



【連携機器】Cisco Meraki MR18 【Case】IEEE802.1X EAP-TLS/EAP-PEAP(MS-CHAP V2)

Rev3.0

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、Cisco Meraki 社製無線アクセスポイント MR18 の IEEE802.1X EAP-TLS/EAP-PEAP(MS-CHAP V2)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
(پ	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、
<u>.</u>	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、NetAttest D3 及び MR18 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。

<mark>S≎liton</mark> 目次

1 塂式	
Ⅰ. 作用 戊	
1-1 構成図	
1-1-1 機器	
1-1-2 認証方	5式 7
1-1-3 ネット	>ワーク設定7
2. NetAttest EPS	の設定
2-1 初期設定ウ	ィザードの実行 8
2-2 システム初	期設定ウィザードの実行9
2-3 サービス初	期設定ウィザードの実行10
2-4 ユーザーの	登録11
2-5 クライアン	ト証明書の発行 12
3. NetAttest D3 (の設定
3-1 スコープの	 設定
3-2 IP アドレス	の静的割り当て15
3-3 DHCP サー	バーの起動 17
4 MR18の設定	10
4-1 RADIUS 認	証設定
4-1 RADIUS 認 5. EAP-TLS 認証	証設定18 証設定
4-1 RADIUS 認 5. EAP-TLS 認証 5-1 Windows 8	証設定
4-1 RADIUS 認 5. EAP-TLS 認証 5-1 Windows 8 5-1-1 クラィ	証設定
4-1 RADIUS 認 5. EAP-TLS 認証 5-1 Windows 8 5-1-1 クラィ 5-1-2 サプリ	証設定
4-1 RADIUS 認 5. EAP-TLS 認証 5-1 Windows 8 5-1-1 クラィ 5-1-2 サプリ 5-2 iOS(iPhone	証設定
4-1 RADIUS 認 5. EAP-TLS 認証 5-1 Windows 8 5-1-1 クラィ 5-1-2 サプリ 5-2 iOS(iPhone 5-2-1 クラィ	証設定
4-1 RADIUS 認 5. EAP-TLS 認証 5-1 Windows 8 5-1-1 クライ 5-1-2 サプリ 5-2 iOS(iPhone 5-2-1 クライ 5-2-2 サプリ	 証設定
4-1 RADIUS 認 5. EAP-TLS 認証 5-1 Windows 8 5-1-1 クライ 5-1-2 サプリ 5-2 iOS(iPhone 5-2-1 クライ 5-2-2 サプリ 5-3 Android(Go	 証設定
4-1 RADIUS 認 5. EAP-TLS 認証 5-1 Windows 8 5-1-1 クライ 5-1-2 サプリ 5-2 iOS(iPhone 5-2-1 クライ 5-2-2 サプリ 5-3 Android(Go 5-3-1 クライ	 証設定
4-1 RADIUS 認 5. EAP-TLS 認証 5-1 Windows 8 5-1-1 クライ 5-1-2 サプレ 5-2 iOS(iPhone 5-2-1 クライ 5-2-2 サプレ 5-3 Android(Go 5-3-1 クライ 5-3-2 サプレ	証設定 18 Eでのクライアント設定 20 S.1 での EAP-TLS 認証 20 アント証明書のインポート 20 リカント設定 22 e 6)での EAP-TLS 認証 23 アント証明書のインポート 23 アント証明書のインポート 23 リカント設定 24 pogle Nexus 7)での EAP-TLS 認証 25 アント証明書のインポート 25 リカント設定 25 リカント設定 25 リカント設定 26
4-1 RADIUS 認 5. EAP-TLS 認証 5-1 Windows 8 5-1-1 クラィ 5-2 iOS(iPhone 5-2-1 クラィ 5-2 tOS(iPhone 5-2-2 サプリ 5-3 Android(Go 5-3-1 クラィ 5-3-2 サプリ 6. EAP-PEAP 認	証設定 18 Eでのクライアント設定 20 S.1 での EAP-TLS 認証 20 アント証明書のインポート 20 リカント設定 22 e 6)での EAP-TLS 認証 23 アント証明書のインポート 23 アント証明書のインポート 23 アント証明書のインポート 23 リカント設定 24 pogle Nexus 7)での EAP-TLS 認証 25 アント証明書のインポート 25 リカント設定 26 シント設定 26 アント証明書のインポート 25 アント証明書のインポート 25 アント証明書のインポート 25 アント設定 26 副市でのクライアント設定 27
4-1 RADIUS 認 5. EAP-TLS 認証 5-1 Windows 8 5-1-1 クライ 5-1-2 サプリ 5-2 iOS(iPhone 5-2-1 クライ 5-2-1 クライ 5-2-2 サプリ 5-3 Android(Go 5-3-1 クライ 5-3-2 サプリ 6. EAP-PEAP 認 6-1 Windows 8	証設定 18 ごのクライアント設定 20 3.1 での EAP-TLS 認証 20 (アント証明書のインポート



	6-3 Android(Google Nexus 7)のサプリカント設定	29
7.	動作確認結果	.30
	7-1 EAP-TLS 認証	30
	7-2 EAP-PEAP(MS-CHAP V2)認証	30

S≎liton 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



Seliton

1-1-1 機器

製品名	メーカー	役割	バージョン
NetAttest EPS ST-04	Soliton Systems	RADIUS/CA サーバー	4.8.4
MR18	Cisco Meraki	RADIUS クライアント (無線アクセスポイント)	_
Surface	Microsoft	802.1X クライアント (Client PC)	Windows 8.1 64bit Windows 標準サプリカント
iPhone 6	Apple	802.1X クライアント (Client SmartPhone)	9.2.1
Google Nexus 7	ASUS	802.1X クライアント (Client Tablet)	5.1
NetAttest D3 SX-04	Soliton Systems	DHCP/DNS サーバー	4.2.2

1-1-2 認証方式

IEEE802.1X EAP-TLS/EAP-PEAP(MS-CHAP V2)

1-1-3 ネットワーク設定

製品名	IP アドレス	RADIUS port (Authentication)	RADIUS Secret (Key)
NetAttest EPS ST-04	192.168.1.2/24		secret
MR18	192.168.1.1/24	UDF 1812	secret
Client PC	DHCP		
Client SmartPhone	DHCP	-	-
Client Tablet	DHCP	-	-

<u>Seliton</u>

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

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。

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

<u>Seliton</u>

2. NetAttest EPS の設定

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

CA種別選択		
CAMPEER	μ−トCA ¥	
CANCER		
● 内部で新しい鍵を生成する		
公開能方式	RSA 🗸	
親長	2048 🗸	
○ 外部HSMデバイスの鍵を修	用する	
要求の署名		
要求署名アルゴリズム	SHA256 V	
CA情報		
	TestCA	
	日本 🗸	
都通府県名	Tokyo	
市区町村名	Shinjuku	
会社名(組織名)	Soliton Systems	
部署名		
CA署名設定		





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

Seliton

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。

・ いっちょはなて ・ ワ・ワ・マ・● ● 飯田谷 ● ワクフ ・ シ・フちょはなて ・ シ・フィーを ・ シ・フィーを ・ ワ・ワ・マ・● ・ ● ・ ● ・ ● ・ ● ・ ● ・ ● ・ ● ・ ● ・ ●
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
 ○ 2.75.468 ○ 2.75.468 ○ 2.75.468 ○ 1.0009 - バー ○ 1.0009 - ○ 1.0009 - ○
 ・ は明時間 ・ は日サワーパー、 ・ しはサワーパー、 ・ しはサワーパー、 ・ しはサローパー、 ・ コーブーI ・ マンズー・ ・ マンボー・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
• BPDP-F-F- • DDPP-F-F- • AA • 2-5-5- • AA • 4 • 4 • 4 • 4 • 4 • 4 • 4 • 4 • 4 • 4
• КАЦКУ-Л-К- • - 2-7-К- • 2-7-К-
1 1
エクスポー ・ インボー・ ・ インボー・ ・ インボー・ ・ コーヴーバスワードポリシー・ ・ デフォ)パムユーザープロファイル レ test user レ user 01 ・ - ザーB ・ レ user 01 ・ - リー・ - ド ・ レ user 01 ・ - リー・ - ド ・ レ user 01 ・ - パスワード ・ レ user 01 ・ - マーリー ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
 * インボー * ニーザーバスワードボリシー * デフォルトユーザーブロファイル
■ ユーザーガロファイル ■ ユーザープロファイル ■ ゴーザーボー 加 user01 コーザー「 加 user01 パスワード password
項目 値 姓 user01 ユーザーID user01 パスワード password
項目 値 姓 user01 ユーザーID user01 パスワード password
項目 値 姓 user01 ユーザーID user01 パスワード user01 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
項目 値 姓 User01 ユーザーID user01 パスワード password
項目 値 姓 user01 ユーザーID user01 パスワード
項目 値 姓 user01 ユーザーID user01 パスワード
項目 値 姓 user01 ユーザーID user01 パスワード ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
項目 値 姓 user01 ユーザーID user01 パスワード password
姓 user01 ユーザーID user01 パスワード password
ユーザーID user01 パスワード password
ユーザーID user01 パスワード password
パスワード password
(トップページ) 口グオフ
■ naeps.local ユーザー-覧
■システム設定 ■システム管理 フーザー ● 一部 ● 完全 グルーナ ▼ ユーザーまで 検索
■ 証明機関 詳細オブションの設定
■ RADIUSサーバー ユーザー削除時の証明書生効オプション
■ ユーザー ■ 名前 ユーザーID 最終認証成功 証明書 タスク
■ エクスポート test user test 第行 変更 創除

2-5 クライアント証明書の発行

Scliton

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)

Net Attest EPS	保存されていない設定またはデ	ータがあります!		ログオンダ
	<u> </u>		(1)トップページ) 🖻	設定保存 🛛 🔁 🗆
■ naeps.local ■ システム設定	▲ ユーザー→覧			
■ システム管理	ユーザー ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	完全 グループ 💙	ユーザーまで 検索	
■ DHCPサーバー	<u>詳細オラションの設定</u> エクスポート			
■ LDAPサーバー ■ RADILSサーバー			つ ― ++* ― お川区合口	
	□ 名前	<u>ユーザーID</u>	最終認証成功 証明書	すい証明者天Xルリン タスク
■ <u>ユーザーー宜</u> ■ エクスポート	test user	test	近日日日	変更 削
■ インボート ■ ユーザーバスワードポリシー	user01	<u>user01</u>	۲ <mark>۴</mark> ۲	変更 削
		编集対象: user01	¥	
		基本情報		
		姓	user01	_
		+5 E-Mail		_
		≣∓¥⊞fā¥k		\sim
		読 正 情報 スーザーm	userf1	
		有効期限		
		● 日数 365 ● 日付 2016 ¥	日 年 <mark>7 ~ 月 9 ~ 日 23 ~</mark> 時 59	<mark>></mark> 分 <mark>59 ></mark> 秒まで
	值	証明書ファイルオブション パスワード		
		バスワード(確認)		
信 有勿期限	365	※バスワードが空間の場合に	は、ユーザーのパスワードを使用します。	
#12 ファイルに証明機関の・・	チェック有	☑ PKCS#12ファイルに語	明機関の証明書を含める	
				発行 キャ
	📥 ユーザー論	明書のダウンロード		
				Key D
	ユーザー証明書ダウ	ンロードの準備ができました。対	象でノアイルに体行しててい。	377
	ユーザー証明書ダウ	ンロードの準備ができました。対		

Seliton®

3. NetAttest D3 の設定

MR18 は、デフォルトでは DHCP から 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 MR18 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。

NetAttest D3				
 	ポスト名(d3.solitonsso.com) DNS り DHCP り			
✔ システム設定				
✔ システム管理				
✔ ドメインネームサービス	<u>ネットワーク</u> IP使用率(%)			
▼ DHCPサービス	表示するデーターはありません			
サーバー状態				
サーバー設定	追加 CSVダウンロード CSVアップロード			
リース情報				
登録クライアント				
肝的割り目で				
認証用NetAttest EPS設定				
ユーザー定義オプション				

NetAttest	D3			
 	ホスト名 d3.solitonsso.com DNS 1	DHCP 1		
 ✓ システム設定 ✓ システム管理 	DHCP - スコープの	D追加		
✔ ドメインネームサービス	スコープの設定			
✔ DHCPサービス サーバー状態 サーバー設定	ネットワーク サブネットマスク	92.168.1.0 255.255.255.0		
リース情報 スコープ	ルーター	192.168.1.254	項目	値
登録クライアント 静的割り当て	ドメイン名 ドメインネームサーバー	solitontest.com	スコープの設定	
び設まれLaRAE 認証用NetAttest EPS設定 ユーザー定義オプション	レンジの設定		- ネットワーク	192.168.1.0
ベンダー固有オプション	レンジ開始アドレス	192.168.1.1	- サブネットマスク	255.255.255.0
	レンジ終了アドレス	192.168.1.140	- ルーター	192.168.1.254
	時外レンジ網路アトレス 除外レンジ終了アドレス	192.168.1.99	- ドメイン名	solitontest.com
	OK キャンセル		- ドメインネームサーバー	192.168.1.3
Copyright @ 2007-2016, Soliton Systems	K.K., All rights reserved.		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

MR18の MAC アドレスに IP アドレスを静的に割当てるため、事前に MR18の MAC アドレスを 確認します。MR18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。 MR18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。



00:18:0A:6F:29:84

NetAttest	D3		
Image: Image: Image	ホスト名 d3.solitonsso.com DNS 🦸 DH	CP 🔰	
 > システム設定 > システム管理 > ドメインネームサービス > DHCPサービス サーバー設定 リース情報 スコーブ 登録クライアント 静約割り当て 八風化設定 送送用NetAttest EPS設定 	ACTA USUMUSSION UNS 7 UN DHCP - 静的割り当て <u> </u>	ビレス 最終リース日散 ド	
NetAttest	D 3		
 (a) (b) 	ホスト名 d3.solitonsso.com DNS 🕴 DH	ср 🕴	
 ✓ システム設定 ✓ システム管理 	DHCP - 静的割り当て -	- 追加/修正	
 ドメインネームサービス DHCPサービス サーバー状態 サーバー設定 リース信報 	ホスト名 ビ moo ロアドレス ビ 192 MACアドレス ビ 00: OK キャンセル	0180o6f2984	
スコープ 登録クライアント		項目	值
静的割り当て			
冗長化設定 認証用NetAttest EPS設定		ホスト名	M00180a6f2984 (任
ユーザー定義オプション		TP アドレス	192.168.1.1

¥				
NetAttest D3				
 	ホスト名 d3.solitonsso.com DNS チ DHCP チ			
✔ システム設定				
◆ システム管理	DHCP - 静旳割り当 C			
▼ ドメインネームサービス	ホスト名 IPアドレス MACアドレス 最終リース日時			
✓ DHCPサービス	m00180a6f2984 192.168.1.1 00:18:0A:6F:29:84 2016-03-29 15:41:11			
サーバー状態	● 全選択			
サーバー設定	1			
リース情報	表示する件数 25 ▼ (全部:1ページ.1件)			
スコープ				
登録クライアント				
静的割り当て	フィルタ			
冗長化設定				
認証用NetAttest EPS設定				
ユーザー定義オプション	コーストMACアトレスの確認			

MAC アドレス



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。

NetAttest D3					
 (a) (b) (b) (c) (c)<!--</th--><th>ホスト名 d3.solitonsso.com</th><th></th><th></th><th></th><th></th>	ホスト名 d3.solitonsso.com				
 ◆ システム設定 ◆ システム管理 	DHCP - שי	ーバー状態			
✓ ドメインネームサービス	動作状態				
✓ DHCPサービス	サーバー稼動状態	動作中			
サーバー状態 サーバー設定	冗長化状態	冗長化しない			
リース情報 スコープ	IP使用率(%)				
登録クライアント	096		C		
静的割り当て	0741 max				
兀長化設定	起動停止初	期化 リース情報全消去 M/	ACアドレス使用履歴全消去	状態の更新	
認証用NetAttest EPS設定					



4. MR18 の設定

MR18の設定はクラウド上の管理ページ[http://dashboard.meraki.com]から行います。

4-1 RADIUS 認証設定

[Network]に[(該当するネットワーク)]を選択し、[Wireless]-[Access control]より設定する SSID を選択し、RADIUS 認証の設定を行います。ここでは、

- 認証方式
- RADIUS 認証ポート
- アカウンティングポート
- クライアント IP の割当方法

を設定します。

				eqs@seq@.netiloe.teil.co.jp	1 new featu	re customer number: 0512-7007	my profile sign out
cisco Meraki	Network: Demo Template	٣				Q Search dashboard	
Network-wide	This network is acting as	the configuration template for <u>1 n</u>	etwork				
Wireless	New in Dashboard: ICMP	Laver 3 Firewall Rules Read m	ore				X
Organization							
Help	Access control	T					
	Network access						
	Association requirements	 Open (no encryption) Any user can associate 					
		Pre-shared key with WPA2 Users must enter a passph	▼ Irase to assoc	iate			
		MAC-based access contro RADIUS server is queried	l (no encryptic at association	n) time			
		WPA2-Enterprise with my User credentials are valida	RADIUS server ted with 802.1	▼ X at association time			
	WPA encryption mode	WPA1 and WPA2 V					
	802.11r 🕲	Disabled V					
	Splash page None (direct access) Users can access the network as soon as they associate						
		Click-through Users must view and ackn	owledge your	splash page before being allowed on the network			
	Sign-on with <u>Ideraki authentication</u> v Users must enter a username and password before being allowed on the network						
	Sign-on with SMS Authentication Users enter a mobile phone number and receive an authorization code via SMS. After a trial period of 25 texts, you will need to connect with your Twilio account on the <u>Network-wide settings</u> page.						
		Billing (paid access) Users choose from various	pay-for-acce	ss options, or an optional free tier			
		 Systems Manager Sentry Only devices with Systems 	enroliment 0 Manager ca	n access this network			
	RADIUS servers	# Host	Port	Secret	Actions		
		1 192.168.1.2 Add a server	1812		$\oplus X$	Test	
	RADIUS testing	RADIUS testing disabled V					
	RADIUS accounting	RADIUS accounting is enabled v					
	RADIUS accounting	# Host	Port	Secret	Actions		
	Servers	1 192.168.1.2	1813		÷Χ		
	RADIUS attribute specifying group policy name	Filter-Id V					
	Assign group policies by device type	Disabled: do not assign group polici	es automatic ally	¥			



Addressing and traffic				
Client IP assignment	I NAT mode: Use Meraki DHCP Clients receive IP addresses in an isolated 10.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the SSID firewall settings permit.			
	Bridge mode: Make clients part of the LAN Meraki devices operate transparently (no NAT or DHCP). Clients receive DHCP leases from the LAN or use static IPs. Use this for shared printers, file sharing, and wireless cameras.			
	Layer 3 roaming Clients receive DHCP leases from the LAN or use static IPs as in bridge mode. If they roam between APs their traffic will be forwarded to an AP on the same subnet they originally joined, so they will keep the same IP address.			
	Cleaver 3 roaming with a concentrator Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs.			
	VPN: tunnel data to a concentrator Meraki devices send traffic over a secure tunnel to an MX or VM concentrator.			
	Note: VPN and Layer 3 roaming with concentrator require an MX or VM concentrator. To use them, add an MX, or create a concentrator.			
VLAN tagging ③ Bridge mode and layer 3 roaming only	[Don't use VLAN tagging *]			
RADIUS override	Ignore VLAN attribute in RADIUS responses 🔻			
Content filtering	Don't filter content			
Bonjour forwarding Bridge mode and layer 3 roaming only	Disable Bonjour Forwarding 💌			
Wireless options				
Band selection	Dual band operation (2.4 GHz and 5 GHz)			
	5 GHz band only 5 GHz has more capacity and less interference than 2.4 GHz, but legacy clients are not capable of using it.			
	Dual band operation with Band Steering Band Steering detects clients capable of 5 GHz operation and steers them to that frequency, while leaving 2.4 GHz available for legacy clients.			
Minimum bitrate (Mbps)	Lower Density Higher Density			
9	1 2 5.58 Q 1112 18 24 38 48 54			
	Maximum device compatibility			
	Save Changes or cancel (Piesse allow 1-2 minutes for changes to take effect.)			
© 2016 Cisco Systems, Inc.	privacy - terms Lastlogin: <u>18 days ago</u> from your current IP address. [wish this page would] make a wish Current session started: <u>5 minutes ago</u>			

項目	値	
Association requirements	WPA2-Enterprise with my RADIUS server	
RADIUS server	192.168.1.2:1812 , secret	
RADIUS accounting server	192.168.1.2:1813 , secret	
Client IP assignment	Bridge mode: Make clients part of the VLAN	



5. EAP-TLS 認証でのクライアント設定

5. EAP-TLS 認証でのクライアント設定

5-1 Windows 8.1 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。

user01_02.p12

証明書のインボート ウィザードの開始
このウィザードでは、証明書、証明書信頼リスト、および証明書夫効リストをディスクから証明書ストアにコピー します。
証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護されたタックコーク接続を提供するための情報を含んています。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。
保存場所 ⑩ 現在のユーザー(C) ○ ローカル コンピューター(L)
統行するには、【次へ】 をグリックしてください。
次へ(N) キャンセル
 ✓ ジョン・ション・ション・ション・ション・ション・ション・ション・ション・ション・シ
インボートする証明書ファイル インボートするファイルを指定してください。
ファイル名(F):
C:#Users#Soliton#Downloads#user01_02.p12 参照(R)
注意: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます: Personal Information Exchange- PKCS #12 (.PFXP12)
Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B)
Microsoft シリアルビされに証明器ストア (.551)
次へ(N) キャンセル



5. EAP-TLS 認証でのクライアント設定

【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。

SolitonLab ワイヤレス ネットワークのプロパティ		
接続 セキュリティ		
セキュリティの種類(E): WPA2 - エンタープライズ >		
暗号化の種類(N): AES 💙		
ネットワークの認証方法の選択(O):		
Microsoft:スマートカードまたはその他の証明書 ・ ログオンするたびに、この独統用の真格情報を使用する(R)	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
詳細設定(D) ●	ネットワークの認証	E・・・ Microsoft: スマートカード・・・
		· · ·
0V 5+-7/1		
	スマート カードまたはその	也の証明書のプロパティ ×
	接続のための認証方法: ○ 自分のスマート カードを使う(S)	2Vément ()
詳細設正	 ● このコンピューターの証明書を使う(C) □ 対体やわび印書の語はを使う(C) 	s+maxE(A)
 ✓ 認証モードを指定する(P): 	● 単純な証明書の進択を使う(注葉)(M) [打る(V)
ユーザー認証 ∨ 資格情報の保存(C)		rv2, .*¥.srv3¥.com)(0):
□ すべてのユーザーの資格情報を削除する(D)		
□このネットワークに対するシングル サインオンを有効にする(S)	信頼されたルート証明機關(R): □ Microsoft Root Certificate Auth	onty 2010
 ユーザーログオンの直前に実行する(E) ユーザーログオンの直接に実行する(E) 	☐ Microsoft Root Certificate Auth	ority 2011
最大特5時間(秒)(M): 10	thawte Primary Root CA Thawte Timestamping CA	
■ シングル サインオン中に追加のダイアログの表示を許可する(L)	UTN - DATACorp SGC	
□ このネットワークでは、コンピューターとユーザーの認証に別の仮想 LAN を使用する(V)	VeriSign Class 3 Public Primary	Certification Authority - G5
	×	証明書を表示する(E)
	□ 新しいサーバーまたは信頼された証明根	4関を承認するようユーザーに求めない(P)
	□ この接続で別のユーザー名を使う(D)	
		OK キャンセル
ОК <i>‡</i> т>тz)		

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を・・・	On
証明書を検証してサーバーの・・・	On
信頼されたルート証明機関	TestCA

<u>Seliton</u>

5-2 iOS(iPhone 6)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として、 下記の方法などがあります。

- 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

MR18 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、[ユーザー名]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[E AP-TLS]を選択します。その後、[ユーザー名]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。



Seliton

5-3 Android(Google Nexus 7)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 5.1 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 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	ок



5-3-2 サプリカント設定

MR18 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アカウントの 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 8.1 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。

SolitonLab ワイヤレス ネットワークのプロパティ		
え セキュリティ	項目	但
セキュリティの種類(E): WPA2 - エンタープライズ >	セキュリティの種類	WPA2-エンタープライズ
音号化の種類(N): AES *	暗号化の種類	AES
	ネットワークの認証・・・	Microsoft:保護された EA
Fットワークの認証方法の選択(O): Microsoft: 保護された EAP (PEAP)		
□グオンするたびに、この接続用の資格情報を使用する(R)	*******	
		れた EAP のプロバティ
	接続のための認証方法:	
詳細設定(D)	■ ■ 証明書を検証してサーバーの」	D で検証9る(V)
	□次のサーバーに接続する(例	: srv1, srv2, .*¥.srv3¥.com)(0):
	信頼されたルート証明機関(R):	
OK ±++>,/7/I.	☐ Microsoft Root Certifica ▼ TestCA	ate Authority 2011 ^
	thawte Primary Root C	A
	UTN - DATACorp SGC	CA
Ŷ	UTN-USERFirst-Object	
詳細設定	VeriSign Class 3 Public	Primary Certification Authority - G5
12.1X の設定 802.11 の設定	接続前の通知(工)・	
✓ 認証モードを指定する(P):	サーバー名またはルート証明書が	指定されなかった場合にユーザーに通知します >
ユ−ザ−認証 > 資格情報の保存(C)		
オペアのコーザーの海牧/告紹を削除する(D)	認証方法を選択する(5):	
94(COT) Oğalılaticanika 9(C)		
「このネットワークに対するシングル サインオンを有効にする(S)		する(N)
 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	□ サーバーに暗号化バインドの TL	∨ がない場合は切断する(D)
◎ ユーザー ログオンの直後に実行する(F)	□ ID フライハシーを有効にする(I)	
最大待5時間(秒)(M):		
マシングル サインオン中に追加のダイアログの表示を許可する(L)		OK キャンセル
このネットワークでは、コンピューターとユーザーの認証に別の仮想		
LAN を使用する(V)		
		EAP MSCHAPV2 070/77
	接続のための	2認証方法:
	U Wind	ows のログオン名とパスワード (およびドメインがある場 メイン) を自動的に使う(A)
	15日 一	· · · / · · · · · · · · · · · · · · · ·
0K ±+++++7+1	1512	

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



6-2 iOS(iPhone 6)のサプリカント設定

MR18 で設定した SSID を選択し、サプリカントの設定を行います。[ユーザー名]、[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
ユーザー名	user01
パスワード	password
モード	自動



6-3 Android(Google Nexus 7)のサプリカント設定

MR18 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]には、 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

Seliton

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	Mar 29 16:27:38 naeps radiusd[2498]: notice 2016/03/29 16:27:38 Login OK: [user01] (from client RadiusClient01 port 0 cli C0-33-5E-DF-2A-23)
MR18	2016/3/29 16:27, 00:18:0a:6f:29:84, SolitonLab, SolitonTestPC, 802.1X EAP success, radio: 1,
	vap: 2, client_mac: C0:33:5E:DF:2A:23""

7-2 EAP-PEAP(MS-CHAP V2)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	Mar 29 16:48:00 naeps radiusd[2498]: notice 2016/03/29 16:48:00 Login OK: [user01] (from client RadiusClient01 port 0 cli C0-33-5E-DF-2A-23 via proxy to virtual server) Mar 29 16:48:00 naeps radiusd[2498]: notice 2016/03/29 16:48:00 Login OK: [user01] (from client RadiusClient01 port 0 cli C0-33-5E-DF-2A-23)
MR18	2016/3/29 16:48, 00:18:0a:6f:29:84, SolitonLab, SolitonTestPC, 802.1X EAP success, radio: 1, vap: 2, client_mac: C0:33:5E:DF:2A:23""

<u>Seliton</u>

改訂履歴

日付	版	改訂内容
2016/04/18	1.0	初版作成
2018/06/13	2.0	誤記修正
2019/03/19	3.0	ロゴ画像更新