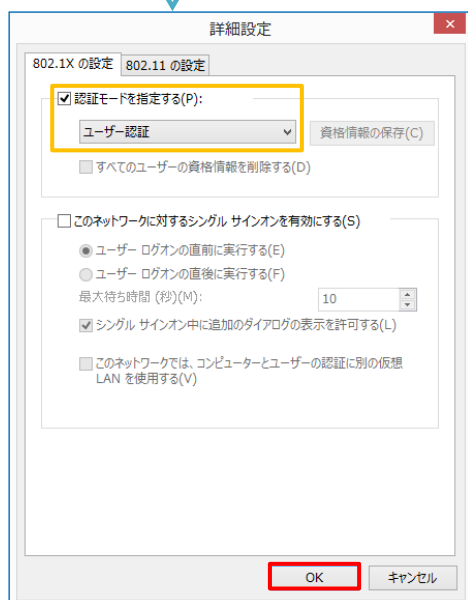
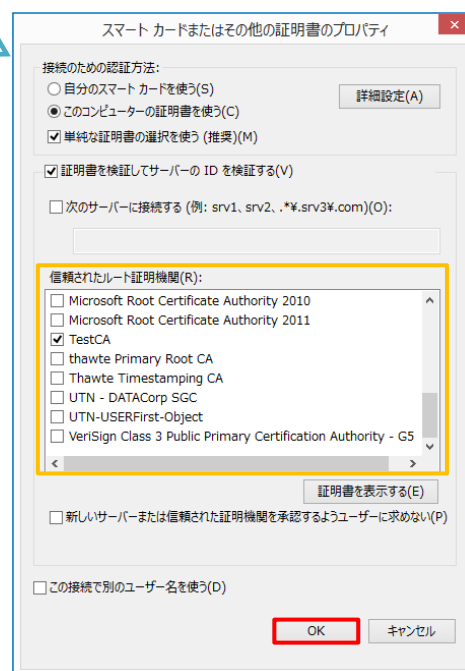
4-1-2 サプリカント設定

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 |

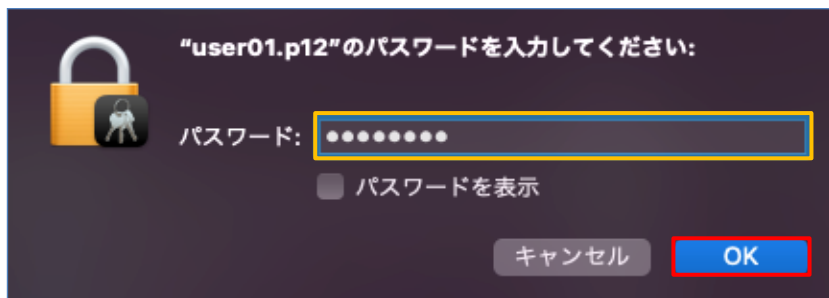
| 項目 | 値 |
|-----------------------|--------|
| 接続のための認証方法 | |
| - このコンピューターの証明書を・・・ | On |
| - 単純な証明書の選択を使う (推奨) | On |
| 証明書を検証してサーバーの ID を・・・ | On |
| 信頼されたルート証明機関 | TestCA |

4-2 Mac での EAP-TLS 認証

4-2-1 クライアント証明書のインポート

PC にデジタル証明書をインポートします。

「キーチェーンアクセス」を起動し、[デフォルトキーチェーン] - [ログイン]を選択後、PKCS#12 ファイルをドラッグ&ドロップし、PKCS#12 ファイル のパスワードを入力します。



インポートした CA 証明書の信頼設定を変更します。

インポートした CA 証明書をダブルクリックし、[信頼] - [この証明書を使用するとき]の項目で「常に信頼」に変更します。



ウィンドウを閉じると、パスワードを求められるため、端末(Mac)に設定しているパスワードを入力し、「設定をアップデート」を選択します。



参考)

CLI コマンドを利用して、PKCS#12 ファイルをインポートすることも可能です。

PKCS#12 ファイルをデスクトップ上へ保存し、ターミナルで以下のコマンドを入力します。

```
security import /Users/<ログインユーザーID>/Desktop/<証明書ファイル名> -k /Users/<ログインユーザーID>/Library/KeyChains/Login.keychain-db -f pkcs12 -x
```

「ログインユーザーID」、「証明書ファイル名」は、環境に合わせて書き換えて下さい。



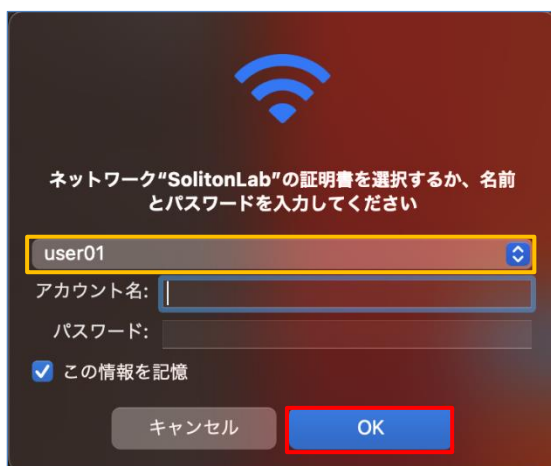
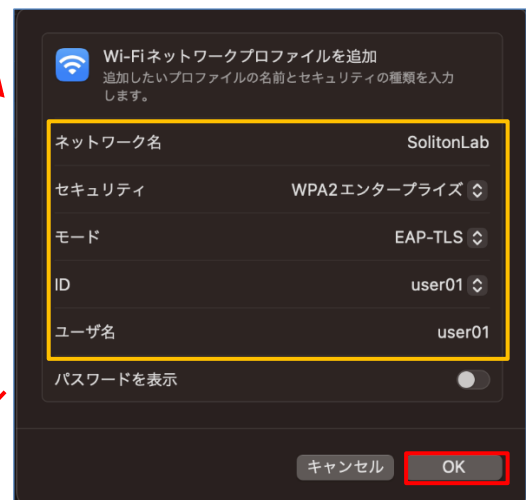
V11.6.6 (macOS Big Sur) 及び V12.5 (macOS Monterey) で確認したところ、コマンドラインからエクスポート禁止オプション ("-x") を設定してインポートしても、キーチェーンアクセスから秘密鍵をエクスポート出来てしまうようです。

なお、ソリトンシステムズの証明書配布ソリューションである EPS-ap を利用してクライアント証明書をインポートした場合は、秘密鍵のエクスポートは不可の状態となります。

4-2-2 サプリカント設定

Mac 標準サプリカントで TLS の設定を行います。

メニューバーのネットワークのアイコンをクリックして、「Wi-Fi 設定…」をクリックし、以下の設定を行います。



| 項目 | 値 |
|---------|---------------|
| ネットワーク名 | ネットワーク名(SSID) |
| セキュリティ | WPA2 エンタープライズ |
| モード | EAP-TLS |
| ID | user01 |
| ユーザ名 | User01 |



4-3 iOS 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 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)

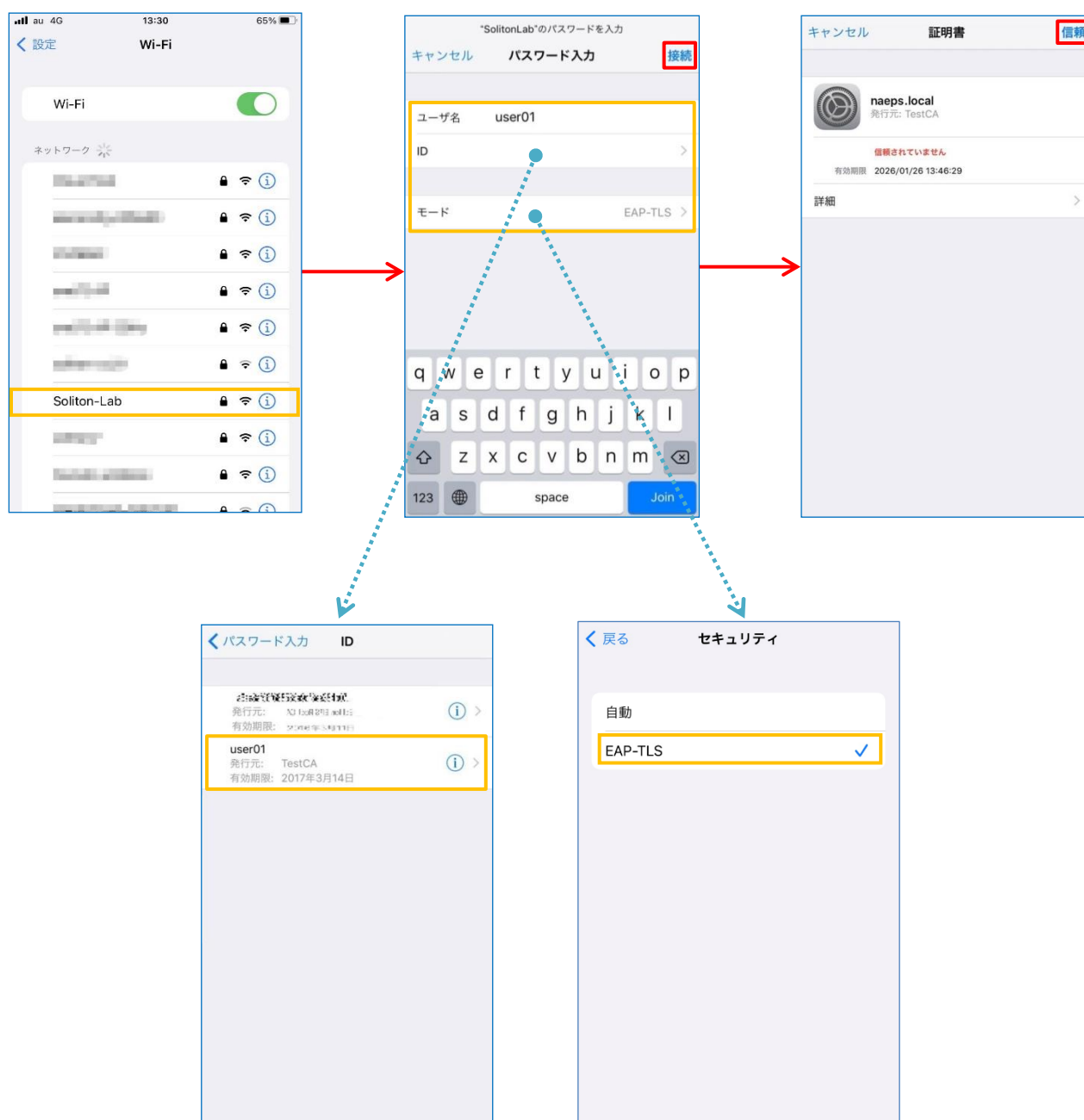
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

4-3-2 サプリカント設定

WAPM-AX8R 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「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。



4-4 Android での EAP-TLS 認証

4-4-1 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 13 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、クライアント証明書は「Wi-Fi 証明書」を選択しています。



4-4-2 サプリカント設定

WAPM-AX8R 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。



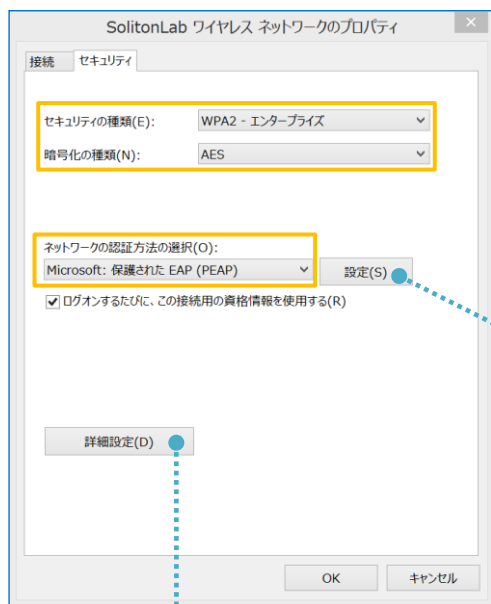
| 項目 | 値 |
|---------|-------------|
| EAP 方式 | TLS |
| CA 証明書 | TestCA |
| ドメイン | example.com |
| ユーザー証明書 | TestCA |
| ID | user01 |

5. EAP-PEAP 認証でのクライアント設定

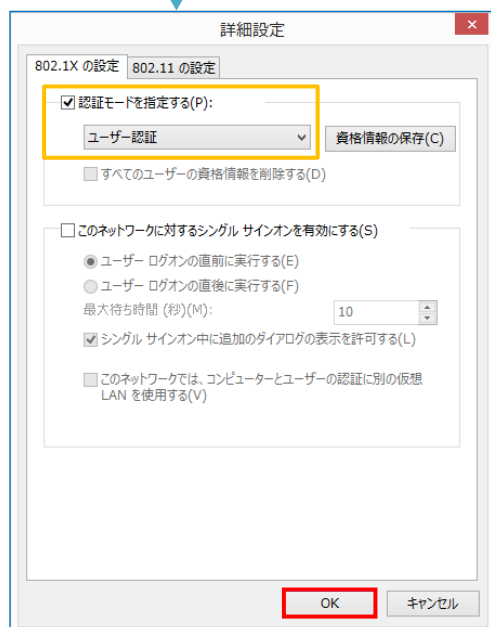
5-1 Windows 10 での EAP-PEAP 認証

5-1-1 Windows 10 のサブリカント設定

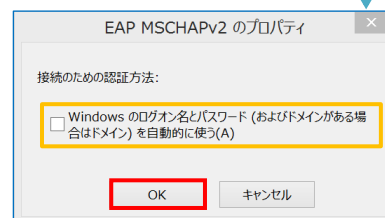
[ワイヤレスネットワークのプロパティ] の「セキュリティ」タブから以下の設定を行います。



| 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 |



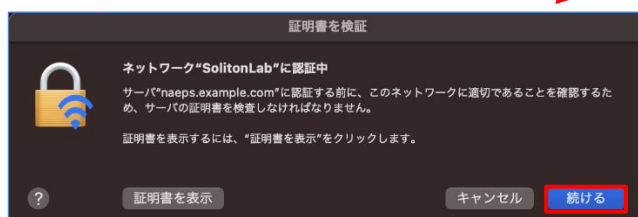
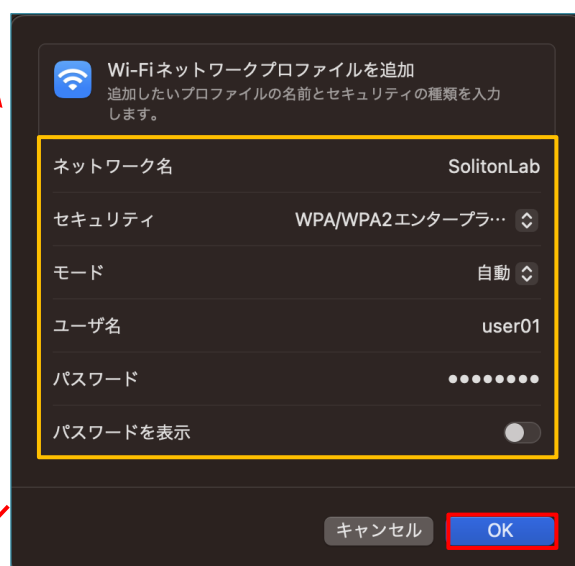
| 項目 | 値 |
|----------------------|--------|
| 接続のための認証方法 | |
| - サーバー証明書の検証をする | On |
| - 信頼されたルート認証機関 | TestCA |
| - Windows のログオン名と・・・ | Off |

5-2 Mac での EAP-PEAP 認証

5-2-1 Mac のサブリカント設定

Mac 標準サブリカントで PEAP の設定を行います。

メニューバーのネットワークのアイコンをクリックして、「Wi-Fi 設定…」をクリックし、以下の設定を行います。



| 項目 | 値 |
|---------|---------------|
| ネットワーク名 | ネットワーク名(SSID) |
| セキュリティ | WPA2 エンタープライズ |
| モード | 自動 |
| ユーザ名 | user01 |
| パスワード | password |

5-3 iOS での EAP-PEAP 認証

5-3-1 iOS のサブリカント設定

WAPM-AX8R で設定した SSID を選択し、サブリカントの設定を行います。「ユーザ名」、「パスワード」には「2-6 利用者の登録」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 |

5-4 Android での EAP-PEAP 認証

5-4-1 Android のサブリカント設定

WAPM-AX8R 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「2-6 利用者の登録」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。

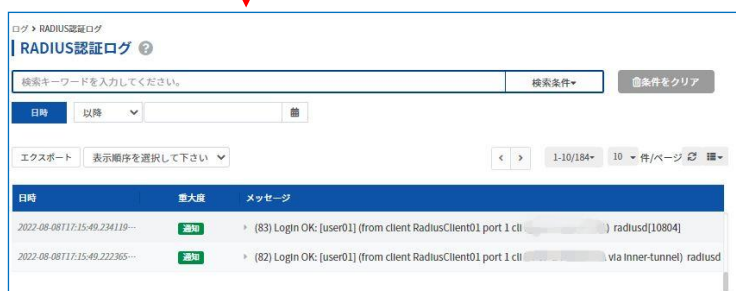
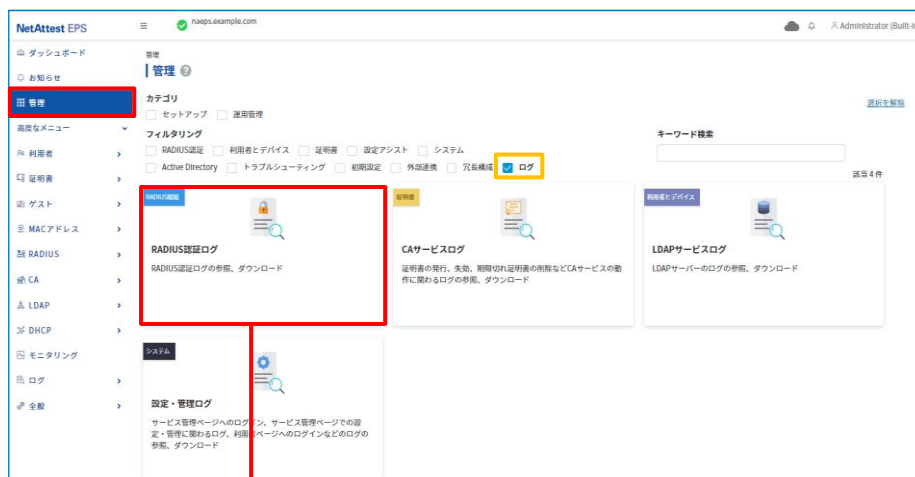


| 項目 | 値 |
|-----------|-------------|
| EAP 方式 | PEAP |
| フェーズ 2 認証 | MSCHAPV2 |
| CA 証明書 | TestCA |
| ドメイン | example.com |
| ID | user01 |
| パスワード | password |

6. 動作確認

6-1 RADIUS 認証ログの確認(EPS)

EPS の RADIUS 認証ログは、サービス管理画面の「管理」メニューにて「ログ」でフィルタリングし、「RADIUS 認証ログ」を選択することで確認可能です。



6-2 認証ログの確認(WAPM-AX8R)

Home 画面より「機器診断」-「ログ情報」をクリックし、ログを表示します。

認証ログのみを表示する場合は上部のチェックボックスの「認証」をチェックし、表示をクリックします。

AirStation Pro

HOME LOGOUT

WAPM-AX8R

LAN設定

ネットワーク設定

無線設定

管理設定

機器診断

システム情報

ログ情報

USB

通信パケット情報

無線環境モニター

CPUモニター

I'm Here

pingテスト

ログ情報

☐ DHCPクライアント
 ☐ DHCPサーバー

☐ USB
 ☐ 無線クライアント

☒ **認証**
☐ 設定変更

☐ システム起動
 ☐ NTPクライアント

☐ 有線リンク
 ☐ ADT

表示 全てチェックする 全てチェック外す

ログ情報

ファイル(logfile.log)に保存する

2021/01/01 04:12:58

| 日付時刻 | 種類 | ログ内容 |
|---------------------|------|--|
| 2021/01/01 04:07:52 | AUTH | w10.0 (5GHz): Authenticated (WPA2-EAP: TTL 1800) User [user01] - 36:b3:86:45:19:c3 |
| 2021/01/01 04:07:15 | AUTH | w10.0 (5GHz): Authenticated (WPA2-EAP: TTL 1800) User [user01] - 36:b3:86:45:19:c3 |
| 2021/01/01 04:05:14 | AUTH | w10.0 (5GHz): Authenticated (WPA2-EAP: TTL 1800) User [user01] - 36:b3:86:45:19:c3 |
| 2021/01/01 04:04:15 | AUTH | w10.0 (5GHz): Authenticated (WPA2-EAP: TTL 1800) User [user01] - ac:ed:5c:69:a8:43 |
| 2021/01/01 04:04:15 | AUTH | w10.0 (5GHz): Session-Timeout expired [user01] - ac:ed:5c:69:a8:43 |
| 2021/01/01 03:56:53 | AUTH | w10.0 (5GHz): Authenticated (WPA2-EAP: TTL 1800) User [user01] - 3c:06:30:2d:6a:43 |
| 2021/01/01 03:53:52 | AUTH | w10.0 (5GHz): Authenticated (WPA2-EAP: TTL 1800) User [user01] - c6:80:3d:54:ca:bc |
| 2021/01/01 03:52:27 | AUTH | w10.0 (5GHz): Authenticated (WPA2-EAP: TTL 1800) User [user01] - c6:80:3d:54:ca:bc |
| 2021/01/01 03:51:00 | AUTH | w10.0 (5GHz): Authenticated (WPA2-EAP: TTL 983) User [user01] - c6:80:3d:54:ca:bc |
| 2021/01/01 03:37:24 | AUTH | w10.0 (5GHz): Authenticated (WPA2-EAP: TTL 1800) User [user01] - c6:80:3d:54:ca:bc |
| 2021/01/01 03:34:45 | AUTH | w10.0 (5GHz): Authenticated (WPA2-EAP: TTL 1800) User [user01] - 3c:06:30:2d:6a:43 |
| 2021/01/01 03:34:18 | AUTH | w10.0 (5GHz): Authenticated (WPA2-EAP: TTL 1800) User [user01] - ac:ed:5c:69:a8:43 |

・ 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 | <div>メッセージ</div> <ul style="list-style-type: none"> ▶ (29) Login OK: [user01] (from client RadiusClient01 port 1 cli [redacted]) radiusd[12050] ▶ (29) Login OK: [user01] (from client RadiusClient01 port 1 cli [redacted] via check-eap-tls) radiusd[12050] ▶ clientcert_Info: Serial:[redacted], Expiration:230809072025Z, ValidSince:220809071525Z, Subject:/C=JP/ST=Tokyo-to/L=Shinjuku-ku/O=Soliton Systems/CN=user01, Issuer:/C=JP/ST=Tokyo-to/L=Shinjuku-ku/O=Soliton Systems/CN=TestCA, CommonName:user01 radiusd[12050] ▶ cacert_Info: Serial:[redacted], Expiration:320805020335Z, ValidSince:220808015835Z, Subject:/C=JP/ST=Tokyo-to/L=Shinjuku-ku/O=Soliton Systems/CN=TestCA, Issuer:/C=JP/ST=Tokyo-to/L=Shinjuku-ku/O=Soliton Systems/CN=TestCA, CommonName:TestCA radiusd[12050] ▶ Adding client [redacted] radiusd[12050] |
| WAPM-AX8R | <div>種類 ログ内容</div> <div>AUTH w10.0 (5GHz): Authenticated (WPA2-EAP: TTL 1800) User [user01] - 36:b3:86:45:19:c3</div> |

・ 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 | <div>メッセージ</div> <ul style="list-style-type: none"> ▶ (86) Login OK: [user01] (from client RadiusClient01 port 1 cli [redacted]) radiusd[12050] ▶ (85) Login OK: [user01] (from client RadiusClient01 port 1 cli [redacted] via Inner-tunnel) radiusd[12050] ▶ Adding client [redacted] radiusd[12050] |
| WAPM-AX8R | <div>種類 ログ内容</div> <div>AUTH w10.0 (5GHz): Authenticated (WPA2-EAP: TTL 1800) User [user01] - 36:b3:86:45:19:c3</div> |

[illegible]