

NetAttest EPS Cloud

認証連携設定例

【連携機器】 Riverbed Xirrus XD2-240

【Case】 IEEE802.1X EAP-TLS

Rev2.0



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 NetAttest EPS Cloud と、Riverbed 社製無線アクセスポイント Xirrus XD2-240 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。

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 Cloud 及び Xirrus XD2-240 の操作方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

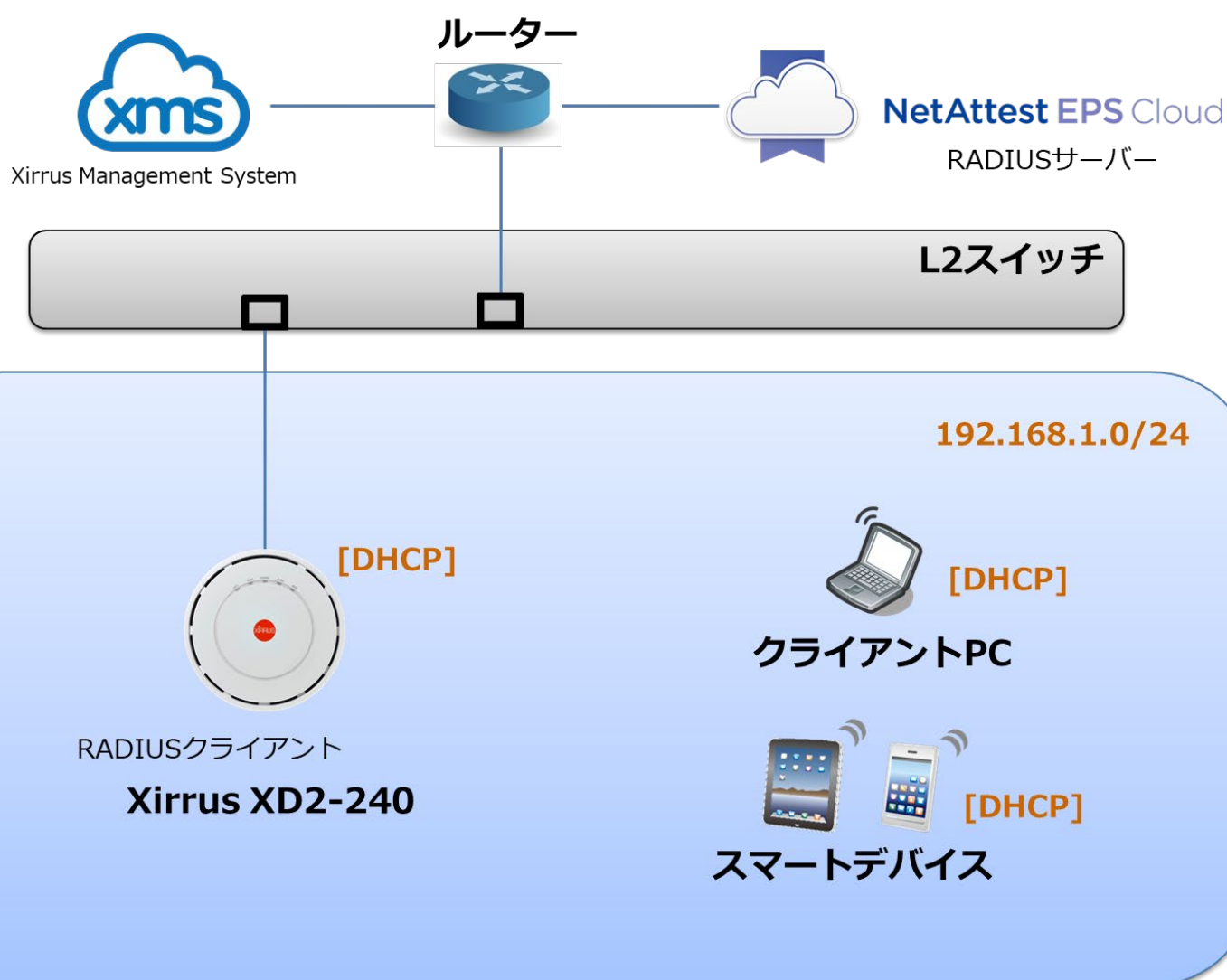
1. 構成.....	5
1-1 構成図.....	5
1-2 環境.....	6
1-2-1 機器.....	6
1-2-2 認証方式.....	6
1-2-3 ネットワーク設定.....	6
2. NetAttest EPS Cloud の設定.....	7
3. Xirrus XD2-240 の設定.....	8
3-1 プロファイルの作成.....	9
3-2 無線の設定.....	10
3-3 External RADIUS サーバーの設定.....	11
4. EAP-TLS 認証のクライアント設定.....	13
4-1 Windows 10 のサブリカント設定.....	13
4-2 iOS のサブリカント設定.....	14
4-3 Android のサブリカント設定.....	15
4-4 MacOS のサブリカント設定.....	16
5. 認証結果の確認手順.....	17
5-1 NetAttest EPS Cloud の RADIUS 認証ログ確認手順.....	17
5-2 Xirrus XD2-240 の接続端末確認手順.....	18
6. 動作確認結果.....	19

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



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 Cloud	ソリトンシステムズ	RADIUS/CA サーバー	-
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 標準サブリカント
iPhone 7	Apple	802.1X クライアント (Client SmartPhone)	iOS 11.3.1
Pixel C	Google	802.1X クライアント (Client Tablet)	Android 8.1.0

1-2-2 認証方式

IEEE802.1X EAP-TLS

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 Cloud	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 Cloud の設定

NetAttest EPS Cloud では、ご利用者様に提供されるアカウント通知書に、以下の様な RADIUS サーバーの情報が含まれています。この情報を元に無線アクセスポイントに設定を行って下さい。

本資料では、RADIUS サーバーの設定値を下表に記載した値として設定を行います。

RADIUS サーバーの IP アドレスは、実際にはグローバル IP アドレスとなります。

Soliton クライアント証明書認証サービス	
アカウント通知書	
Soliton クライアント証明書認証サービスにお申し込みいただきまして、誠に有り難う御座います。 本サービスをご利用いただくにあたり、必要な情報をお知らせいたします。	
サービス契約情報	
お客様名	株式会社ソリトンシステムズ
Plan	クライアント証明書認証サービス
開通日	2018年2月1日
契約ライセンス数	5
サポート ID	sp-000001
サービスポータル	
アクセス先 URL	https://www01.soliton-ods.jp
ユーザーID	XXXXXXXXXX
初期パスワード	string@123
RADIUS サーバー	
RADIUS サーバー(メイン)	192.168.1.2
RADIUS サーバー(バックアップ)	192.168.1.3
認証用ポート	1812
アカウントングポート	1813
RADIUS シークレット	secret
RADIUS クライアント IP 制限	なし
証明書取得サイト	
Soliton Key Manager 用ホスト名	keymgr01.soliton-ods.jp
iOS用 URL	https://keymgr01.soliton-ods.jp
取得用ポート(各 OS 共通)	80/443/5467(TCP)
取得用 ID/PW(各 OS 共通)	サービスポータル>各種資料より入手
ID 毎の証明書発行枚数	4
<p>■サポート窓口名 株式会社ソリトンシステムズ クラウドサービスサポート</p> <p>■受付フォーム URL https://www.soliton.co.jp/support/contact/form_cloud.php サポート ID は、お問い合わせをご利用いただく際に必要となります。</p> <p>■営業時間 9:00~17:30(土・日・祝祭日、12/29~1/4 は除く)</p>	
項目	値
RADIUS サーバー(メイン)	192.168.1.2
認証用ポート	1812
アカウントングポート	1813
RADIUS シークレット	secret

3. Xirrus XD2-240 の設定

Xirrus XD2-240 は、AC アダプタの PoE 対応スイッチにケーブルで接続すると起動します。
Xirrus XD2-240 の XMS-Cloud による設定を記載します。

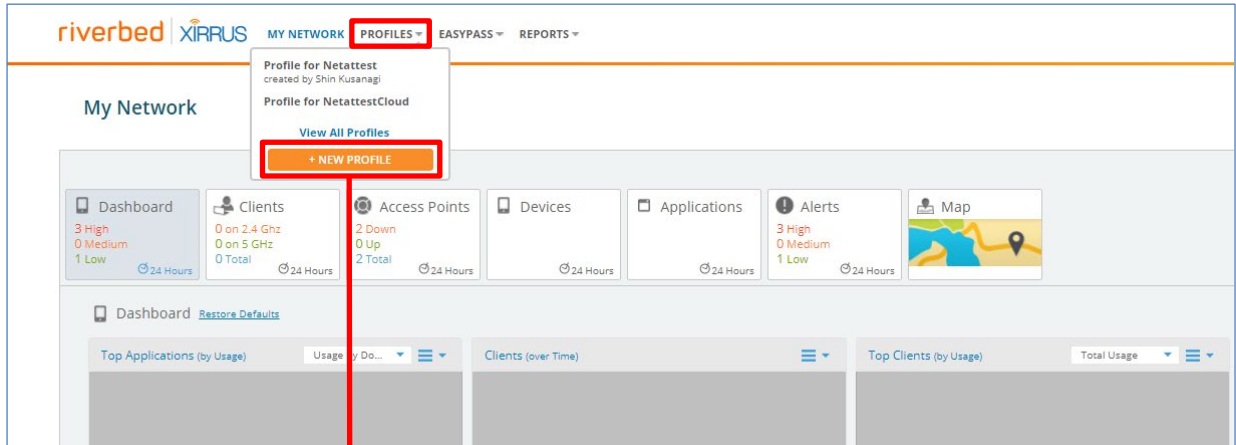
デフォルトでは DHCP で IP アドレスが取得されるようになっているため、別途設置された DHCP サーバーから払い出された IP アドレスに対して、Firefox でアクセスします。Xirrus が DHCP で受け取った IP アドレスは、XMS-Cloud か DHCP サーバー側で確認する必要があります。

セットアップは下記の流れで行います。

1. プロファイルの作成
2. 無線の設定
3. External RADIUS サーバーの設定

3-1 プロファイルの作成

始めにプロファイルを作成します。トップページより[PROFILES]-[+ NEW PROFILE]を選択し、設定します。プロファイルの Locale の Country、Time Zone は日本の物を選択してください。



The 'New Profile' dialog box is shown. The 'Profile Name *:' field contains 'EPS Cloud'. The 'Description:' field is empty. The 'CREATE NEW PROFILE' button is highlighted with a red box. There are 'Cancel' and 'Show Advanced' options as well.

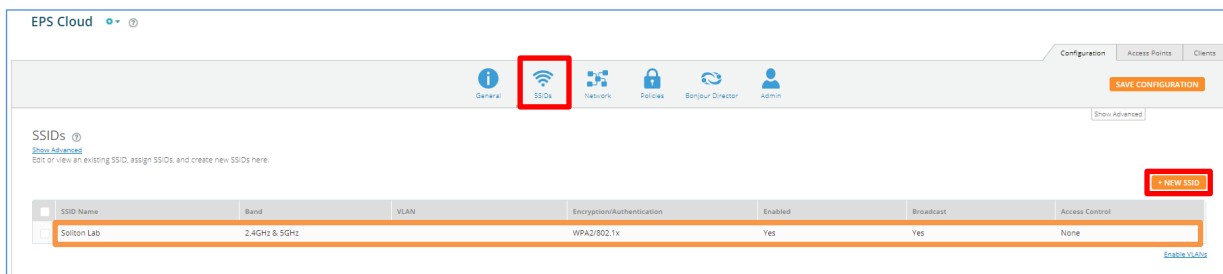
項目	値
Profile Name	EPS Cloud(任意)

The 'EPS Cloud' configuration page is shown. The 'General' tab is active. The 'Profile Name' is 'EPS Cloud'. The 'Locale' section has 'Country' set to 'Japan' and 'Time Zone' set to '(GMT + 09:00) Osaka, Sapporo, Tok...'. The 'SAVE CONFIGURATION' button is visible.

項目	値
Locale	
- Country	Japan
- Time Zone	(GMT + 09:00) Osaka, Sapporo, Tokyo

3-2 無線の設定

[SSIDs]タブに移動し、[+NEW SSID]より SSID を追加します。



項目	値
SSID Name	SolitonLab(任意)
Band	2.4GHz & 5GHz
Encryption/Authentication	WPA2/802.1x
Enabled	Yes
Broadcast	Yes
Access Control	None

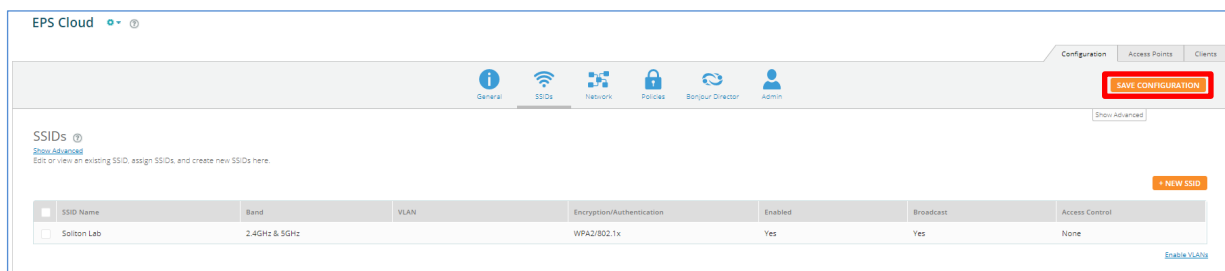
3-3 External RADIUS サーバーの設定

追加した SSID に暗号化と認証の設定を行います。

The image shows a sequence of three screenshots from the Xirrus XD2-240 configuration interface, illustrating the steps to configure encryption and authentication for an SSID.

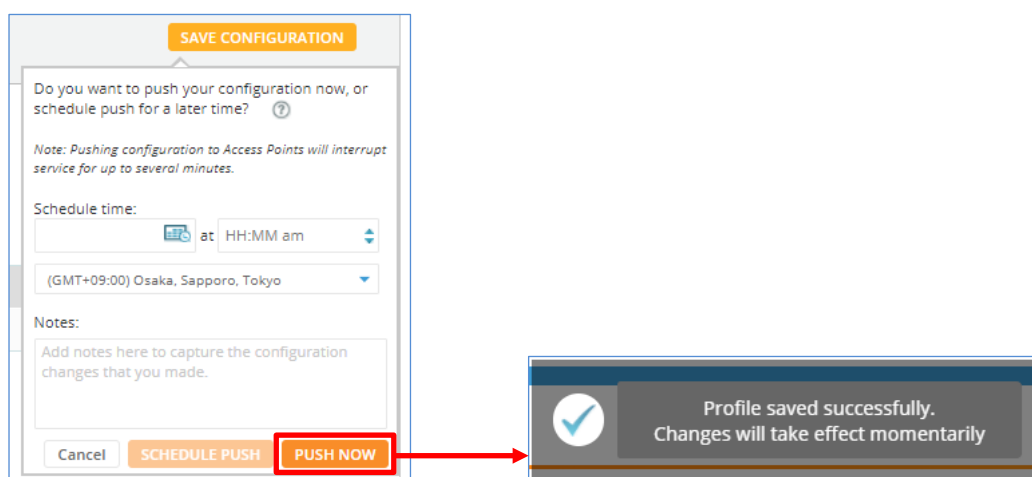
- Top Screenshot:** The main configuration page for the SSID 'Soliton Lab'. The 'Encryption/Authentication' dropdown menu is highlighted with a red box, and a red arrow points to the 'Configure' button.
- Middle Screenshot:** The 'Encryption & Authentication' dialog box, 'Encryption' tab. The question 'What encryption type would you like to use?' is shown. The 'AES (recommended stronger than TKIP)' option is selected and highlighted with a red box.
- Right Screenshot:** The 'Encryption & Authentication' dialog box, 'Authentication' tab. The question 'Which authentication method would you like to use?' is shown. The 'EAP' option is selected and highlighted with a red box. Below this, the 'Configuration External RADIUS Server' section is highlighted with a red box, showing fields for Primary Host/IP (192.168.1.2), Port (1812), Shared Secret (secret), and Confirm Shared Secret (secret).
- Bottom Screenshot:** A sub-dialog box for 'Accounting' settings. The 'Accounting' checkbox is checked and highlighted with a red box. Below it, the 'Remove Alternate Accounting Server' section is highlighted with a red box, showing fields for Primary Host/IP (192.168.1.2), Port (1813), Shared Secret (secret), and Confirm Shared Secret (secret).

項目	値
What encryption type would you like to use?	AES (recommended stronger than TKIP)
Which authentication method would you like to use?	EAP
Configuration External RADIUS Server	
- Primary Host/IP	192.168.1.2
- Port	1812
- Shared Secret/Confirm Shared Secret	secret
- Accounting	Yes
- Primary Host/IP	192.168.1.2
- Port	1813
- Shared Secret/Confirm Shared Secret	secret



以上でクラウドでの Xirrus XD2-240 の設定は完了です。

「SAVE CONFIGURATION」を押下し設定を保存してください。



4. EAP-TLS 認証のクライアント設定

本書では、各 OS への証明書インポート手順は記載していません。証明書のインポート手順については、「NetAttest EPS Cloud_かんたんクライアント設定マニュアル」をご参照ください。

4-1 Windows 10 のサブリカント設定

Windows 標準サブリカントで TLS の設定を行います。Xirrus XD2-240 で設定した SSID の [ワイヤレスネットワークのプロパティ]を開き、[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
詳細設定	
- 認証モードを指定する	ユーザー認証
スマートカードまたはその他の証明書のプロパティ	
- 信頼されたルート証明機関	クライアント証明書インストール時に インストールした CA 証明書

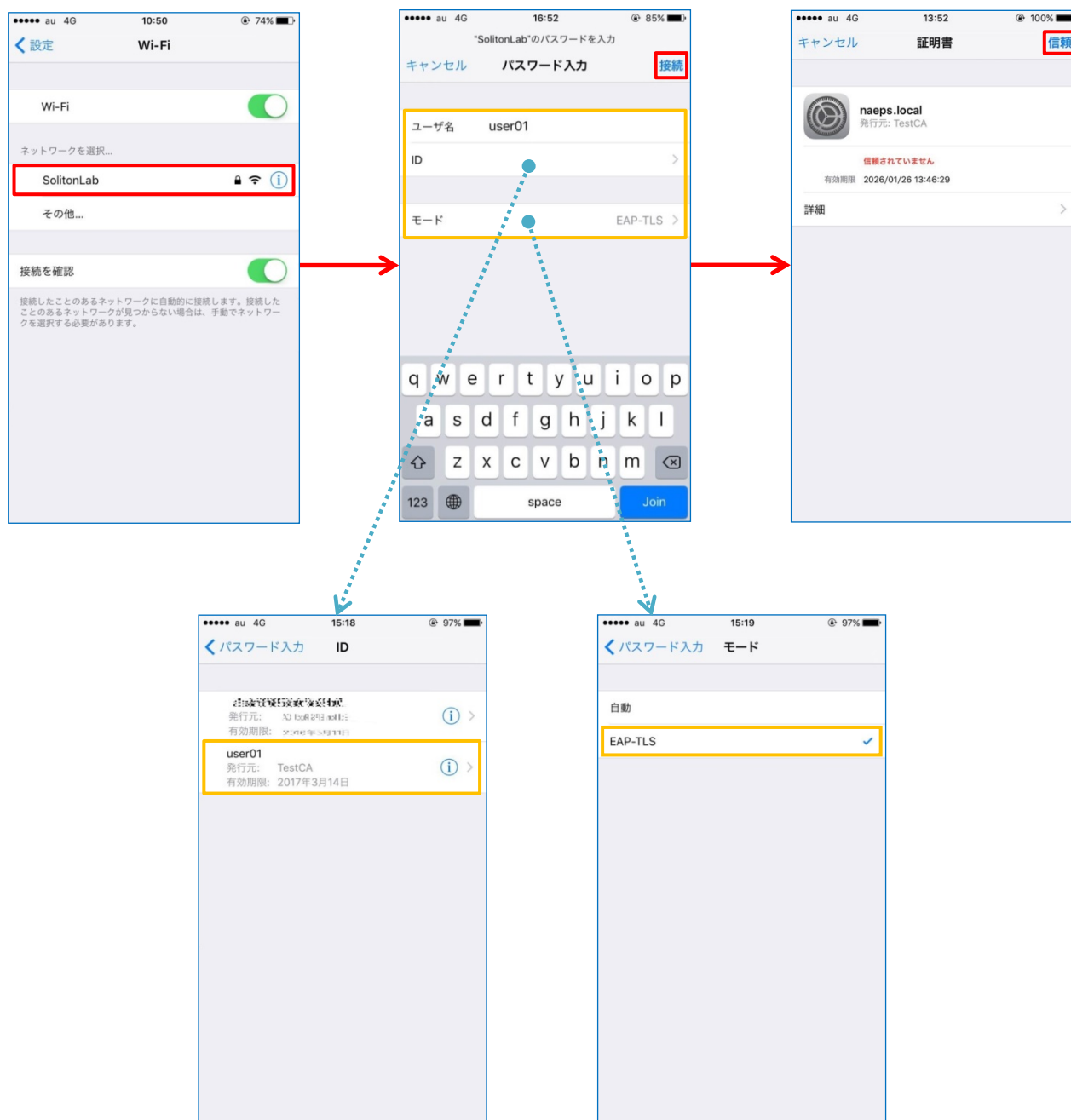
項目	値
詳細設定	
- 認証モードを指定する	ユーザー認証
スマートカードまたはその他の証明書のプロパティ	
- 信頼されたルート証明機関	クライアント証明書インストール時に インストールした CA 証明書

4-2 iOS のサブリカント設定

Xirrus XD2-240 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。

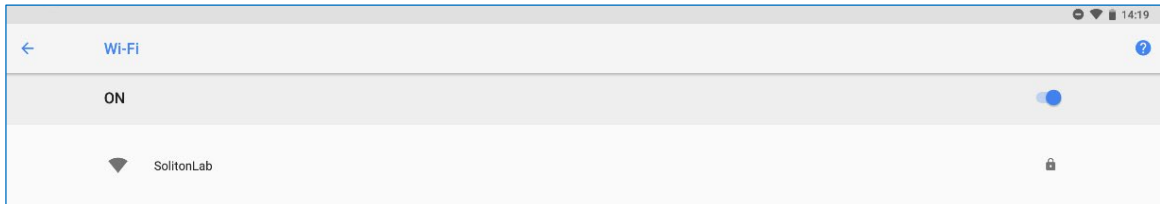
※初回接続時は「信頼されていません」と警告が出るので、「信頼」を選択し、接続します。



4-3 Android のサブリカント設定

Xirrus XD2-240 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」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。



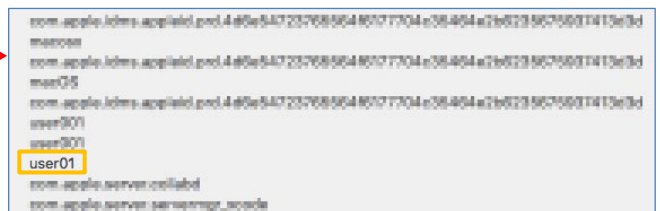
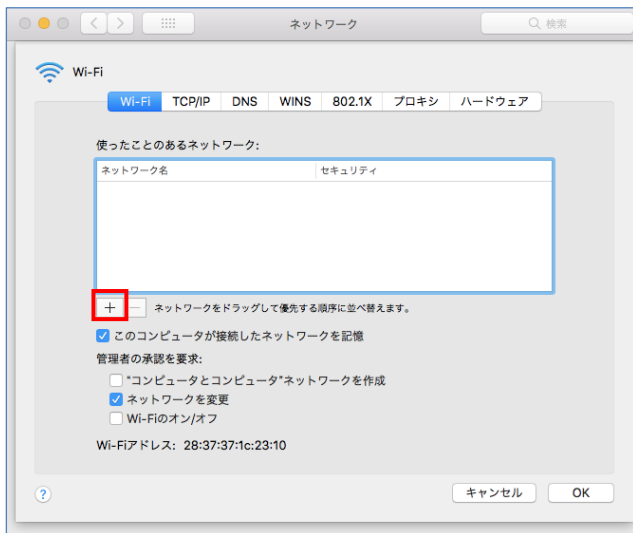
項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

4-4 MacOS のサブリカント設定

MacOS 標準サブリカントで TLS の設定を行います。

["ネットワーク"環境設定を開く...]-[詳細]で表示される画面にてネットワークの追加を行います。

ネットワーク名には Xirrus XD2-240 で設定した SSID を設定します。「ID」「ユーザ名」には証明書を発行したユーザーのユーザーID を設定します。



項目	値
ネットワーク名	SolitonLab
セキュリティ	WPA/WPA2 エンタープライズ
モード	EAP-TLS
ID	user01
ユーザ名	user01

5. 認証結果の確認手順

5-1 NetAttest EPS Cloud の RADIUS 認証ログ確認手順

EPS Cloud ログ閲覧ページにログオンすると、認証ログを確認することができます。
ポータルページの下記のアイコンよりログ閲覧ページにアクセスしてください。
ポータルページのアクセス先 URL は、アカウント通知書に記載されています。



NetAttest EPS Cloud

ログ絞り込み条件

検索日時: 2018-04-05 00:00 - 2018-04-05 23:59
本日を含まない過去 7 日間のログを検索することが可能です。初期状態では本日のログが表示されます。

ログ種別フィルタ: 認証成功 証明書取得 認証失敗(パスワード間違い) 認証失敗(無効な証明書) 認証失敗(シークレットキー不一致)

ユーザーIDフィルタ: user-name @e105004 入力欄を増やす

EPSフィルタ: IP address

検索 検索結果ダウンロード

検索結果 1 - 6件 (全6件)

ページ選択 1ページ目 / 全 1ページ

1	Apr 5 11:01:25	192.168.113.135	radiusd[21665]: notice	2018/04/05 11:01:25	Login OK: [tuser001@e105004] (from client 10_MAIN2 port 1812)
2	Apr 5 11:02:01	192.168.113.135	radiusd[21665]: notice	2018/04/05 11:02:01	Login OK: [tuser001@e105004] (from client NAT1_160_1 port 1812)
3	Apr 5 11:26:22	192.168.113.135	radiusd[21665]: notice	2018/04/05 11:26:22	Login OK: [tuser100@e105004] (from client 10_MAIN port 1 cli 60-67-20-C6-3F-54)
4	Apr 5 11:29:48	10.34.0.2	radiusd[30761]: notice	2018/04/05 11:29:48	Login OK: [tuser100@e105004] (from client test_ap port 1 cli 60-67-20-C6-3F-54)
5	Apr 5 11:32:01	10.34.0.2	radiusd[30761]: notice	2018/04/05 11:32:01	Login OK: [tuser100@e105004] (from client test_ap port 1 cli 60-67-20-C6-3F-54)
6	Apr 5 11:40:30	192.168.113.135	radiusd[21665]: notice	2018/04/05 11:40:30	Login OK: [tuser100@e105004] (from client 10_MAIN2 port 1 cli 60-67-20-C6-3F-54)

ページ選択 1ページ目 / 全 1ページ

5-2 Xirrus XD2-240 の接続端末確認手順

プロフィール設定画面の[Clients]タブにて、接続している端末の一覧を確認可能です。

EPS Cloud

Configuration Access Points **Clients**

Clients on EPS Cloud
Manage the clients connected to your profile.

Show: Online 2.4 GHz & 5 GHz

+

Client Hostname	Last Connected	Device Class	Online	Client IP Addr...	Status	Usage (Upload)	User Name
No results found							

6. 動作確認結果

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 Cloud	Login OK: [000001@e999001] (from client XirrusAP port 1 cli 80-A5-89-53-B4-0F)																
Xirrus XD2-240	<table border="1"><thead><tr><th>Client Hostname</th><th>Last Connected</th><th>Device Class</th><th>Online</th><th>Client IP Addr...</th><th>Status</th><th>Usage (Upload)</th><th>User Name</th></tr></thead><tbody><tr><td>80:a5:89:53:b4:0f</td><td>8/2/2018 3:27 pm</td><td>Notebook</td><td>Online</td><td>192.168.1.15</td><td>Allowed</td><td></td><td>000001@e999001</td></tr></tbody></table>	Client Hostname	Last Connected	Device Class	Online	Client IP Addr...	Status	Usage (Upload)	User Name	80:a5:89:53:b4:0f	8/2/2018 3:27 pm	Notebook	Online	192.168.1.15	Allowed		000001@e999001
Client Hostname	Last Connected	Device Class	Online	Client IP Addr...	Status	Usage (Upload)	User Name										
80:a5:89:53:b4:0f	8/2/2018 3:27 pm	Notebook	Online	192.168.1.15	Allowed		000001@e999001										

