



【連携機器】MSM4xx シリーズ、MSM7xx シリーズ 【Case】IEEE802.1x EAP-TLS 認証、VASCO ワンタイムパスワード認証

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 CA 内蔵 RADIUS サーバーアプライアンス NetAttest EPS と HP 社製 無線アクセ スポイント、無線コントローラー MSM シリーズの IEEE802.1x EAP-TLS 環境での接続と ゲストアクセス用ワンタイムパスワード認証(PAP)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。

表記方法

表記方法	説明
ſ J	参照するドキュメントを示します。
٢J	参照する章、節、ボタンやメニュー名、強調する単語を示します。
[+-]	キーボード上のキーを表します。
[+-1]+[+	「七」11を押したがら「七」21を押すことを手します
-2]	$[-\tau^{-1}]^{(c)} \tau^{(a)} \mathcal{O}[\tau^{-2}]^{(c)} \tau^{9} \mathcal{O}(\tau^{a})$

表記方法(コマンドライン)

表記方法	説明
%, \$, >	一般ユーザーのプロンプトを表します。
#	特権ユーザーのプロンプトを表します。
[filonamo]	[] は省略可能な項目を示します。この例では、filename は省
[mename]	略してもよいことを示しています。

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 MSM4xx シリーズ、MSM7xx シリ ーズ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。

<u>Saliton</u>

1.	構成6
	1-1 構成図6
	1-2 環境7
	1-2-1 機器7
	1-2-2 認証方式
	1-2-3 ネットワーク設定7
2.	NetAttest EPSの設定8
	2-1 システム初期設定ウィザード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 RADIUS クライアントの追加12
	2-6 クライアント証明書の発行13
3.	MSM4xx シリーズの設定14
	3-1 アクセスポイントへのログイン14
	3-2 アクセスポイントの初期設定15
	3-3 IP アドレスの設定16
	3-4 コントローラーの指定17
4.	MSM7xx シリーズの設定19
	4-1 コントローラーへのログイン 19
	4-2 End User License Agreement 20
	4-3 Product Registration 20
	4-4 国コードの設定21
	4-5 ユーザーアカウントの設定 21
	4-6 Automated workflows 22
	4-7 コントローラーIP アドレスの変更23
	4-8 デフォルトゲートウェイの設定24
	4-9 アクセスポイントの接続と認識25
	4-10 VLAN の作成

4-11 RADIUS サーバーの指定	27
4-12 VSC の作成	28
4-13 AP グループの作成	29
4-14 AP 名、グループの変更	30
4-15 グループと VSC の紐付け	31
4-16 コンフィグの同期	32
5. アクセスポイントへの TLS 認証	33
5-1 iOS (iPad)	33
5-1-1 iOS へのデジタル証明書のインストール	33
5-1-2 サプリカントの設定	34
5-2 Android (Nexus7)	35
5-2-1 Android へのデジタル証明書のインストール	35
5-2-2 サプリカントの設定	36
6. アクセスポイントへのゲスト用ワンタイムパスワード認証	37
6-1 NetAttest EPS の設定変更	37
6-1 NetAttest EPS の設定変更 6-1-1 DPX ファイルのインポート	37 37
6-1 NetAttest EPS の設定変更 6-1-1 DPX ファイルのインポート 6-1-2 ユーザーとトークンの紐付け	37 37 38
 6-1 NetAttest EPS の設定変更 6-1-1 DPX ファイルのインポート 6-1-2 ユーザーとトークンの紐付け 6-2 MSM7xx シリーズの設定変更 	37 37 38 39
 6-1 NetAttest EPS の設定変更 6-1-1 DPX ファイルのインポート 6-1-2 ユーザーとトークンの紐付け 6-2 MSM7xx シリーズの設定変更 6-2-1 コントローラーIP アドレスの変更 	37 37 38 39 39
 6-1 NetAttest EPS の設定変更 6-1-1 DPX ファイルのインポート 6-1-2 ユーザーとトークンの紐付け 6-2 MSM7xx シリーズの設定変更 6-2-1 コントローラーIP アドレスの変更 6-2-2 DHCP サーバーの起動 	37 37 38 39 39 40
 6-1 NetAttest EPS の設定変更 6-1-1 DPX ファイルのインポート 6-1-2 ユーザーとトークンの紐付け 6-2 MSM7xx シリーズの設定変更 6-2-1 コントローラーIP アドレスの変更 6-2-2 DHCP サーバーの起動	37 37 38 39 39 40 41
 6-1 NetAttest EPS の設定変更 6-1-1 DPX ファイルのインポート 6-1-2 ユーザーとトークンの紐付け 6-2 MSM7xx シリーズの設定変更 6-2-1 コントローラーIP アドレスの変更 6-2-2 DHCP サーバーの起動	37 37 38 39 39 40 41 42
 6-1 NetAttest EPS の設定変更. 6-1-1 DPX ファイルのインポート	37 37 38 39 39 40 41 42 43
 6-1 NetAttest EPS の設定変更	37 37 38 39 39 40 41 42 43 44
 6-1 NetAttest EPS の設定変更	37 37 38 39 39 40 41 42 43 44 45
 6-1 NetAttest EPS の設定変更	37 37 38 39 39 40 41 42 43 44 45 46
 6-1 NetAttest EPS の設定変更	37 37 38 39 39 40 41 42 43 44 45 45 46 47
 6-1 NetAttest EPS の設定変更	37 37 38 39 39 40 41 42 43 43 44 45 45 46 47 48



1-1 構成図



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。

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 ST04	Soliton Systems	Authentication Server (認証サーバー)	Ver. 4.6.8
MSM710	HP	Authenticator (認証機器:無線 LAN コントローラー)	Ver. 6.0.2.2
MSM430	HP	Authenticator (認証機器:無線 AP)	Ver. 6.0.2.2
iPad mini	Apple	Client Tablet① (802.1x クライアント)	Ver. 7.1.2
Nexus 7	Google	Client Tablet② (802.1x クライアント)	Ver. 4.4.2

1-2-2 認証方式

IEEE802.1x EAP-TLS 認証、VASCO ワンタイムパスワード認証(PAP)

1-2-3 ネットワーク設定

IP アドレス		RADIUS port (Authentication)	RADIUS Secret (Key)
NetAttest EPS ST-04	192.168.1.2/24		secret
MSM710	192.168.1.1/24	UDP 1812	secret
MSM430	192.168.1.3/24		secret
Client Tablet① 固定		-	-
Client Tablet② 固定		-	-

2. NetAttest EPS の設定

2-1 システム初期設定ウィザード

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、インターネットエクスプロー ラーから「http://192.168.2.1:2181/」にアクセスします。

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、インターネットエクスプロー ラーから「http://192.168.2.1:2181/」にアクセスします。

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

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

Concerns of the local data	
KAR222917 後先期位 認証9477 1 TLS - 1 TLS - 1 TLS - 3 TLS - 3 TLS - 4 TLS - 4 TLS - 5 TLS	
LAP-ILS/ILSPLAP# 201	
	1024 - AS-(1-
メッセージの長さ情報	フラヴェルされた 戦物のパケットにのみ含まれる ・
EAP-TILSPEAP3 25/12	
CTC認証を有効にする	
■ ILSE999974+99938	4.例にする
EAP-FASTオプション	

CARDIN		
CARLER	a-+ca •	
CAREN		
SHEAK	RSA ·	
	2045 •	
	HILTO	
RECES		
	59431 ·	
catter		
	TestCA	
	0* -	
BORDER TO	Tseyo-lo	
MECHINE.	Shanjyuka-ku	
211/5 (0008-6)	Soltan Systems K.K.	
CATI GREE		
	39VA1 +	
1.1ADM	3670	



項目	値
EAP 認証タイプ	TLS

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
NAS/RADIUS クライアント名	MSM430
IP アドレス	192.168.1.3
シークレット	secret

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。



Seliton 2-5 RADIUS クライアントの追加

NetAttest EPS の管理画面より、無線 LAN コントローラー MSM710 の登録を行います。 「RADIUS サーバー」→「NAS/RADIUS クライアント」→「NAS/RADIUS クライアント一覧」か ら、『追加』ボタンで RADIUS クライアント登録を行います。



2-6 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_02.p12 という名前で保存)

Not Attact EDC			ログオン中: admin
NetAttestera	-		 (1) トップページ (1) ログオフ)
■ naeps.local	🔰 ユーザー覧		
 システム設定 システム管理 	ユーザー ● 一部 ● 完全 グル	,ブ ✔ 200 ユーザーまで 検索	
■ 証明機関	and the second se		ut ئۆ
■ DHCPサーバー ■ LDAPサーバー		7 ff m	ユーザー削除時の証明書失効オブション
■ RADIUSサーバー	fold test user	test	
ユーリー ユーザー 暫		usar01	
	uservi	USCIUT	9611 & C 19710
■デフォルトユーザープロファイル			
		編集対象: user01	
		基本情報	
		姓	user01
		名	
		E-Mail	
		-X40 kt #1	
		37 401 11 Mz	<u></u>
		認証情報	
		ユーザーID	user01
Copyright © 2004-2014, Soliton Systems K.K., A	All rights reserved.	有効期限	
		● 日付 2013 V 年	ョ F <mark>2 ~ 月 28 ~ 日 23 ~ 時 59 ~</mark> 分 <mark>59 ~ </mark> 秒まで
		証明書ファイルオブション	
		パスワード	
		バスワード(確認)	
		*パスワードが空間の場合に	
		☑ PKCS#12ファイルに証明	機関の証明書を含める
			発行 キャンセル
			1
	ユーザー証明書の	ダウンロード	•
		5、17、17小洋供品でおもしま 54番4	
		7 フロードの卒業がてきました。対象で	

3. MSM4xx シリーズの設定

3-1 アクセスポイントへのログイン

MSM4xx シリーズのデフォルト IP アドレスは 192.168.1.1/24 に設定されています。

Web ブラウザよりアクセスを行うと、証明書エラーの画面が表示されますが、"Continue to this website"をクリックします。

※MSM4xx シリーズのインターフェイスは DHCP Client も動作していますので、DHCP の環境下で は DHCP より IP アドレスが付与されます。

The security certificate pre The security certificate pre	sented by this website was not issued by a trusted cer sented by this website was issued for a different webs	tificate authority. ite's address.	
Security certificate problem server.	ns may indicate an attempt to fool you or intercept ar	y data you send to the	
We recommend that you	close this webpage and do not continue to this w	ebsite.	
Click here to close this	webpage.		
Continue to this years	e (not recommended).		
 More information 			

"Continue to this website"をクリックするとログイン画面が表示されます。

デフォルトのユーザー名、パスワードは"admin"です。"admin"でログインします。

Velcome to Hi ISM430 Multis) Service Access Point		
	Autho This system is p Contact [EM	orized access only. property of [COMPAN AIL] for more inform	IY NAME]. hation.
	Current IP	address: 192.168.1.1	
	Ethernet base MAC	address: 2C:41:38:DB:F8:C2	
	Wireless MAC address	(radio 1): 2C:76:8A:EC:FC:80	
	Wireless MAC address	(radio 2): 2C:76:8A:EC:FC:90	R.
		Uptime: 9 minutes	
	Software	e version: 6.0.2.2-16979	
	Username:	Password:	
	admin	•••••	Login

<u>Seliton</u>

3-2 アクセスポイントの初期設定

コントローラーに接続するために、アクセスポイントの初期設定を行います。

画面の「Provision…」をクリックします。

Swich to Autonomous Mode はアクセスポイントのみで動作させる場合に利用します。

コントローラーで管理する場合は Operation Mode は"Controlled"となります。

Inn	MSM430	System name: CN19DX008Y
WP	Home	Logout
You are i	n controlled mode. <u>Click here for more information.</u>	
Welcome to	HP BiComico Accors Doint	?
MSM450 MU		
	Current IP address: 192.168.1.1	
	Ethernet base MAC address: 2C:41:38:DB:F8:C2	
	Wireless MAC address (radio 1): 2C:76:8A:EC:FC:80	
	Wireless MAC address (radio 2): 2C:76:8A:EC:FC:90	
	Uptime: 12 minutes	
	Software version: 6.0.2.2-16979	
	Hardware revision: 39652-60001:54-A	
	Serial number: CN19DX008Y	
	Operational mode: Controlled	

「Provision…」をクリックすると、Connectivity 設定画面が表示されます。

「Connectivity」をチェックします。また、「Assign IP address via」で"Static"を選択し、「Stati c IP Settings」に指定の IP アドレス、サブネットマスク、デフォルトゲートウェイを入力します。



最下部の「Save」をクリックします。

Local mesh radio co	onfiguration	
Radio	Wireless mode	Antenna selection
Radio 1 🗸	802.11a (5 GHz) 🛛 🗙	Diversity

「Discovery」タブをクリックすると、Discovery 設定画面に切り替わります。

「Discovery」をチェックします。「Discovery using Address」にチェックし、「IP address」欄 にコントローラーに設定する IP アドレスを入力し、「Add」をクリックします。



「Add」をクリックすると、「Address to search for」に入力した IP アドレスが表示されます。 最下部の「Save」をクリックします。

	Connectivity Di	scovery Location	
		en e	
liscovery			
			_
-			
Discover using DNS		✓ Discover using IP address	
Names to search for:		Addresses to search for:	
		192.168.1.1	
Name:		IP address:	
Domain name:		Controller authentication	
Domain name: Primary DNS server: Secondary DNS server:		Controller authentication Controller shared secret: Confirm controller shared	



「Connectivity」と「Discovery」の設定が完了したら、左側にある「Info」より「Restart」ボタンをクリックします。

約1分後に「Connectivity」にて設定した IP アドレスで起動します。

			Provisioning	
		Connectivity	Discovery	Location
-				
Summary	🖾 Dis	covery		?
Controlled AP is provisioned.				
Connectivity Yes		Discover using DNS		Discover using IP address
Discovery Yes Location No		Names to search for:		Addresses to search for:
				192.168.1.1
Info				
Once provisioning is complete				
you must restart the AP for				
Portat				
restar				
Restart and stop the provisioning		Name:		IP address:
		Remove Add		Remove Add
	D	omain name:		
		Primary DNS server:	C.	
	s	econdary DNS	0	Controller shared secret:
		serveri		confirm controller shared secret:
				Controller authentication
				Save

<mark>Saliton</mark> 4. MSM7xx シリーズの設定

4-1 コントローラーへのログイン

MSM7xx シリーズのデフォルト IP アドレスは 192.168.1.1/24 に設定されています。

Web ブラウザよりアクセスを行うと、証明書エラーの画面が表示されますが、"Continue to this website"をクリックします。



"Continue to this website"をクリックするとログイン画面が表示されます。

デフォルトのユーザー名、パスワードは"admin"です。"admin"でログインします。



4-2 End User License Agreement

初めてログインを行った場合、End User License Agreement 画面が表示されます。

「Accept HP End User License Agreement」ボタンをクリックします。

End User License Agreement	
PLEASE READ CAREFULLY BEFORE USING Agreement ("EULA") is a legal agrees or a single entity) and (b) Hewlett ("HP") that governs your use of any installed on or made available by H Product") or ii) made available as ; a standalone basis ("HP Software Pr may contain a EULA in its online do means computer software and may inc and "online" or electronic document EULA may accompany the HP Product o	THIS EQUIPMENT: This End-User license ment between (a) you (either an individual -Rackard Company or in-country legal entity Software Product, which is either i) P for use with your HP product ("HP part of the HP product portfolio for use on oduct"), that is not otherwise subject to a you and HP or its suppliers. Other software cumentation. The term "Software Product" lude associated media, printed materials ation. An amendment or addendum to this r HP Software Product.
RIGHTS IN THE SOFTWARE PRODUCT ARE TO ALL TERMS AND CONDITIONS OF THIS OR OTHERWISE USING THE SOFTWARE PRO THIS EULA. IF YOU DO NOT ACCEPT THE RETURN THE ENTIRE UNUSED PRODUCT (H. REFUND, SUBJECT TO THE REFUND POLIC	OFFERED ONLY ON THE CONDITION THAT YOU AGRE EULA. BY INSTALLING, COPYING, DOWNLOADING DUCT, YOU AGREE TO BE BOUND BY THE TERMS OF SE LICENSE TERMS, YOUR SOLE REMEDY IS TO ARDWARE AND SOFTWARE) WITHIN 14 DAYS FOR A Y OF YOUR PLACE OF PURCHASE.
1	

4-3 Product Registration

「Accept HP End User License Agreement」をクリックすると、次は製品登録ページが表示されます。「Register Later」をクリックします。

※「Register Now」をクリックすると、製品登録 URL へ移行します(Internet に接続している必要 があります)。

We recommend registering your product at	t this time.
Product information: Product name: MSM710 Serial number: Z004-00043 MAC address: 00:03:52:BF:03:D2 Firmware version: 6.0.2.2-16979 Hardware revision: 50-00-1029-00:35	Now is a good time to register your MSM710. When you have completed the product registration process, you can continue with initial product configuration. If you chose to register your product later, you can do so by selecting Maintenance > Registration.
Register Later	Register Now

4-4 国コードの設定

「Register Later」をクリックすると、国コード設定画面が表示されます。

国コードを選択し、「Save」をクリックします。

Configure t	he country where the product will	be used
Country:	APAN (W52 & W53 & W56)	Please select the country that this product will operate in. This ensures that wireless radio settings will be configured in accordance with local regulations.
		Save
項目		
Country	JAPAN(W52 & W53 & W56)	

4-5 ユーザーアカウントの設定

デフォルトだとユーザー名、パスワードは"admin"に設定されています。

変更を行う場合は変更します。今回は「Cancel」をクリックします。

Username:	Access to the MSM710 management tool can be restr by an administrator password. It is highly recommend that you change your unit password, especially if it is
Current password:	exposed to external networks.
New password:	For optimum security, your password should be at lea characters long. The password is case-sensitive.
Confirm new password:	
Enable Password Console Reset	
Enable Password Console Reset	

4-6 Automated workflows

問答方式で簡易的にコントローラーの初期設定、SSID の作成ができます。

今回は作成せず、「Home」ボタンをクリックします。

It is highly recommended to run the Configu	ure initial controller settings workflow after a fa	ctory reset.
itomated workflows		
These workflows help you quickly configure c the controller until you click Apply on the wor Select a workflow and click Start to begin.	common controller settings. Changes are not sa rkflow summary page. Description	ived to
Configure initial controller settings Create a wireless network for employees Create a wireless network for guests	This workflow helps you define basic settings for the controller, including r connections, security settings, and s It is recommended that you run this before any other workflow. Prerequisites None	operational network ystem time. workflow
		Start
ne 画面 C y 。]ログインからこの画面が表示されま	हक.	
IE 画面 C 9 。 Iログインからこの画面が表示されま atw <u>r</u> k Security VPN Controlled APs Auth Welcome to HP	たす。 hentication Public access Users Management	Status Tools Mai
Iログインからこの画面が表示されま Exercise Security VPN Controlled APs Auth Welcome to HP MSM710 Controller	たす。 hentication Public access Users Management	Status Tools Mai
Iログインからこの画面が表示されま Example Security VPN Controlled APs Auth Welcome to HP MSM710 Controller Internet pa	hentication Public access Users Management	Status Tools Mai
IDDグインからこの画面が表示されま Security VPN Controlled APs Auth Welcome to HP MSM710 Controller Internet po	hentication Public access Users Management met port address: port MAC address: 00:03:52:8F:03:D2 Default country: JAPAN (W52 & W53 & W56) meteodes sectors Busines	Status Tools Mai
Iログインからこの画面が表示されま Controlled APs Author Welcome to HP MSM710 Controller Internet pa Author Author	hentication Public access Users Management met port address: port MAC address: 00:03:52:8F:03:D2 Default country: JAPAN (W52 & W53 & W56) antication system: Running thenticated users: 0	Status Tools Mai
Iログインからこの画面が表示されま Controlled APs Author Welcome to HP MSM710 Controller Internet pa Author Author	hentication Public access Users Management renet port address: port MAC address: 00:03:52:8F:03:D2 Default country: JAPAN (W52 & W53 & W56) entication system: Running thenticated users: 0 Uptime: 3 hours 48 minutes	Status Tools Mai
Iログインからこの画面が表示されま Security VPN Controlled APs Auth Welcome to HP MSM710 Controller Internet pa Auther Auther	hentication Public access Users Management Public access Users Management met port address: port MAC address: 00:03:52:8F:03:D2 Default country: JAPAN (W52 & W53 & W56) entication system: Running thenticated users: 0 Uptime: 3 hours 48 minutes MP system name: Z004-00043	Status Tools Mai
The 画面 C 9 。 コログインからこの画面が表示されま Controlled APs Author Welcome to HP MSM710 Controller Internet po Author Author SNM	hentication Public access Users Management met port address: bort MAC address: 00:03:52:BF:03:D2 Default country: JAPAN (W52 & W53 & W56) antication system: Running thenticated users: 0 Uptime: 3 hours 48 minutes MP system name: 2004-00043 Software version: 6.0.2.2-16979	Status Tools Mai
IE 画面 C 9 。 Iログインからこの画面が表示されま Controlled APs Auth Welcome to HP MSM710 Controller Internet pr Auther Auther Auther Bind	hentication Public access Users Management hentication Public access Users Management met port address: bort MAC address: 00:03:52:BF:03:D2 Default country: JAPAN (W52 & W53 & W56) antication system: Running thenticated users: 0 Uptime: 3 hours 48 minutes MP system name: Z004-00043 Software version: 6.0.2.2-16979 Hardware revision: 50-00-1029-00:35 Serial number: Z004-00043	Status Tools Mai
IE 画面 C 9 。 Iログインからこの画面が表示されま Controlled APs Auth Welcome to HP MSM710 Controller Internet pr Auther Auther Auther Binder	hentication Public access Users Management met port address: met port address: Management met port address: 00:03:52:8F:03:D2 Default country: JAPAN (W52 & W53 & W56) entication system: Running thenticated users: 0 Uptime: 3 hours 48 minutes MP system name: 2004-00043 Software version: 50-00-1029-00:35 Serial number: 2004-00043	Status Tools Mai

<u>Seliton</u>

4-7 コントローラーIP アドレスの変更

左側の「Network Tree」より「Controller」をクリックします。

[Network]-[IP interface]より「IPv4 Interface」の「LAN port」をクリックします。

LAN Interface Configuration 画面が表示されますので、「Addressing」で IP アドレス、サブネットマスクを変更し、「Save」をクリックします。

※「Save」を行うと即座に設定が反映されます。アドレスを変更した場合は、変更したアドレスで 再度ログインしてください。

Automated workflows		Network		VPN Controlled								
	IP interfaces	Network profiles	VLANs	Ports GRE tunnel:	Address allocatio	n Bandwidth contro	Discove	ry protocols	DNS	IP routes	NAT IP	QoS IGMP proxy
and the second se			Property and									
Alarms			IPv4 int	ace IP	ddress M	isk	Allocation	method	-	Delete		
4 2 4 2 5 2			Intern	et port 0.0	0.0 0.	0.0.0	DHCP			1		
Summary 🛱 ?			LAN p	議, 192	.168.1.1 25	5.255.255.0	STATIC			1		
Controlled APs								Add	New Interfa	C0		
Network Tree EL 2												
Epand All												
Controller												
				/								
Network	Security VP	Controller	APs A	uthentication	Public access	Users Manag	pement	Status	Tools	Mainte	nance	
ID interfaces Natural confiles		GRE MINON		net allocation	Bandwidth control	Discourse are	rocala	DNS	1D routes	NAT	120-5	TOMP MONT
								0.000				
	LAN interfa	ce configura	tion									
							_	_	_			
		- F	Addressi	ng								
				IP address: 19	2.168.1.1							
				Mask: 25	5.255.255.0	<						
		- L										
			Managen	nent address								
				IP address:								
				Mask:								
				1.02		-12						
	Cancel								Save			

項目	値
IP address	192.168.1.1
Mask	255.255.255.0

4-8 デフォルトゲートウェイの設定

[Network]-[IP routes]より「Default routes」のゲートウェイおよびメトリックを設定し、「Add」 をクリックします。

	Network	Security	VPN Controller	APs Authentication	Public access L	Isers Management	Status Tools	Maintenance	
IP interfaces No	etwork profiles	VLAN: P	orts GRE tunne	Is Address allocation	Bandwidth control	Discovery protocols	DNS IP routes	NAT IP Qo	5 IGMP proxy
		Active ro	outes				?		
		Interface	Destination	Mask	Gatew	ay P	letric Delete		
		LAN port	192.168.1.0	255.255.25	55.0 *		0		
			2] [Add		
		Default r	outes				?		
		Interface	Gate	eway		Metric	Delete	1	
			192	.168.1.254		0	LAPO I		
		Persister	nt routes				3		
		Interface	De	stination	Mask	Gatewa	y Delete		
		PPTP Clie	ent V				APO		
	/=±								
項日	1旦								
Gateway	192.1	168.1.25	54						
	0		_						
Metric	0								
							1		
A other neut	-							2	
Active rout	Destination		Mark		Cataway	_	Motels	Delete	
LAN port	192,168,1.0	•	255.2	55.255.0	s Gateway		O	Delete	
		<u> </u>	20012						
								Add	
								Add	
Default rou	ites							Add ?	
Default rou Interface	ites	Gateway				Metric		Add ? elete	
Default rou Interface LAN port	ites	Gateway 192.168.1	1.254			Metric 0	D	Add ? elete	
Default rou Interface LAN port	ites	Gateway 192.168.1	1.254			Metric 0	D	Add ? elete Add	
Default rou Interface LAN port	ites	Gateway 192.168.1	1.254			Metric 0	D	Add ? elete Add	
Default rou Interface LAN port Persistent	ites	Gateway 192.168.7	1.254			Metric 0	D	Add ? elete Add	
Default rou Interface LAN port Persistent Interface	ites	Gateway 192.168.1	1.254	M]	Metric 0	D	Add ? elete Add ? Delete	
Default rou Interface LAN port Persistent Interface	routes	Gateway 192.168.1	1.254	M	ask	Metric 0 Ga	D	Add ? elete Add ? Delete Add	

4-9 アクセスポイントの接続と認識

Provisioning 設定を行ったアクセスポイントを接続します。

アクセスポイントとコントローラーが IP 通信できている場合は「summary」欄にアクセスポイントの状態が表示されます。

表示項目	説明
Synchronized	アクセスポイントとコントローラーのコンフィグが同期しています
Unsynchronized	アクセスポイントとコントローラーコンフィグに差異があります
Detected	コントローラーが発見したアクセスポイント数が表示されます
Configured	コントローラーからコンフィグを流したアクセスポイント数が表示されます
Pending	コントローラーがアクセスポイントに対して操作を行っています

正常に認識がされた場合は、「Network Tree」の[Controller]-[Controlled APs]-[Default Group] にアクセスポイントが表示され、インジケーターは緑で表示されます。

Automated workflows	Network	Security	VPN	Controlled APs	Authentication	Public access
Alarms 🕫 ? 🗛 ፬ 🌲 ፬ 🧥 ፬		Welco MSM7	ome to 10 Cor	HP htroller		
Summary E ?				Int	Internet port add ternet port MAC add	dress: dress: 00:03:52:1
Synchronized 1 Detected 1 Configured 1					Default co Authentication sys	untry: JAPAN (W stem: Running
Ŀş.					Authenticated u	users: 0
Expand All					Up	time: 4 hours 4
IT VSCs					SNMP system n	ame: 2004-000
					Software ve	rsion: 6.0.2.2-16
Default Group					Hardware rev	ision: 50-00-107
CN19DX008Y					Serial nur	mber: 2004-000
		11				

4-10 VLAN の作成

端末の通信データを出力する VLAN を作成します。

「Network Tree」の[Controller]より[Network]-[Network Profiles]の「Add New Profile」をク リックします。「Name」に VLAN を入力し、 VLAN ID にチェックを入れ、 ID を入力します。 「Save」 をクリックします。

作成できると Network Profiles 画面に作成した VLAN が表示されます。

	Network	Security	VPN	Controlled APs	Authentication	Public access	Users	Management	Status	Tools	Maintenance		
IP interfaces Net	work profiles												IGMP proxy
										_			
		Netwo	ork profil	es						?			
		Na	me				VLAN ID		Dele	ete			
		Int	ternet port	network			N/A		2	1			
		LAI	N port netw	ork			N/A	_	2	1			
								A	dd New Pro	ofile			
								_					
									_				
	_	_		1					Y			_	
	Network	Security	VPN	Controlled APs	Authentication	Public access	Users	Management	Status	Tools	Maintenance		_
IP interfaces Net	work profiles	VLANs	Ports	GRE tunnels	Address allocation	Bandwidth contr	ol Disco	ivery protocols	DNS	IP routes	NAT	IP Q₀S	IGMP proxy
		-								_			
		Add/	Edit netv	ork profile									
				Settings									
				Name: VLAN	100								
				VI AN	100								
		Canc	el							Save			
пан	庙												
坦口													
Name		N100											
Hame	V L/1	NICO		_									
VLAN ID	100												
										↓			
	Network	Sacurity	VPN	Controlled APs	Authentication	Public access	Users	Management	Status	Tools	Maintenance	3	
IR interfaces Net	work profiles	VI AN-	Borte	GRE tunnels	Address allocation	Bandwidth cost	Dire	overs protocole	DNS	IR router	NAT		IGMP provo
	more promez		- Contraction			Sandmoth Cont		arely proceeds	- Child	ip routes	and a second	te que	romp proxy
		Netw	ork profi	es						?			
		Na	me				VLAN ID		De	lete			
		In	ternet port	network			N/A		,	1			
		LA	N port netv	ork			N/A			× _			
		XL.	AN100				100		t))			
								A	Add New Pr	ofile			

4-11 RADIUS サーバーの指定

「Network Tree」の[Controller]より[Authenticate]-[RADIUS profiles]の「Add New Profile」 をクリックします。「Profile name」を入力し、必要に応じて「Settings」の内容を変更します。 「Primary RADIUS server」にRADIUSサーバーのIPアドレス、シークレットを入力します。「Save」 をクリックします。

Network Security VPN C	ontrolled APs Auther	ntication Public	access Users	Management	Status	Tools	Maintenance
	RADIUS profiles	RADIUS server	Active directory	802.1X			
RADIUS profiles						2	
Name Prima	iry server	Second	ary server		NAS ID	_	
Add New Profile							
18							
.							
Add/Edit RADIUS profile							
Profile name	Primary RADIUS server						
Profile name: Not Attest EPS	Berver address: 192.168	2					
	Secret:						
Settings	Confirm secret:						
port 1912	Secondary RADIUS server (optional)					
Accounting parts 1613	Terrer address						
Refry [co	Secret						
tomatudi 00 seconde	Confirm secret:						
mathedi MSCHAP-2 V							
Always the primary server first	Authentication realms						
 Use message authenticator 	Changing the realm configur authenticated users.	ration will logout all					
Force SAS-Port to ingress VLAN ID	Associated realmax						
Describe RAS ID when acting as a RADIUS proxy							
L	_						
						1	
				項目		値	
	Support regular expression	one in realm names		D (1			
				Profile na	me	NetAt	test EPS
	Remove			Server ad	dress	192.1	68.1.2
Cause		[Real]		Secret		secret	
A CONTRACTOR OF THE OWNER OWNER OF THE OWNER OWNER OF THE OWNER OWNE OWNER OWNE		orie	L	Schet		300181	-

Network	Security	VPN	Controlled APs	Authentication	Public access	Users	Management	Status	Tools	Maintenance
			RADIUS ;	rofiles RADIO	server Active	directory	802.1X			
	RADIU	IS profile	15						?	
	Name	115	Primary	server	Secondary s	erver	NA	SID		
	Net Atte	st EPS	192.168	.1.2	not configured	f .	Z00	4-00043		
	_									
	Ad	d New Dro	file							
		u ivew r-tu	me							

4-12 VSC の作成

HPの MSM シリーズは SSIDの Profileの総称として VSC(バーチャルサービスコミュニティー) と呼ばれています。

「Network Tree」の[Controller]-[VSCs]より「Add New VSC Profile」をクリックします。

「Profile name」を入力し、「Use Controller for」の「Authentication」、「Access Control」のチ ェックを外します。

※「Authentication」のチェックを入れると、コントローラー内蔵 RADIUS もしくは、コントロー ラー内蔵 RADIUS 経由で外部 RADIUS サーバーに問い合わせます。

「Virtual AP」にチェックを入れ、Name(SSID)を入力します。

「Wireless Protection」にチェックを入れ、「WPA」を選択します。「Mode」に「WPA2」を選択し、「Key source」は「Dynamic」を選択します。

「802.1x authentication」の「RADIUS profile」に[4-11]で作成した RADIUS プロファイルを選 択します。「Save」をクリックします。

s (0.7)	Unerview VIC profiles VIC respirate Windext client: User sanches VIC respirate Windext client: User sanches	
A 2 A 2 wary C 1 Canadad ek Free C 2 Canadad SC3	Image Express Express Express Express Express All 0* (0) (MA) (0) (MA) <th>ethentica • HAI</th>	ethentica • HAI
netrolled APs		
Durvies	Configuration	
	iC profile	
C: HP VSC profile		
Gobal 7	✓ Wireless protection WPA ▼	
Profile name: Soliton	Mode*s WPA2 (AES/CCMP) V	
Use Controller for: D Authentication	Terminate WDA at the controller "On radius where client access is restricted to r-clients only. WDA2 is always used instead of WDA	
🖉 Virtual AP	< 002.1X authentication	
WLAN Name (SSID): Soliton	Authentication	
DTIM count: 1 Ø Broadcast name (SSID) Advertise TX pover	General RADIUS accountings	
Broadcast filtering Band steering	Called-Station-1d contents BSSID V	
Wireless clients Max clients per 100 Allow teams: and a	MAC-based authentication	
between: 21 V sineless clients	V sature and a Net Attest EPS V	
Nority mechanism: DiffSetv V	Net Attest EPS V	
	🖉 called-teation-1d contents Wireless Radio 🛩	
O MAC address:		
		-

項目	値
Profile name	Soliton
Name(SSID)	Soliton
Wireless Protection	WPA
Mode	WPA2
Key source	Dynamic
Authentication	NetAttes EPS

4-13 AP グループの作成

アクセスポイントのグループごとに VSC を選択することができます。

「Network Tree 」の[Controller]-[Controlled APs] より[Group management]-[Group management]の「Add New Group」をクリックします。

「Group settings」の「Name」を入力し、「Save」をクリックします。

作成すると「Base Group」に作成したグループが表示されます。

Automated workflows	Overview	Configuration Rad	io management Group management	Security Tools Provisioning
			Group management	
-	Become and a second			
Alarms 🖽 ?	Base Group: /	MI Group manage	ament APr la group	17
	Default Group		0	
Summary 612				
Carbolled 4D	Add New Gi	oup.		
Controlled APS				
Network Tree 🛛 🛱 ?				
Expand All				
HP (Default)				
Soliton				
E Controlled APs				
Default Group				
		-		
Overview Configurat	ton Kacio management Group management Security 10015	Provisioning		
	Group management			
Bace Croup: All Crou	n profile			
Buse Group. Mit Grou	p prome			
	Group settings			
	Name: Soliton OFFICE ×			
			75 12	店
			項目	1旦
Cancel		Save		
		لقبلك	Name	Soliton OFFICE
			-	I

Overview	Configuration	Radio management	Group management	Security	Tools	Provisioning
		Grou	up management			
Base Group: (All Group ma	nagement				?
Group name			APs in group			
Default Group			0			_
Soliton OFFICE			0			
						_
Add New G						
Add New G	oup					

4-14 AP 名、グループの変更

「Network Tree」の[Controller]-[Controlled APs]-[Default Group]に表示されているアクセス ポイントをクリックします。

※デフォルトはシリアルナンバーがアクセスポイント名となっています。

[Device management]-[AP management]の「Access point name」を変更し、「Group」は[4-13] で作成したグループを選択します。「Save」をクリックします。

「Save」をクリックすると、[Network Tree]の[Controller]-[Controlled APs]の[Default Group] から作成したグループへアクセスポイントが移動します。

インジケーターは黄色になり、「Summary」では「Unsynchronized」となります。



項目	値
Access point name	AP-01
Group	Soliton OFFICE



4-15 グループと VSC の紐付け

作成したグループは何も SSID を出力していない状態です。VSC を紐付けることで、SSID を出力します。

「Network Tree」の[Controller]-[Controlled APs]の作成したグループより[VSC bindings]の「Add New Binding」をクリックします。

「VSC Profile」にて[4-12]で作成した VSC を選択します。「Egress network」にチェックを入れ、 「Network Profile」で[4-10]で作成した VLAN を選択します。

※「Egress network」にチェックを入れることで、アクセスポイントから直接指定の VLAN へ出力 できるようになります。「Save」をクリックします。



?			pindings	OFFICE VSC b	Group: Solito
	io behavior	Dual-radio	Egress network	VSC SSID	VSC Name
	radios 1 and 2	Active on ra	VLAN100 (100)	Soliton	Soliton
	radios 1 and 2	Active on ra	VLAN100 (100)	Soliton	Soliton

4-16 コンフィグの同期

ここまでは、アクセスポイントのコンフィグの作成を行いました。コントローラーとアクセスポイントを同期させることによって、アクセスポイントから設定した SSID が出力できるようになります。 [Summary]の「Unsynchronized」をクリックし、「Select the action to all listed APs」で「Synchronize Configuration」を選択し、「Apply」をクリックします。

[Summary]にて「Synchronized」となり、アクセスポイントのインジケーターが緑に表示されれ ば、同期が完了となります。

Alarms [] ? Summary [] ? Status Controlled APs [] ? Unavorbranized 1 Configured 1 Controlled APs 1	Automated workflows	Overview
Alarms (d) ? Alarms (d) ? Summary: Unsynchronized Discovered APs (f) ? Summary: Onscient APs (f) ? Summary: On controlled APs ? Controlled APs ? Controlled APs ? O Controlled APs ? Default Group ? > Solution OFFICE ? AP-01 >		Discovered APs Witteless clients
A 2 A 3 Summory C Summory C Status Controlled AP ame Serial number of vicess service Wreless cleants Diagnostic Act in Controlled AP ame C C C AP Mode [10] = Local Mesh Mode C] = MP/Local Mesh Mode C] = Monitor Mode C] = Sensor Mode X = Disate et I Network Tree C C Controlled APs I O Controlled APs Default Group AVone Configured> Soliton OFFICE AP-01	Alarms 11 7	Summary: Unsynchronized Discovered APs 🛱 ?
Select the action to apply to all listed AD Synchronized Configuration Activity Status Controlled AP Disanostic Activity Unsynchronized 1 Configuradio 1 Configuradio 1 Configuradio 1 Retwork Tree 1 Excand All 0 VSCs Controlled APs Default Group Overfigured> Note Configured> Soliton OFFICE AP-01	🛆 Q 🔺 Q 🔥 Q	Number of access points: 1
Summary Clip Introduct APs 1 Controlled APs 1 Controlled APs 1 Controlled APs 1 Controlled APs 1 Status Controlled APs 1 Status Controlled APs 1 Status Controlled APs 1 Controlled APs 1 Octored 2 Solution OFFICE AP-01		Select the action to apply to all listed AD Synchronize Configuration 🗸 Apply
Image: Controlled APs □ Default Group < None Configured>	Summary C ?	Status Controlled AP name Serial number Wireless services Wireless clients Diagnostic Action O CN19DX008Y CN19DX008Y \$128 \$198 0 Unsynchronized Synth
Network Tree Expand All Controller VSCs Controlled APs Default Group KNone Configured> Soliton OFFICE AP-01	Detected 1 Configured 1	💱 = AP Mode 🏣 = Local Mesh Mode 🢱 = AP/Local Mesh Mode 🔍 = Monitor Mode 👰 = Sensor Mode 🗶 = Disat ed
Controller VSCs Controlled APs Default Group <none configured=""> Soliton OFFICE AP-01</none>	Network Tree 🕮 ?	
Controlled APs Default Group None Configured> Soliton OFFICE AP-01	Controller VSCs	
Soliton OFFICE AP-01	 Controlled APs Default Group <none configured=""></none> 	
	Soliton OFFICE O AP-01	

Automated workflows	Overview
	Discovered APs Wireless clients
Alarms 🛱 7	Summary: Unsynchronized Discovered APs 🛱 ?
🗛 ହ 🔥 ହ	Number of access points: 0
	Select the action to apply to all listed APs (= Select an Action = 🗸 Apply
Summary P ?	Status Controlled AP.name Serial number Wireless services Wireless clients Diagnostic Action
Controlled APa Synchronized 1 Detected 1 Configured 1	👫 = AP Mode 🐉 = Local Mesh Mode 💱 = AP/Local Mesh Mode 🔍 = Monitor Mode 😻 = Sensor Mode 🗶 = Disabled
Network Tree 🕮 ? Expand All	
Controller IN VSCs	
Controlled APs Default Group <inone configured=""> Controlled APs AP-01</inone>	

 \mathbf{J}

<u>Seliton</u> 5. アクセスポイントへの TLS 認証

5-1 iOS (iPad)

5-1-1 iOS へのデジタル証明書のインストール

NetAttest EPS から発行したデジタル証明書を iOS デバイスにインストールする方法として、下記の方法などがあります。

1) iPhone 構成ユーティリティ(構成プロファイル)を使う方法

2) デジタル証明書をメールに添付し iOS デバイスに送り、インストールする方法

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ストールします。本書では割愛します。

5-1-2 サプリカントの設定

MSM7xx シリーズで設定した SSID をタップし、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アカウントの 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」よりインストールされたユーザ ー証明書を選択します。



5-2 Android (Nexus7)

5-2-1 Android へのデジタル証明書のインストール

NetAttest EPS から発行したデジタル証明書を Android デバイスにインストールする方法として、 下記 3 つの方法等があります。いずれかの方法で CA 証明書とユーザー証明書をインストールします。 手順については、本書では割愛させて頂きます。

1) SD カードにデジタル証明書を保存し、インストールする方法※1

2) デジタル証明書をメールに添付し Android デバイスに送り、インストールする方法※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、インストール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、インストール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、EPS-ap Android アプリ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。

5-2-2 サプリカントの設定

MSM7xx シリーズで設定した SSID をタップし、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。また、本書では、CA 証明書を含めた PKCS#12 ファイルをインストールしたため、CA 証明書及びユーザー証明書が同じ名前になっています。 CA 証明書を個別にインストールした場合は、その CA 証明書を選択してください。

				🛜 🛢 15:54
া	🕽 wi-Fi	ON	Ø	+ :
	NUMBER OF STREET, STRE			
	entrenet Receive annual fint			
	nanar Maria Antonia			7
	titan na Maria Maria			A
	NA Asiani Anno 1995			1
	a la tracta de la composition de la compo			Â
	Aller Market			1
	Soliton 802.1xで保護			9
	nina anti-ante			R
	internationalises Internationalises			1
	initia in			(¢
	in the state			1
	age and a set of the s			7
	()	\triangle	Ē	

A = 1				AB 📚 I	17:00
Wi-Fi			65		
保存済み、WPA2で保護				Ţ	6
Soliton					
電波強度	非常に強い				
セキュリティ	802.1x EAP				
EAP方式					
CA証明書	(指定なし)				
ユーザー証明書	(指定なし)				
ID					
□ 詳細オプションを	表示				
キャンセ	ль		接続		
and the second sec				Į.	2
Soliton					
\mathbf{q}^{1} \mathbf{w}^{2} \mathbf{e}^{3}	r ⁴ t ⁵	y u	18	9 0	p
a s d	fg	h	jŀ		
ф z x	c v	b n	m	@	×
文字 😓	,		?	⇔	次へ
~		2	0		

項目	値
セキュリティ	802.1x EAP
EAP 方式	TLS
CA 証明書	user01
ユーザー証明書	user01
ID	user01

6. アクセスポイントへのゲスト用ワンタイムパスワード認証

6-1 NetAttest EPS の設定変更

6-1-1 DPX ファイルのインポート

EPS のシステム管理ページより[RADIUS サーバー]-[VASCO DIGIPASS]-[DPX ファイルイン ポート]にて DPX ファイルを参照し、転送キーを入力します。「インポート」をクリックします。 ※DPX ファイルはご購入頂くと、製品と一緒に納品されます。評価用の DPX ファイルもご用意して おります。

DPX ファイルをインポートすると、[RADIUS サーバー]-[VASCO DIGIPASS]-[トークン一覧]にて、 ご購入頂いた数だけ一覧に表示されます。

NetAttest EPS	ログオン中: admin
 mappalocal システム(数定) システム(数定) システム(数定) ロドロドリーバー ロレロドリーバー ロレロドリーバー ロムロドリーバー RADILSサーバー(数定) RADILSサーバー(数定) RADILSサーバー(数定) PROFINET(1) RADILSサーバー(数定) PROFINET(1) RADILSサーバー(数定) ロントー(数定) ロントー(1) ロント(1) ロント(1) ロント(1) ロントー(1) ロント(1) ロント(1)<	
Sopyright Prost 2014, Golden Systems K.K. A	

NetAttest ころの ・ napsubai ・ システム後空 ・ システム後空 ・ システム後空 ・ システム ・ レロクサーバー ・ レロクサーバー ・ レロレターバー ・ レフィー ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・					(0 Hz	=05 (~-2)	オン中: adm ① ロジオフ
■ meptioni							
 システム管理 証明報因 	トークンシリアルNo	•	· 元순 1/18 경지는 ~ 2	100 Att MA			
■ LDAPサーバー	トークンシリアルNo	トーケノモデル	- <u></u> ∠ポート日時	使用中のユーザー田		タスク	
RADIUS 7-15-					Utzak	安里	Rei Na
 記録/停止 RADIUSサーバー設定 					Utzot	¥.E	MIN .
■ RAELLS ワーパー管理					Utzah	*E	NR
NetAttest EFS - mepsion - 277-1852 - 277-1852 - 277-1852 - 277-1852 - 277-1852 - 277-16- - 2840/194 - 10207-16- - 2840/194 - 840189-16-852 - 840189-16-852 - 840189-16-852 - 840189-16-852 - 840189-16-852 - 84018 - 84018					Utest	**	M Rk
					Utzah	¥ P	THE RM
	-	10000			Utzat	**	IN I RE
■トークン情報エクスポート					Utzak	R.E.	PI IX
JetAttest EFS respectional システム協会 システム協会 システム協会 システム協会 システム協会 システム協会 エロークーバー モルロレター モルロレター モルロレター モルロレター モルロレター モルロレター モルロレター モルロレター モルロレター モルロレター モルロレター モルロレ モルロレター モルロレ モルロレ モルロレ モルロ モルロ モルロ モルロ モルロ モルロ モルロ モルロ	and the second se				Utest	東東	M Nk
					Utest	**	IFI RE
Converted # 2014-2014 Soliton Systems K K	All rights manual						

6-1-2 ユーザーとトークンの紐付け

ユーザーとトークンの紐付けを行います。

[ユーザー]-[ユーザー一覧]より、作成済みのユーザーの「変更」をクリックします。

「OTP」タブの「トークンシリアル No」に、このユーザーに割り当てたいトークンシリアルナンバ ーを[6-1-1]のトークン一覧の中から選択し、入力します。

「チェックアイテム」タブの「認証タイプ」より「VASCO」を選択します。「適用」をクリックしま す。



6-2 MSM7xx シリーズの設定変更

[4. MSM7xx シリーズの設定]が完了している前提で、ゲスト用ワンタイムパスワード認証を行うための MSM7xx シリーズの設定変更方法の説明を行います。

6-2-1 コントローラーIP アドレスの変更

「Network Tree」の[Controller]より[Network]-[IP interfaces]において、「IPv4 interfaces」の「Internet port」をクリックします。

「Assign IP Address via」で「Static」を選択し、「Configure」をクリックします。

「Port settings」において、指定の IP アドレス、サブネットマスクを入力し、「Save」をクリック します。





6-2-2 DHCP サーバーの起動

ゲストユーザーに対して、コントローラーから IP アドレスを付与するために、DHCP サーバーを 起動します。

「Network Tree」の[Controller]より[Network]-[Address allocation]において、「DHCP services」の「DHCP server」を選択し、「Configure」をクリックします。

「Addresses」において、DHCP プールを設定します。「Settings」において、「LAN port」のチェ ックを外し、「Save」をクリックします。

Netw	ork Security VPN	Controlled APs	Authentication	Public access	Users	Management	Status	Tools	Maintenano	e .	
Network Security VPN Controlled 1P Interfaces Network profiles VLAxs Parts GRE tunnel Address allocation confi DHCP services Image: Configuration Image: Configuration DHCP server configuration None Image: Configuration Addresses Start: 192.168.1.2 Image: Configuration Addresses Start: 192.168.1.254 Image: Configuration Excluding the MSM710 which is assigned the address/mask: 192.168.1.1/255.255.00 Image: Configuration DNS servers to assign to client stations Addresses Image: Configuration Fixed Leases Image: Configuration Image: Configuration	GRE tunnels Ad	ddress allocation	Bandwidth co	itrol Disc	overy protocols	DNS	IP routes	NAT	IP QoS	IGMP	
	Address alloca	ation configurati	on								
	DHCP services		2	VPN address	pool						
	• DHCF	P server Cor	nfigure	Addr	ess allocation	Use Static IP	Addresses	~			
		Prelay agent Cor	nfigure	Startin	g IP address:	192.168.2.1					
	O None	r		Max	connections	: 10					
								Save			
HCP server co	nfiguration										
0.577.0			and history								
Addresses			Setti	ngs							
Starts	192.168.1.2		Dom	ain name:	hp.lan						
End	192 168 1 254	รี	ال	ase time:	3600		12				
	100 400 4 4				Locaut II	seconds	discourse				
Gatewayı	192.106.1.1			<u> </u>	Logout Hi	ML User on	discovery	request			
Excluding the M	SM710 which is assign sk: 192 168 1 1/255 2	ned 55,255.0	Lis	sten for DH	CP reques	its on:					
					LAN port						
DNS servers t	o assign to client sta	tions		2	Client dat	a tunnel					
Address list	192.100.1.1										
	Eined Lanses	Certorilize Adv Advises allection Date scenario Date scenario Date scenario Date scenario Cdf curveliz Address allection Date scenario Date scenario </td									
	Fixed Leases		Ad	Idress list:							
		Security VPN Controlled APs A VLANS Ports GRE tunnels Addre Address allocation configuration DHCP services DHCP relay agen OHCP relay agen None 2.168.1.2 2.168.1.254 2.168.1.254 2.168.1.1 10 which is assigned 192.168.1.1 10 which is assigned 192.168.1.1 Xed Leases									
						IP addr	ess:				
	Network Security VPN Controlled APS Network probles VLANs Ports GRE tunnels Add Address allocation configuration Image: Configuration Image: Configuration Image: Configuration Prer configuration Image: Configuration Image: Configuration Image: Configuration es ? Start: 192.168.1.2 Image: Configuration es ? Start: 192.168.1.254 Image: Configuration intervalue 192.168.1.254 Image: Configuration Image: Configuration es ? Start: 192.168.1.255 Image: Configuration intervalue 192.168.1.2 Image: Configuration Image: Configuration intervalue 192.168.1.2 Image: Configuration Image: Configuration intervalue 192.168.1.2 Image: Configuration Image: Configuration intervalue 192.168.1.1 Image: Configuration Image: Configuration intervalue 192.168.1.1 Image: Configuration Image: Configuration intervalue 192.168.1.1 Image: Configuration Image: Configuration							0			
					Remo	we A	bb				
			h					_	-1		
Cancel								Sa	we		
									2		



6-2-3 アクセスポイントの接続と認識

Provisioning 設定を行ったアクセスポイントを接続します。

アクセスポイントとコントローラーが IP 通信できている場合は「summary」欄にアクセスポイントの状態が表示されます。

表示項目	説明
Synchronized	アクセスポイントとコントローラーのコンフィグが同期しています
Unsynchronized	アクセスポイントとコントローラーコンフィグに差異があります
Detected	コントローラーが発見したアクセスポイント数が表示されます
Configured	コントローラーからコンフィグを流したアクセスポイント数が表示されます
Pending	コントローラーがアクセスポイントに対して操作を行っています

正常に認識がされた場合は、「Network Tree」の[Controller]-[Controlled APs]-[Default Group] にアクセスポイントが表示され、インジケーターは緑で表示されます。





6-2-4 RADIUS サーバーの指定

「Network Tree」の[Controller]より[Authenticate]-[RADIUS profiles]の「Add New Profile」 をクリックします。「Profile name」を入力し、「Settings」の「Authentication method」を「PAP」 に変更します。「Primary RADIUS server」に RADIUS サーバーの IP アドレス、シークレットを入 力します。「Save」をクリックします。

RADIUS profiles 2 RADIUS profiles 2 Add New Profile Add New Profile Add New Profile NAS ID Add New Profile NAS ID Add New Profile Name Mathematic and the data of the	Network Security VPN	Controlled APs Auther	ntication Public acc	tess Users	Management Statu:	s Tools	Maintenance
RADULUS profiles Primary server NAS ID Add New Profile. Add New Profile. Add New Profile. Image: Add New Profile. Image: Add New Profil		RADIUS profiles	RADIUS server	Active directory	802.1X		
Name Primary server Secondary server NAS ID Add New Profile	RADIUS profile					?	
Add New Pofile Add/add SADDES profile Add/add SADDES profile Write warm: low defease 100° files Write warm: low defease Write warm warm Write warm warm warm Write warm warm warm warm warm	Name P	rimary server	Secondary	server	NAS II	,	
Add New Profile Add/clat RACIOS profile Image: Racio profile <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>							
Add/r_cdit ZACIUS prodit Furfik same File Furfik same File <	Add New Prot	file					
Add/ddt ZADDIDS.profile Fundie zame: Fining MADDID server Fining Fining MADDID server Fining MADDID server Fining MADDID server Fining M							
Add/Add LADUUS provide Image: Mathematication Image: Mathematicati							
Add/tell LABIUS provide	<u> </u>						
Proteins same Proteins (M2 100) Server Settings Server Server Numerity Settings Server Mathematication Server Mathematication Mathematication Server address 192.168.1.2 Server address 192.168.1.2 Server address Server	Add/Edit RADIUS profile						
Predite name Predite name	Profile same	Primary RADIUS server					
Setting Setting	Profile name: Net Attest EPS	Berver address: 192.168.1	12				
Server Gendrem Names Authentication reading MAXIMUM Server (lystimus/) Server address Server intervision Maximum Server address Server address Server address Server address Server address Server address Server address Server	Company and Company and Company	Secret:					
yes 1013 Accounting partin 1013 Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment) Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment) Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment) Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment) Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment) Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment) Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment) Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment) Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment) Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment) Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment) Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment) Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment) Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment) Secondary AADD05 server (getiment) Image: Secondary AADD05 server (getiment)	Settings	Confirm secret:					
Reary intervit Image: Securit Base: Image: Securit Securit Securit Securit	port: 1812	Secondary RADIUS server (optional)				
Image: second	Retry interval: 10 accords	Server eddress:					
Secret	Retry 60	Secret:					
Image and and a set of a s	Authentication (MS/NAD-2 M	Confirm secret:					
Adversity primary server first User message authentication reading From MAG-front to ingress VLAN ID Describe MAG front to ingress VLAN ID Describe MAG front to ingress VLAN ID Bupport regular respressions in realma Bupport regular respressions in realma Bupport regular respressions in realma Remove Add Cancel	NAS ID: 2004-00043						
Cancel Charactery authentication Concel Concel	Always by primary server first	Authentication realmo					
Image: Forme Ned-Port to ingress VLAN ID Associated reading: Duardide NAS ID when setting as a Image: Forme Ned-Port to ingress value of the setting as a Image:	② Use message authenticetor	Changing the realm configur authenticated users.	ration will logout all				
東本のtruits pressy 項目 値 Image: Support regular expressions in regin names Profile name NetAttest EPS Authentication method PAP Server address 192.168.1.2 Secret secret	Force NAS-Port to ingress VLAN Override NAS ID when acting as	Associated realmax					
項目 値 Bupport regular segmentations in regmentations in regmentati	L RADIUS proxy						
Image: Secret Image: Secret<							
Buygert regular segmentions in realm names Profile name NetAttest EPS Authentication method PAP Server address 192.168.1.2 Secret secret				項目		値	
Integration regular segressions in regime names Frome frame NetAttest EPS Authentication method PAP Server address 192.168.1.2 Secret secret				Drofile	namo	NotA	toct EDS
Authentication method PAP Server address 192.168.1.2 Secret secret		U Support regular augressi	one in realm names	Profile		INELA	LIESL EFS
Cancel Server address 192.168.1.2 Secret Secret		New readout		Authe	ntication metho	d PAP	
Cancel Saw Secret secret		Remove		Serve	r address	192.1	68.1.2
	Cancel		Saw	Secre	t	secre	t

		802.1X	iny 📗										These of the
			COMPANY OF	e directory	Active	5 serve	RADIUS	profiles	RADIUS				
												-	
1113	_				_				_	25	JS profile	RADI	
_	NASID	NA		erver	econdary s			vserver	Primary			Name	
13	Z004-00043	Z0		d	et configured			8.1.2	192.168		est EPS	Net Atte	
									7				
										ofile	id New Pro	Ad	
]	ofile	id New Pro	Ad	

<u>Seliton</u>

6-2-5 VSC の作成

「Network Tree」の[Controller]-[VSCs]より、今回はデフォルト VSC である「HP」をクリック します。

「Use Controller for」の「Authentication」、「Access Control」のチェックを入れます。

「Wireless Protection」にチェックを入れ、「WPA」を選択します。「Mode」に「WPA2」を選択し、「Key source」は「Preshared Key」を選択します。

「Client data tunnel」の「Always tunnel client traffic」にチェックを入れ、「HTML-based user logins」にチェックを入れます。

「Authentication」で「Remote」をチェックし、[6-1-4]で作成したプロファイルを選択します。 「Save」をクリックします。



値

HP

HP

WPA

WPA2

Preshared Key

NetAttes EPS



6-2-6 AP グループの追加

「Network Tree」の[Controller]-[Controlled APs]より、[Group management]の「Add New Group」をクリックします。

「Group settings」に任意のグループ名を入力します。「Save」をクリックします。

Automated workflows	Overview	Configuration Radio manageme	ant Group management	Security Tools Provisioning
			Group management	
Alarms D ?	Base Group:	MI Group management		7
A0 A0 A0	Group name		APs in group	
	Default Group		0	
Summary # ?	Soliton OFFICE		1	
Industrial Control of				
Synchronized 1	Add New Gr	pupment		
Detected 1		0		
BRENE WAR AND				
Network Tree 🖽 ?				
Expand All				
E VSCs				
HP (Default)				
Soliton				
Controlled APc				
Controlled Ars				
	· · · · · · · · · · · · · · · · · · ·			
Overview Configuratio	an Radio management Group management Security Tools	Provisioning		
Connightatio				
	Group management			
Base Group: All Group	profile			
	Group settings			
	Name: HP Office X			
			項日	1旦
Cancel		Sauth		
Concer		Dave 2	Name	HP OFFICE
			L	1

Overview Co	Ingeration	Racio management	Group management	Becuncy	roons	Provisioning
		Grou	ip management			
Base Group: All	Group ma	nacement				
Group name		nagement	APs in group		_	
Default Group			0			
IP Office			0			
Soliton OFFICE			1			
Add New Group						
ride from broup						



6-2-7 AP 名、グループの変更

「Network Tree」の[Controller]-[Controlled APs]-[Default Group]に表示されているアクセス ポイントをクリックします。

※デフォルトはシリアルナンバーがアクセスポイント名となっています。

[Device management]-[AP management]の「Access point name」を変更し、「Group」は[6-1-6] で追加したグループを選択します。「Save」をクリックします。

「Save」をクリックすると、[Network Tree]の[Controller]-[Controlled APs]の[Default Group] から作成したグループへアクセスポイントが移動します。

インジケーターは黄色になり、「Summary」では「Unsynchronized」となります。



項目	値
Access point name	AP-01
Group	HP OFFICE



6-2-8 グループと VSC の紐付け

作成したグループは何も SSID を出力していない状態です。VSC を紐付けることで、SSID を出力します。

「Network Tree」の[Controller]-[Controlled APs]の作成したグループより[VSC bindings]の「Add New Binding」をクリックします。

「VSC Profile」にて[6-1-5]で作成した VSC を選択します。「Save」をクリックします。

Image: Second Jackson VSC Standings Provide labolator Image: Second Jackson VSC Standing Dadrada labolator Image: Second Jackson Statistic Alling Statistic Alling (Cristak) torn OFFCE VSC bindings Statistic Alling VSC bindings Configuration Statistic Alling VSC bindings On multiple radio products VSC list active on: Both radios Image: IPO Office On multiple radio products VSC list active on: Both radios Image: IPO Office Istervice, profile: VLANIDO (100) Image: IPO Office VSC Profile Intervice Image: IPO Office VSC Profile	Automated workflows	Overvie	w VSC bindings Configuration	Radio management Gro	ip management Security Tools	Provisioning
M S & S S Server WS SD Genes network Dual-radio behavior Add Hee Binding Add Hee Binding Add Hee Binding Scattelied ADs at the Binding Add Hee Binding Image: State and	rms the ?	Gro	sup: HP Office VSC bindings			2
Image: Stand Add Address Add Address Add Address Add Address Add Address Add Address Ad	a 🔺 a 🔥 a	vsc	Name VSC SSID	Egress network	Dual-radio behavior	_
Second 4.5% Tree Second 4.5% Second 4.0% Used 4.0% Visc bindings	nmary 티 ?		Add New Binding			
Tree Image: Configuration Configuration Redo management VSC bindings Configuration VSC bindings VSC bindings rest VSC bindings rest Configuration VSC bindings Configuration VSC bindings VSC bindings rest Configuration Sc Profile Usel radio behavior On multiple radio behavior On multiple radio security Sc Profile Imagement rest Configuration - aware group Group name: Imagement Group name: Imagement VSC Profile VSC Profile	Controlled APs chronized 1 isted 1 figured 1					
bler k (Grauk) ton Torlid APs aut Group ton OFFICE VSC bindings VSC bindings vSC bindings vSC bindings ty SC binding	work Tree 🗇 ?					
Opfaukt) ton Colfaukt) ton VSC bindings Configuration Radio management VSC bindings Configuration Realize management Group names: Provisioning VSC Profile: HP Group names: HP Office VSC Profile: VID Group names: HP Office VSC Profile	Expand All Controller					
VSC bindings Configuration Radio management Group management Security Tools Provisioning vSC bindings Configuration Radio management Group management Security Tools Provisioning up: HP Office VSC bindings VSC bindings Imagement Group management Security Tools Provisioning up: HP Office VSC bindings Imagement Group management Security Tools Provisioning up: HP Office VSC bindings Imagement Group management Group Group </td <td>VSCs HP (Default)</td> <td></td> <td></td> <td></td> <td></td> <td></td>	VSCs HP (Default)					
VSC bindings Configuration Radio management Security Tools Provisioning VSC bindings Configuration Radio management Security Tools Provisioning up: HP Office VSC bindings VSC bindings Imagement Security Tools Provisioning sc Profile VSC bindings Imagement Security Tools Provisioning sc Profile VSC bindings Imagement Security Tools Provisioning sc Profile Imagement Imagement Security Tools Provisioning sc Profile Imagement Imagement Security Imagement Imagement sc Profile Imagement Imagement Imagement	Controlled APs					
ton OFFICE VSC bindings Configuration Radio management Group management Security Tools Provisioning USC bindings up: IIP Office VSC binding sc Profile	Default Group					
VSC bindings Configuration Radio management Group management Security Tools Provisioning USC bindings up: HP Office VSC binding SC Profile: USC binding Configuration Radio behavior On multiple radio products VSC is active on: Both radios Configuration Security Group name: HP Office	Soliton OFFICE					
VSC bindings Configuration Radio management Group management Security Tools Provisioning up: HP Office VSC binding VSC binding Image: Configuration			\checkmark			
VSC bindings up: IP Office VSC binding csc Profile	erview VSC bindings Configuratio	n Radio management Group m	anagement Security 1	Tools Provisioning		
up: HP Office VSC binding 7 SC Profile Dual-radio behavior On multiple radio products VSC is active on: Both radios マ Egress network Location-aware group Group name: HP Office JEE		VSC bindings				
sc Profile Usal-radio behavior On multiple radio products VSC is active on: Both radios Cocation-aware group Group name: HP Office Incel VSC Profile VSC Profile	Group: HP Office VSC binding			2		
ASC Profile: HP Cn multiple radio products VSC is active on: Both radios Egress network tetwork profile: VLAN100 (100) Croup name: HP Office Tg目 Cred	VSC Profile	Dual-radio I	behavior			
Egress network tetwork profile: VLAN100 (100) Group name: 卅P Office Incel Incel IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	VSC Profile: HP	On multiple	e radio products VSC is active Both radios	on:		
tetwork profile: VLAN100 (100) Group name: HP Office Incel	Egress network					
Group name: HP Office ncel	Network profile: VLAN100 (100)	Location-av	rare group			
		Group	name: HP Office		項目	
	Cancel			24ve	VSC Profile	

		VSC bindin	05	
Group: HP Of	fice VSC bindings			
VSC Name	VSC SSID	Egress network	Dual-radio behavior	
HP	HP	n/a	Active on radios 1 and 2	

6-2-9 コンフィグの同期

ここまでは、アクセスポイントのコンフィグの作成を行いました。コントローラーとアクセスポイントを同期させることによって、アクセスポイントから設定した SSID が出力できるようになります。 [Summary]の「Unsynchronized」をクリックし、「Select the action to all listed APs」で「Synchronize Configuration」を選択し、「Apply」をクリックします。

[Summary]にて「Synchronized」となり、アクセスポイントのインジケーターが緑に表示されれ ば、同期が完了となります。

Automated workflows	Overview
	Discovered APs Wireless cliants
dia a dia	Community Uncomplemented Decoursed ADc
	Number of access points 1
* × •× ••×	Select the action to apply to all listed AP
Summary EL ?	Status Controlled AP name Serial number Wireless services Wireless clients Diagnostic Action
ontrolled APs	O AP-01 CN19DX008Y ⁶ f ³ 0 Unsynchronized Sinch
Detected 1	
Configured 1	T = AP Mode [1:] = Local Mesh Mode "[1:] = AP/Local Mesh Mode 🐪 = Monitor mode 🦹 = pensor mode 🥂 = Usagred
Network Tree 13 7	
Expand All	
Controller	
 HP (Default) 	
Soliton	
Controlled APs	
Default Group	
AP-01	
Soliton OFFICE	
<none configured=""></none>	
-	
	↓
Automated workflows	Overview VSC bindings Configuration Radio management Group management Security Toola Provisioning
	Discovered APs Canfigured APs Wireless clients Wireless rates Local mesh neighborhood Local mesh links RTLS Licenses
Alarma and	Crowne UB Office Discovered ABc // 2
	Number of access points: 1
	Select the action to apply to all listed APs: - Select an Action - V Apply
Summary 🛱 ?	Status Controlled AP name Serial number Wireless services Wireless clients Diagnostic Action
Controlled APs Synchronized 1	AP-01 CN19DX008Y 678 0 Synchronized Remove
Detected 1 Configured 1	💱
Network Tree 🕮 7	
Expand All	
⊡ VSCs	
HP (Default) Soliton	
Controlled APs	
Default Group	
E HD Office	
• AP-01	
Soliton OFFICE None Configured>	
chone compared?	

iPad にて SSID「HP」をタップすると WEB ページにリダイレクトされます。

Wi-Fi

ALC: NOT THE OWNER, MANAGER, M

€ ? (i)

≜ ╤ (i)

「Username」、「Password」を求められますので、今回は「Password」部分に弊社で取り扱っている、VASCO 社製のワンタイムパスワードを入力します。

※ワンタイムパスワードである「DIGIPASS」はハードウェアタイプ、ソフトウェアタイプ(Windows、 iOS、Android)をご用意しております。ソフトウェアタイプの各 OS でのアクティベーション方法 などは割愛させて頂きます。詳しくは、「ワンタイムパスワード 利用者向け簡易設定手順書」をご

参照ください。

設定

▶ 機内モード

iPhone



Password

ワンタイムパスワード

Seliton 7. 証明書配布ソリューション連携について

EAP-TLS 認証に必要となるクライアントへの証明書配布について、マルチデバイス対応の証明書 配布ソリューション「NetAttest EPS-ap」との連携も可能です。コントローラーのキャプティブポ ータル機能と連携し、未登録端末は証明書発行申請ページへ誘導させることができます。



図 証明書配布ソリューションとの連携イメージ

改訂履歴

日付	版	改訂内容
2014/09/09	1.0	初版作成