Microsoft Internet Authentication Service(IAS)を使用した Unified Wireless Network での PEAP

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 表記法 PEAP の概要 設定 ネットワーク図 設定 Microsoft Windows 2003 Server の設定 Microsoft Windows 2003 Server の設定 <u>Microsoft Windows 2003 Server での DHCP サービスのインストールと設定</u> Microsoft Windows 2003 Server の認証局(CA)サーバとしてのインストールと設定 ドメインへのクライアントの接続 Microsoft Windows 2003 Server での Internet Authentication Service のインストールと証明書の要 求 Internet Authentication Service での PEAP-MS-CHAP v2 認証の設定 Active Directory へのユーザの追加 ユーザに無線アクセスを許可する Wireless LAN Controller と Lightweight AP の設定 MS IAS RADIUS サーバで RADIUS 認証を行うための WLC の設定 WLAN でのクライアントの設定 ワイヤレス クライアントの設定 ワイヤレス クライアントでの PEAP-MS-CHAP v2 認証の設定 確認とトラブルシューティング 関連情報

<u>概要</u>

このドキュメントでは、RADIUS サーバに Microsoft Internet Authentication Service(IAS)を使 用した Cisco Unified Wireless Network で Microsoft Challenge Handshake Authentication Protocol(MS-CHAP)バージョン 2 認証を使用した Protected Extensible Authentication Protocol(PEAP)を設定する際の設定例を紹介しています。

<u>前提条件</u>

<u>要件</u>

このドキュメントではテストを行うための特定の設定のみが取り上げられており、読者に Windows 2003 と Cisco コントローラのインストールに関する基本知識があることが前提となっ ています。

注:このドキュメントは、PEAP - MS CHAP認証のためにMSサーバで必要な設定の例を読者に 示すことを目的としています。このセクションで示す Microsoft サーバの設定はラボでテスト済 みで、期待通りに動作することが確認されています。Microsoft サーバを設定する上で問題がある 場合は、Microsoft に連絡してください。Cisco TAC では、Microsoft Windows サーバの設定に関 するサポートは行っていません。

Cisco 4400 シリーズ コントローラの初期インストールと設定については、『<u>クイック スタート</u> ガイド: Cisco 4400 シリーズ Wireless LAN Controller』を参照してください。

Microsoft Windows 2003 のインストールおよび設定のガイドについては、『<u>Installing Windows</u> <u>Server 2003 R2</u>』を参照してください。

開始する前に、テスト ラボの各サーバに Microsoft Windows Server 2003 SP1 のオペレーティン グシステムをインストールし、すべての Service Pack をアップデートしておいてください。コ ントローラと Lightweight Access Point(LAP; Lightweight アクセス ポイント)をインストールし 、最新のソフトウェア更新プログラムが設定されていることを確認します。

<u>使用するコンポーネント</u>

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- •ファームウェア バージョン 4.0 が稼働している Cisco 4400 シリーズ コントローラ
- Cisco 1131 Lightweight Access Point Protocol (LWAPP) AP
- Internet Authentication Service (IAS)、Certificate Authority (CA; 認証局)、DHCP、および Domain Name System (DNS; ドメイン ネーム システム)のサービスを搭載した Windows 2003 Enterprise Server (SP1)
- Windows XP Professional SP2(および最新の Service Pack)と Cisco Aironet 802.11a/b/g Wireless Network Interface Card(NIC; ネットワーク インターフェイス カード)
- Aironet Desktop Utility バージョン 4.0
- Cisco 3560 スイッチ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

<u>表記法</u>

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

<u>PEAP の概要</u>

PEAP では、Transport Level Security (TLS)を使用して、ワイヤレス ラップトップなど認証対 象の PEAP クライアントと Microsoft Internet Authentication Service (IAS) や任意の RADIUS サ ーバなどの PEAP オーセンティケータとの間に暗号化チャネルを作成します。PEAP では認証方 式は指定されませんが、PEAP により提供される TLS 暗号化チャネルで動作できる EAP-MSCHAPv2 などの他の EAP 認証プロトコルに対してセキュリティが付加されます。PEAP の認 証プロセスは、主に次の 2 つのフェーズで構成されます。

PEAPフェーズ1:TLS暗号化チャネル

ワイヤレス クライアントで AP とのアソシエーションが確立されます。IEEE 802.11 ベースの関 連付けでは、クライアントとアクセス ポイント(LAP)でセキュアなアソシエーションが確立さ れる前に、オープン システムや共有秘密鍵による認証が提供されます。クライアントとアクセス ポイントの間に IEEE 802.11 ベースのアソシエーションが確立されると、AP との TLS セッショ ンがネゴシエートされます。ワイヤレス クライアントと IAS サーバの間での認証が完了すると、 それらの間で TLS セッションがネゴシエートされます。このネゴシエーションで生成された鍵が 、後続のすべての通信の暗号化に使用されます。

PEAPフェーズ2:EAP認証通信

PEAP 認証プロセスの最初の段階で PEAP が作成した TLS チャネルで、EAP ネゴシエーション を含む EAP 通信が発生します。IAS サーバでは、EAP-MS-CHAP v2 でワイヤレス クライアント の認証が行われます。LAP とコントローラでは、ワイヤレス クライアントと RADIUS サーバの 間でのメッセージの転送だけが行われます。この WLC と LAP は TLS のエンド ポイントではな いため、これらのメッセージの復号化はできません。

PEAP のステージ 1 が発生し、IAS サーバと 802.1X ワイヤレス クライアントの間で TLS チャネ ルが作成された後、PEAP-MS-CHAP v2 でパスワード ベースの有効なクレデンシャルをユーザが 提供した成功時の認証における RADIUS のメッセージ シーケンスは次のようになります。

- 1. IAS サーバが ID 要求メッセージをクライアントに送信します(EAP-Request/Identity)。
- 2. クライアントが ID 応答メッセージを返します(EAP-Response/Identity)。
- 3. IAS サーバが MS-CHAP v2 チャレンジメッセージを送信します (EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge))。
- 4. クライアントが MS-CHAP v2 のチャレンジと応答で答えます(EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response))。
- 5. IAS サーバがクライアントの認証に成功すると、サーバが MS-CHAP v2 成功パケットを返します (EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success))。
- 6. クライアントがサーバの認証に成功すると、クライアントは MS-CHAP v2 成功パケットで 答えます(EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success))。
- 7. IAS サーバが認証の成功を示す EAP-TLV を送信します。
- 8. クライアントが EAP-TLV ステータスの成功メッセージを返します。
- 9. サーバが認証を完了し、EAP-Success メッセージをプレーン テキストで送信します。クラ イアントの分離に VLAN が展開されている場合は、このメッセージに VLAN の属性が含ま れています。

<u>設定</u>

このドキュメントでは、PEAP MS-CHAP v2 の設定例を紹介しています。

注:このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool(登

録ユーザ専用)を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセス できない場合がありますことをご了承ください。

<u>ネットワーク図</u>

このドキュメントでは、次のネットワーク セットアップを使用します。



この設定では、Microsoft Windows 2003 Server は次の役割を果たします。

- ・ドメイン Wireless.com のドメイン コントローラ
- DHCP/DNS サーバ
- 認証局(CA)サーバ
- Active Directory:ユーザデータベースの管理
- ・Internet Authentication Service(IAS): ワイヤレス ユーザの認証

図のように、このサーバはレイヤ2スイッチを介して有線ネットワークに接続しています。

Wireless LAN Controller(WLC)と登録済み LAP もレイヤ 2 スイッチを介してネットワークに接続しています。

ワイヤレス クライアント C1 と C2 は、Wi-Fi Protected Access 2(WPA 2)- PEAP MSCHAP v2 認証を使用してワイヤレス ネットワークに接続しています。

目標は、PEAP MSCHAP v2 認証でワイヤレス クライアントを認証するように、Microsoft 2003 Server、Wireless LAN Controller、および Light Weight AP を設定することです。

次のセクションでは、この構成でデバイスを設定する方法を説明します。

<u>設定</u>

このセクションでは、この WLAN に PEAP MS-CHAP v2 認証を設定するために必要な設定を確認しています。

- Microsoft Windows 2003 Server の設定
- ・Wireless LAN Controller (WLC)と Light Weight AP の設定
- ワイヤレス クライアントの設定

Microsoft Windows 2003 Server の設定から始めます。

<u>Microsoft Windows 2003 Server の設定</u>

<u>Microsoft Windows 2003 Server の設定</u>

ネットワーク設定のセクションで説明されているように、Microsoft Windows 2003 Server はネッ トワークで次の機能を行うために使用されます。

- ・ドメイン コントローラ:ドメイン Wireless 用
- ・DHCP/DNS サーバ
- 認証局 (CA) サーバ
- Internet Authentication Service (IAS) : ワイヤレス ユーザの認証
- Active Directory : ユーザ データベースの管理

Microsoft Windows 2003 Server を、上記のサービスを行うように設定します。ドメイン コント ローラとしての Microsoft Windows 2003 Server の設定から開始します。

ドメイン コントローラとしての Microsoft Windows 2003 Server の設定

Microsoft Windows 2003 Server をドメイン コントローラとして設定するには、次の手順を実行します。

1. **Start、Run** の順にクリックし、dcpromo.exe と入力して **OK** をクリックし、Active Directory Installation Wizard を起動します。



2. Next をクリックして Active Directory Installation Wizard を実行します。

rity settings in Windows S	erver 2003 affect older versions of	R.
lers running Windows Ser and other servers to comm	ver 2003 implement security settings that nunicate with those domain controllers in .	a more
sions of Windows, includi neet these requirements. X and SAMBA clients, mi	ng Windows 95 and Windows NT 4.0 SF Similarly, some non-Windows systems, inc ght not meet these requirements.	23 or Iuding
nation, see <u>Compatibility H</u>	<u>elp</u> .	

3. 新しいドメインを作成するため、オプション Domain Controller for a new domain を選択し ます。

Specify	the role you want this server to have.
Do you additior	want this server to become a domain controller for a new domain or an al domain controller for an existing domain?
• Dor	nain controller for a new domain
Sel Thi	ect this option to create a new child domain, new domain tree, or new forest. s server will become the first domain controller in the new domain.
	litional domain controller for an existing domain
⚠	Proceeding with this option will delete all local accounts on this server.
	All cryptographic keys will be deleted and should be exported before continuing.
	All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.

4. New をクリックし、ドメイン ツリーの新しいフォレストを作成します。

Active Directory Installation Wizard	×
Create New Domain Select which type of domain to create.	
Create a new:	
Domain in a new forest	
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.	
Child domain in an existing domain tree	
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.	
O Domain tree in an existing forest	
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.	
< <u>B</u> ack <u>N</u> ext > Cancel	

5. システムに DNS がインストールされていない場合は、ウィザードにより DNS を設定する ためのオプションが提示されます。このコンピュータでは No, Just Install and Configure DNS を選択します。[next] をクリックします。

Active Directory Installation Wizard	×
Install or Configure DNS You can configure or install Domain Naming Service (DNS) on this com	nputer.
Domain Naming Service (DNS) is not configured on this computer. Is D running on this network?	NS already
Yes, I will configure the DNS client	
No, just install and configure DNS on this computer	
< <u>B</u> ack <u>N</u> ext (> Cancel

6. 新しいドメインの完全な DNS 名を入力します。この例では、Wireless.com が使用されており、Next をクリックします。

Directory Installation Wizard			
ew Domain Name Specify a name for the new domain.			SA CONTRACTOR
Type the full DNS name for the new dom (for example: headquarters.example.micr	ain osoft.com).		
Eull DNS name for new domain:			
Wireless.com			8
	(Pack	Neuts	

7. ドメインの NETBIOS 名を入力し、**Next** をクリックします。この例では **WIRELESS** を使用 しています。

ctive Directory Installation Wi	zard	2
NetBIOS Domain Name Specify a NetBIOS name for	the new domain.	X
This is the name that users o domain. Click Next to accept	f earlier versions of Windows will use to identify the new t the name shown, or type a new name.	
Domain NetBIOS name:	WIRELESS	[
	< <u>B</u> ack <u>N</u> ext > Can	cel

8. ドメインのデータベースとログのロケーションを選択します。[next] をクリックします。

e Directory Installation Wizard		
atabase and Log Folders Specify the folders to contain the Active Directory dat	abase and log file	s. S
For best performance and recoverability, store the dat hard disks.	abase and the log	j on separate
Where do you want to store the Active Directory data	base?	
<u>D</u> atabase folder:		
C:\WINDOWS\NTDS		Browse
Where do you want to store the Active Directory log?		
C:\WINDOWS\NTDS		Browse
1		I

9. Sysvol フォルダのロケーションを選択します。[next] をクリックします。

em volume.	Star Star
y of the domain's public file: Iomain controllers in the dom	s. The contents nain.
NTFS volume.	
	B <u>r</u> owse
	B <u>r</u> owse
< Back Next	> Cance
	y of the domain's public files lomain controllers in the dom NTFS volume. ≺ <u>B</u> ack <u>N</u> ext

ennissions				
Select default permissions fo	r user and group obj	ects.		
Some server programs, such stored on domain controllers.	as Windows NT Re	mote Acces	ss Service, read	informatio
Permissions compatible v	with pre-Windows 20	00 server op	perating systems	
Select this option if you r systems or on Windows members of pre-Window	un server programs o 2000 or Windows Se s 2000 domains.	on pre-Wind rver 2003 o	lows 2000 server operating systems	r operatir s that are
🔥 Anonymous users (can read information	on this dom	iain.	
 Permissions compatible of operating systems 	only with Windows 20)00 or Wind	lows Server 200	3
Select this option if you r Server 2003 operating sy authenticated users can	un server programs o vstems that are memb read information on t	only on Wind bers of Activ his domain.	dows 2000 or W /e Directory dom	indows ains. Onl
		< <u>B</u> ack	<u>N</u> ext>	Lõ
		< <u>B</u> ack	<u>N</u> ext >	Lå
音のパスワードを設定し、N	lext をクリックし	く <u>B</u> ack ます。	<u>N</u> ext>	
音のパスワードを設定し、N re Directory Installation W	lext をクリックし izard	< <u>B</u> ack ます。	<u>N</u> ext >	
音のパスワードを設定し、N re Directory Installation W Pirectory Services Restore	lext をクリックし izard Mode Administral	< <u>B</u> ack ます。 tor Passw	ord	
音のパスワードを設定し、N e Directory Installation W F irectory Services Restore This password is used when Mode.	lext をクリックし izard Mode Administral you start the compu	< <u>B</u> ack ます。 tor Passw terin Direct	ord cory Services Re:	store
音のパスワードを設定し、N re Directory Installation W Pirectory Services Restore This password is used when Mode.	lext をクリックし izard Mode Administral you start the compu	く <u>B</u> ack ます。 t or Passw ter in Direct	ord tory Services Re:	store
そのパスワードを設定し、N e Directory Installation W Pirectory Services Restore This password is used when Mode. Type and confirm the passw when this server is started in	lext をクリックし izard Mode Administrat you start the compu ord you want to assig Directory Services F	く <u>B</u> ack ます。 tor Passw ter in Direct gn to the Ad	ord tory Services Read Iministrator accord	store
着のパスワードを設定し、N e Directory Installation W Pirectory Services Restore This password is used when Mode. Type and confirm the passw when this server is started in The restore mode Administra account. The passwords for both.	lext をクリックし izard Mode Administrat you start the compu ord you want to assig Directory Services F tor account is differe the accounts might t	< <u>B</u> ack ます。 tor Passw ter in Direct gn to the Ad lestore Mod nt from the be different,	<u>N</u> ext> ord tory Services Rea dministrator accor de. domain Administr so be sure to re	store unt used rator member
きのパスワードを設定し、N e Directory Installation W Firectory Services Restore This password is used when Mode. Type and confirm the passw when this server is started in The restore mode Administra account. The passwords for both. Restore Mode Password:	lext をクリックし izard Mode Administrat you start the computed ord you want to assig Directory Services F tor account is different the accounts might t	< <u>B</u> ack ます。 tor Passw ter in Direct gn to the Ad lestore Moo nt from the be different,	ord tory Services Read dministrator accorde. domain Administrator accorde.	store unt used rator member
きのパスワードを設定し、N e Directory Installation W Firectory Services Restore This password is used when Mode. Type and confirm the passw when this server is started in The restore mode Administra account. The passwords for both. Restore Mode Password: Confirm password:	lext をクリックし izard Mode Administrat you start the computed ord you want to assig Directory Services F tor account is different the accounts might the accounts might	< <u>B</u> ack ます。 tor Passw ter in Direct gn to the Ad estore Moo nt from the be different,	ord tory Services Rea dministrator account de. domain Administrator account so be sure to re	store unt used rator member
きのパスワードを設定し、N e Directory Installation W Firectory Services Restore This password is used when Mode. Type and confirm the passw when this server is started in The restore mode Administra account. The passwords for both. Restore Mode Password: Confirm password: For more information about D	Iext をクリックし izard Mode Administrat you start the computed ord you want to assign Directory Services Fitter the account is different the accounts might the accounts	< <u>B</u> ack ます。 tor Passw ter in Direct gn to the Ad estore Mode	<u>Next</u> > ord tory Services Rea diministrator accorde. domain Administr so be sure to re	store unt used rator member
着のパスワードを設定し、N re Directory Installation W Directory Services Restore This password is used when Mode. Type and confirm the passw when this server is started in The restore mode Administra account. The passwords for both. Restore Mode Password: Confirm password: For more information about D	Iext をクリックし izard Mode Administrate you start the compu- ord you want to assig Directory Services Fi tor account is different the accounts might to ooccounts might to ooccounts might to ooccounts might to ooccounts might to ooccounts might to	< <u>B</u> ack ます 。 tor Passw ter in Direct gn to the Ad restore Mode estore Mode	<u>N</u> ext > ord tory Services Read diministrator accord de. domain Administr so be sure to re	store

12. Next をクリックして、先ほど設定したドメインのオプションを承認します。

iun	imary
	Review and confirm the options you selected.
	You chose to:
	Configure this server as the first domain controller in a new forest of domain trees.
	The new domain name is Wireless.com. This is also the name of the new forest.
	The NetBIOS name of the domain is WIRELESS
	Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL
	The password of the new domain administrator will be the same as the password of the administrator of this computer.
	To change an option, click Rack. To begin the operation, click Nevt

13. Finish をクリックして Active Directory Installation Wizard を閉じます。

Active Directory Installation	Wizard 🔀
	Completing the Active Directory Installation Wizard
	Active Directory is now installed on this computer for the 💻 domain Wireless.com.
	This domain controller is assigned to the site Default-First-Site-Name. Sites are managed with the Active Directory Sites and Services administrative tool.
	To close this wizard, click Finish.
	< <u>B</u> ack Finish Cancel
サーバを再起動して変更を有햧	かにします。
Active Directory Installation	Wizard
Windows must be restarted before Directory Installation wizard take	ore the changes made by the Active e effect.

この手順では、Microsoft Windows 2003 Server をドメイン コントローラとして設定し、新しい ドメイン **Wireless.com** を作成しました。次に、サーバ上に DHCP サービスを設定します。

Don't Restart Now

<u>Microsoft Windows 2003 Server での DHCP サービスのインストールと設定</u>

Microsoft 2003 Server 上の DHCP サービスは、ワイヤレス クライアントに IP アドレスを提供す るために使用されます。DHCP サービスをサーバにインストールし設定するには、次の手順を実 行します。

- 1. Control Panel で Add or Remove Programs をクリックします。
- 2. Add/Remove Windows components をクリックします。

Restart Now

- 3. Networking Services を選択し、Details をクリックします。
- 4. Dynamic Host Configuration Protocol (DHCP) を選択し、OK をクリックします。

 Domain Name System (DNS) Dynamic Host Configuration Protocol (DHCP) Internet Authentication Service Internet Authentication Service Remote Access Quarantine Service RPC over HTTP Proxy Simple TCP/IP Services Windows Internet Name Service (WINS) Serviption: Sets up a DHCP server that automatically assigns temporary IP addresses to client computers on the same network. tal disk space required: 3.4 MB Details 	ub <u>c</u> omponents of Networking Services:	
Internet Authentication Service 0.0 MB Internet Authentication Service 0.0 MB Remote Access Quarantine Service 0.1 MB RPC over HTTP Proxy 0.0 MB Simple TCP/IP Services 0.0 MB Windows Internet Name Service (WINS) 0.9 MB scription: Sets up a DHCP server that automatically assigns temporary IP addresses to client computers on the same network. tal disk space required: 3.4 MB Details	🛛 🚐 Domain Name System (DNS)	1.7 MB 🔺
 Internet Authentication Service Remote Access Quarantine Service RPC over HTTP Proxy Simple TCP/IP Services Windows Internet Name Service (WINS) Windows Internet Name Service (WINS) Scription: Sets up a DHCP server that automatically assigns temporary IP addresses to client computers on the same network. tal disk space required: 3.4 MB Details 	🛛 😓 Dynamic Host Configuration Protocol (DHCP)	0.0 MB
 Remote Access Quarantine Service RPC over HTTP Proxy Simple TCP/IP Services Windows Internet Name Service (WINS) Windows Internet Name Service (WINS) Sets up a DHCP server that automatically assigns temporary IP addresses to client computers on the same network. tal disk space required: 3.4 MB Details 	🗌 畏 Internet Authentication Service	0.0 MB
RPC over HTTP Proxy 0.0 MB Simple TCP/IP Services 0.0 MB Windows Internet Name Service (WINS) 0.9 MB scription: Sets up a DHCP server that automatically assigns temporary IP addresses to client computers on the same network. tal disk space required: 3.4 MB Details 2224 5 MB	🗌 🚚 Remote Access Quarantine Service	0.1 MB
Simple TCP/IP Services 0.0 MB Windows Internet Name Service (WINS) 0.9 MB scription: Sets up a DHCP server that automatically assigns temporary IP addresses to client computers on the same network. tal disk space required: 3.4 MB	🛛 🚚 RPC over HTTP Proxy	0.0 MB
Windows Internet Name Service (WINS) 0.9 MB scription: Sets up a DHCP server that automatically assigns temporary IP addresses to client computers on the same network. tal disk space required: 3.4 MB Details	🛛 🚚 Simple TCP/IP Services	0.0 MB
scription: Sets up a DHCP server that automatically assigns temporary IP addresses to client computers on the same network. tal disk space required: 3.4 MB 	🛛 🚚 Windows Internet Name Service (WINS)	0.9 MB 👱
tal disk space required: 3.4 MB Details	escription: Sets up a DHCP server that automatica addresses to client computers on the sa	ally assigns temporary IP ame network.
ace available on disk: 7224.5 MB	otal disk space required: 3.4 MB	Details
ace available of rusk. (224.3 MD	pace available on disk: 7224.5 MB	25 245 (2019) VI

5. Next をクリックして DHCP サービスをインストールします。

You can add or remove components of Windows.	
To add or remove a component, click the checkbox. A shaded box part of the component will be installed. To see what's included in a Details.	r means that only component, click
Components:	
🔲 🥶 Internet Explorer Enhanced Security Configuration	0.0 MB 📐
🗔 🚔 Management and Monitoring Tools	6.3 MB
🗹 🚆 Networking Services	2.7 MB
🔲 🚔 Other Network File and Print Services	0.0 MB
🖂 📾 Bemote Storage	4.2 MB 💻
Description: Contains a variety of specialized, network-related serv Total disk space required: 3.4 MB Space available on disk: 7212.1 MB	rices and protocols. Details

6. [Finish] をクリックしてインストールを完了します。



- 7. DHCP サービスを設定するため、Start > Programs > Administrative tools の順にクリックし、DHCP スナップインをクリックします。
- 8. DHCP サーバ(この例では tsweb-lapt.wireless.com)を選択します。
- 9. Action をクリックし、Authorize をクリックして DHCP サービスを認可します。



- 10. コンソール ツリーで tsweb-lapt.wireless.com を右クリックし、New Scope をクリックし 、ワイヤレス クライアントの IP アドレスの範囲を定義します。
- 11. New Scope Wizard の Welcome to the New Scope Wizard ページで、Next をクリックします。



12. Scope Name ページで、DHCP のスコープ名を入力します。この例では、スコープ名に DHCP-Clients を使用します。[next] をクリックします。

Scope Wizard	
Scope Name You have to p providing a de:	ovide an identifying scope name. You also have the option of scription.
Type a name a how the scope	nd description for this scope. This information helps you quickly identify is to be used on your network.
N <u>a</u> me:	DHCP-Clients
Description:	DHCP Server for Wireless Clients
	Z Back Nevt > Cancel

13. IP Address Range ページで、範囲の最初と最後の IP アドレスを入力し、**Next** をクリックします。

IP Address Range You define the sco addresses.	pe address range by identifying a set of consecutive IP
Enter the range of a	addresses that the scope distributes.
<u>S</u> tart IP address	10 . 77 . 244 . 218
End IP address:	10 . 77 . 244 . 219
A subnet mask defi	nes how many hits of an IP address to use for the network /subnet
IDs and how many length or as an IP a Length:	bits to use for the host ID. You can specify the subnet mask by address.
IDs and how many length or as an IP a Length: S <u>u</u> bnet mask:	bits to use for the host ID. You can specify the subnet mask by address.
IDs and how many length or as an IP a Length: S <u>u</u> bnet mask:	bits to use for the host ID. You can specify the subnet mask by address.

14. Add Exclusions ページで、DHCP スコープから留保または除外する IP アドレスを指定し ます。[next] をクリックします。

Exclusions are address server.	esses or a range of addresses that are not distributed by the
Type the IP address address, type an ad	range that you want to exclude. If you want to exclude a single dress in Start IP address only.
<u>S</u> tart IP address:	End IP address:
	A <u>d</u> d
Excluded address ra	inge:
	Remo <u>v</u> e
I	
	< Back Next > Cance
	· David Monte Carlos

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:



<u>N</u>ext>

16. Configure DHCP Options ページで Yes, I want to configure DHCP Option now を選択し、 Next をクリックします。

New Scope Wizard
Configure DHCP Options You have to configure the most common DHCP options before clients can use the scope.
When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.
Do you want to configure the DHCP options for this scope now?
Yes, I want to configure these options now
No, I will configure these options later
< <u>B</u> ack <u>N</u> ext > Cancel

17. デフォルトのゲートウェイ ルータがある場合は、Router(Default Gateway)ページでその ゲートウェイ ルータの IP アドレスを指定し、Next をクリックします。

To add an IP addres	for a router used by clients, enter the add	dress below.
	Add	
10.77.244.220	<u>H</u> emove	
	Цр	
	Down	

18. Domain Name and DNS Servers ページで、先ほど設定したドメインの名前を入力します 。この例では、**Wireless.com** を使用します。サーバの IP アドレスを入力します。[Add] を クリックします。

Domain Name and DNS Servers The Domain Name System (DNS) maps clients on your network.	and translates domain name:	s used by
You can specify the parent domain you want DNS name resolution.	t the client computers on your	network to use for
Parent do <u>m</u> ain: Wireless.com		
To configure scope clients to use DNS serve servers.	ers on your network, enter the	e IP addresses for thos
<u>S</u> erver name:	I <u>P</u> address:	A <u>d</u> d
<u>S</u> erver name: R <u>e</u> solve	I <u>P</u> address:	A <u>d</u> d <u>B</u> emove
<u>S</u> erver name: R <u>e</u> solve	I <u>P</u> address:	A <u>d</u> d <u>R</u> emove Up
<u>S</u> erver name: R <u>e</u> solve	I <u>P</u> address:	A <u>d</u> d <u>R</u> emove Up D <u>o</u> wn

- 19. [next] をクリックします。
- 20. WINS Server ページで **Next** をクリックします。
- 21. Activate Scope ページで **Yes, I want to activate the scope now** を選択し、**Next** をクリックします。

Activate Scope Clients can obtain address leases only if a s	cope is activate	d.	L.
Do you want to activate this scope now?			
Yes, I want to activate this scope now			
C No, I will activate this scope later			
	< Back	Next>	Cancel

22. New Scope Wizard を終了するため、Finish をクリックします。



23. DHCP Snapin ウィンドウで、作成した DHCP スコープがアクティブであることを確認します。

Artist View Links				الم ا
	la:			
HP	towh-lapt wireless cam [10.77.211.2	1171		
Surficiant on electron (10,77,244,217)	Carters of DHER Serve	Status	Description	
- B Server Optione	Scope [172, 56.0.0] DHCP-Clients	** Artise **	DHCP Server for Wireless Clients	
	1 Down			

これで、サーバ上で DHCP/DNS がイネーブルになったので、サーバをエンタープライズの認証 局(CA)サーバとして設定します。

<u>Microsoft Windows 2003 Server の認証局(CA)サーバとしてのインストールと設</u> 定

EAP-MS-CHAPv2を使用するPEAPは、サーバ上にある証明書に基づいてRADIUSサーバを検証し ます。また、クライアントコンピュータの信頼するパブリックな Certification Authority (CA)が サーバ証明書を発行する必要があります(つまり、パブリックな CA 証明書がクライアント コン ピュータの証明書ストアの Trusted Root Certification Authority フォルダにすでに存在する必要が あります)。この例では、Internet Authentication Service (IAS)へ証明書を発行する認証局 (CA)として、Microsoft Windows 2003 Server を設定します。

サーバ上に証明書サービスをインストールして設定するには、次の手順を実行します。

- 1. Control Panel で Add or Remove programs をクリックします。
- 2. Add/Remove Windows components をクリックします。
- 3. Certificate Services をクリックします。

indows Components You can add or remove components of Windows.	
To add or remove a component, click the checkbox. A s part of the component will be installed. To see what's inc Details.	haded box means that only luded in a component, click
Components:	
🗹 📻 Accessories and Utilities	4.9 MB 🔺
🛛 🗹 🧃 Application Server	34.4 MB 💻
🗹 😰 Certificate Services	1.8 MB
🗌 🛄 E-mail Services	1.1 MB
Eax Services	7.9 MR 💻
Description: Installs a certification authority (CA) to issue public key security programs.	certificates for use with
Total disk space required: 13.8 MB	Dataile
Space available on disk: 7310.6 MB	

4. ^CAfter Installing Certificate Services, the computer cannot be renamed and the computer cannot join or be removed from a domain.Do you want to continue?

Microsof	it Certificate Services
⚠	After installing Certificate Services, the machine name and domain membership may not be changed due to the binding of the machine name to CA information stored in the Active Directory. Changing the machine name or domain membership would invalidate the certificates issued from the CA. Please ensure the proper machine name and domain membership are configured before installing Certificate Services. Do you want to continue?
	<u>Yes</u> <u>N</u> o

5. Certificate Authority Type で Enterprise root CA を選択し、Next をクリックします。

dows	Components Wizard
CA Ty Se	pe elect the type of CA you want to set up.
c	Enterprise root CA
C	Enterprise subordinate CA
C	Stand-alone root CA
С	Stand-alone subordinate CA
	rescription of CA type 'he most trusted CA in an enterprise. Should be installed before any other CA.
	Use custom settings to generate the key pair and CA certificate

6. CA を識別する名前を入力します。この例では Wireless-CA を使用しています。[next] をクリックします。

Enter information to ider	ntify this CA.	Ľ
Common name for this CA:		
Wireless-CA		
Distinguished name suffix:		
DC=Wireless,DC=com		
Preview of distinguished na	ime:	
CN=Wireless-CA,DC=Wirel	less,DC=com	
Validity period:	Expiration date:	
5 Years 🔻	12/12/2012 7:01 PM	

7. 証明書データベース ストレージとして CertLog ディレクトリが作成されます。[next] をクリ ックします。

Се	rtificate Database Settings Enter locations for the certificate database, database log, and configura	ation
	Certificate database:	 1
	L:\WINDUW5\system32\LertLog	Browse
	Certificate database log:	
	C:\WINDOWS\system32\CertLog	Bro <u>w</u> se
	Preserve existing certificate database	Blowse

THE GREET	
	To complete the installation, Certificate Services must temporarily stop the Internet Information Services. Do you want to stop the service now?
	<u>Y</u> es <u>N</u> o

9. Finish をクリックして、認証局(CA)サービスのインストールを完了します。

Windows Components Wizard		×
	Completing the Windows Components Wizard You have successfully completed the Windows Components Wizard.	
	To close this wizard, click Finish.	
	< Back Finish	Help

次の手順では、Microsoft Windows 2003 Server に Internet Authentication Service をインストール して設定します。

<u>ドメインへのクライアントの接続</u>

次の手順では、クライアントを有線ネットワークに接続させ、新しいドメインからドメイン固有 の情報をダウンロードします。つまり、クライアントをドメインに接続させます。このためには 、次の手順を実行します。

- 1. ストレート型のイーサネット ケーブルでクライアントを有線ネットワークに接続します。
- 2. クライアントを起動し、そのクライアントのユーザ名/パスワードでログインします。
- 3. Start、Run の順にクリックし、cmd と入力して、OK をクリックします。
- 4. コマンド プロンプトで ipconfig と入力し、Enter をクリックして、DHCP が正常に動作しク ライアントが DHCP サーバから IP アドレスを受け取ったことを確認します。
- 5. クライアントをドメインに参加させるため、My Computer を右クリックし、**Properties** を選 択します。
- 6. [Computer Name]タブをクリックします。
- 7. [Change] をクリックします。
- 8. Domain をクリックし、wireless.com と入力し、OK をクリックします。

Computer Name Changes 🛛 🛛 🔀
You can change the name and the membership of this computer. Changes may affect access to network resources.
Computer name:
Client1
Full computer name: Client1. More
O Domain:
Wireless
O Workgroup:
WORKGROUP
OK Cancel

9. Username に Administrator と入力し、クライアントが参加するドメインのパスワードを入力します。(これはサーバ上での Active Directory の管理者アカウントです。

	- cumPer	
Enter the name a	nd password of an account w	ith permission
to join the domain	1.	
Licer name:	G administrator	
goor name.		X



- 10. [OK] をクリックします。
- 11. [Yes] をクリックしてコンピュータを再起動させます。
- 12. コンピュータが再起動したら、次の情報でログインします。ユーザ名= Administrator、パ スワード= <domain password>、ドメイン= Wireless。
- 13. My Computer を右クリックし、Properties をクリックします。
- 14. <u>Computer Name タブをクリックし、Wireless.com ドメインにいることを確認</u>します。

ystem Proper	ties			? 🔀	
System Restore		Automatic Updates		Remote	
General	Compu	iter Name	Hardware	Advanced	
Wind on th Computer <u>d</u> esc	dows uses t ne network. ription:	ne following inf	ormation to identify	your computer	
		For example: "I Computer".	Kitchen Computer''	or ''Mary's	
Full computer r	iame:	Client1.Wireles	s.com		
Domain:		Wireless.com			
domain and cre ID.	ate a local	user account,	click Network	<u>N</u> etwork ID	
To rename this	computer o	r join a domain	, click Change.	Change	
🔥 Changes	will take eff	ect after you re	estart this computer.		
		ОК	Cance		

- 15. 次の手順では、クライアントがサーバから CA 証明書(信頼)を受信したことを確認しま す。
- 16. Start、Run の順にクリックし、mmc と入力して、OK をクリックします。
- 17. [File] をクリックし、[Add/Remove] スナップインをクリックします。

dd/Remove Snap	-in	? >
Standalone Extensi	ons	
Use this page to ad	d or remove a standalone Snap-in from the cons	ole.
Snap-ins added to:	🔄 Console Root	
Description		
	Remove Abové	
Add	Remove About	

- 18. [Add] をクリックします。
- 19. Certificate を選択し、Add をクリックしします。
Add Standalone Snap-in

Snap-in	Vendor	^
🏡 .NET Framework 1.1 Configuration	Microsoft Corporation	
🖞 ActiveX Control	Microsoft Corporation	
Certificates	Microsoft Corporation	
Component Services	Microsoft Corporation	
🛃 Computer Management	Microsoft Corporation	
💐 Device Manager	Microsoft Corporation	
👺 Disk Defragmenter	Microsoft Corp, Executi	
👹 Disk Management	Microsoft and VERITAS	
🔟 Event Viewer	Microsoft Corporation	
Folder	Microsoft Corporation	Y
		888
Description he Certificates snap-in allows you to bro ertificate stores for yourself, a service, o	wse the contents of the r a computer.	

?

20. Computer account を選択し、Next をクリックします。

This snap-in will always manage certificates for:	
O My user account	
O Service account	
 Computer account 	
	< Back Next > Ca

elect the computer you wa	anicinis snaphinito manage.
This snap-in will always ma	anage:
 Local computer: (the 	computer this console is running on)
Another computer:	Browse
only applies if you say	ve the console.

22. Close をクリックし、OK をクリックします。

23. Certificates (Local Computer)、Trusted Root Certification Authorities の順に展開し、

Certificates をクリックします。リストから Wireless を探します。

Console Root	Issued To /	Issued By	Expiration Date	Intended Purposes	Friendly Name
Certificates (Local Computer)	SERVICIOS DE CERTIFICACION	SERVICIOS DE CERTIFICACION - A	3/10/2009	Secure Email, Server	SERVICIOS DE CERT
E - Personal	SIA Secure Client CA	51A Secure Client CA	7/9/2019	Secure Email, Server	Societa Interbancari
E- Trusted Root Certification Author	SIA Secure Server CA	SIA Secure Server CA	7/9/2019	Secure Email, Server	Societa Interbancari
Certificates	Setsskey Root CA	Swisskey Root CA	1/1/2016	Secure Email, Server	Seeskey Root CA
Enterprise Trust	Symantec Root CA	Symantec Root CA	5/1/2011	<al></al>	<none></none>
Intermediate Certrication Author	TC TrustCenter Class I CA	TC TrustCenter Class 1 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas
Interested Cartification	TC TrustCenter Class 2 CA	TC TrustCenter Class 2 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas
H-10 Third-Party Boot Certification Au	TC TrustCenter Class 3 CA	TC TrustCenter Class 3 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas
H-M Trusted People	TC TrustCenter Class 4 CA	TC TrustCenter Class 4 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas
H- m SPC	TC TrustCenter Time Stamping CA	TC TrustCenter Time Stamping CA	1/1/2011	Time Stamping	TC TrustCenter Time
_	Thavte Personal Basic CA	Thavite Personal Basic CA	1/1/2021	Client Authentication	Thavke Personal Bas
	Thawte Personal Freemail CA	Thawte Personal Freemail CA	1/1/2021	Client Authentication	Thavke Personal Fre
	Thavte Personal Premium CA	Thavite Personal Premium CA	1/1/2021	Client Authentication	Thavke Personal Pre
	Thawte Premium Server CA	Thavite Premium Server CA	1/1/2021	Server Authenticatio	Thavke Premium Ser
	Thawte Server CA	Thante Server CA	1/1/2021	Server Authenticatio	Thavke Server CA
	Thavte Timestamping CA	Thavite Timestamping CA	1/1/2021	Time Stamping	Thavke Timestampin
	UTN - DATACorp SGC	UTN - DATACorp SGC	6/25/2019	Server Authentication	UTN - DATACorp SGC
	UTN-USERFirst-Client Authenticati	UTN-USERFirst-Client Authentication	7/9/2019	Secure Email	UTN - USERFirst-Cle
	UTN-USERFirst-Hardware	UTN-USER/First-Hardware	7/9/2019	Server Authentication	UTN - USERFirst-Har
	UTN-USERFirst-Network Applications	UTN-USERFirst-Network Applications	7/10/2019	Secure Email, Server	UTN - USERFirst-Net
	UTN-USERFirst-Object	UTN-USER/First-Object	7/10/2019	Time Stamping, Code	UTN - USERFirst-Object
	VeriSign Commercial Software Publ	VeriSign Commercial Software Publis	12/31/1999	Secure Email, Code S	VeriSign Commercial
	VeriSign Commercial Software Publ	VertSign Commercial Software Publis	1/8/2004	Secure Email, Code S	VeriSign Commercial
	VeriSign Individual Software Publis	VertSign Individual Software Publishe	12/31/1999	Secure Email, Code S	VeriSign Individual S
	VeriSign Individual Software Publis	VeriSign Individual Software Publishe	1/8/2004	Secure Email, Code S	VeriSign Individual S
	Veri5ign Trust Network	VertSign Trust Network	5/19/2018	Secure Enail, Clent	Veri5ign Class 2 Prim
	VeriSign Trust Network	VeriSign Trust Network	8/2/2028	Secure Email, Client	VeriSign Class 2 Prim
	Veri5ign Trust Network	VertSign Trust Network	5/19/2018	Secure Email, Clent	Veri5ign Class 3 Prim
	VeriSign Trust Network	VeriSign Trust Network	8/2/2028	Secure Email, Client	VeriSign Class 3 Prim
	VeriSign Trust Network	VertSign Trust Network	5/19/2018	Secure Email, Client	VeriSign Class 4 Prim
	VeriSign Trust Network	VeriSign Trust Network	8/2/2028	Secure Email, Client	VeriSign Class 1 Prim
	VeriSign Trust Network	VertSign Trust Network.	8/2/2028	Secure Email, Clent	VeriSign Class 4 Prim
	VeriSign Trust Network	VeriSign Trust Network	5/19/2018	Secure Email, Client	VeriSign Class 1 Prim
	E Wreless-CA	Wireless-CA	12/17/2012	<al></al>	<hkme></hkme>
	Dicert EZ by DST	Xcert EZ by DST	7/11/2009	Secure Email, Server	Xcert EZ by DST
Sector Se	 nabadadadanakadadadadadada 			odesta de la companya	Activity of the second second

24. 別のクライアントをさらにドメインに追加するには、この手順を繰り返します。

<u>Microsoft Windows 2003 Server での Internet Authentication Service のインストールと証明書の要求</u>

この設定では、PEAP 認証を使用してワイヤレス クライアントを認証するために、Internet Authentication Service(IAS)を RADIUS サーバとして使用します。

次の手順を実行して、サーバ上に IAS をインストールして設定します。

- 1. Control Panel で Add or Remove Programs をクリックします。
- 2. Add/Remove Windows components をクリックします。
- 3. Networking Services を選択し、Details をクリックします。
- 4. Internet Authentication Service を選択し、OK をクリックし、Next をクリックします。

etworking Services]
To add or remove a comp of the component will be i	onent, click the check b nstalled. To see what's in	ox. A shaded box me cluded in a compon	eans that only j ent, click Deta	bart ils.
Sub <u>c</u> omponents of Netwo	orking Services:			
🗹 🚚 Domain Name Sy	stem (DNS)		1.7 MB	•
🗹 🚚 Dynamic Host Co	nfiguration Protocol (DHC	P)	0.0 MB	
🗹 畏 Internet Authentic	ation Service		0.0 MB	
🗆 🚚 Remote Access (Juarantine Service		0.1 MB	
🗆 🚚 RPC over HTTP I	Ргоху		0.0 MB	
🔲 🚚 Simple TCP/IP S	ervices		0.0 MB	_
🔲 🚚 Windows Internet	Name Service (WINS)		0.9 MB	-
Description: Enables au users, IAS	uthentication, authorizatio supports the RADIUS pro	n and accounting of stocol.	dial-up and VF	PN
Total disk space required	3.4 MB		Details	
Space available on disk:	7208.2 MB		<u>Potens</u> .	
		OK	Cancel	

5. Finish をクリックして、IAS のインストールを完了します。



- 6. 次の手順では、Internet Authentication Service(IAS)に対応するコンピュータの証明書をインストールします。
- 7. <u>Start、Run</u>の順にクリックし、mmcと入力して、OKをクリックします。

le lation view	Envarites Window Help		ala -
+ 10 2 0	₹ E		
ansole Foot	Norec		
		There are no items to shave in this view.	
	1		
	1		
1 6	Network Connections	DHC? 🕺 dranget - [DH2],12400 🕸 Interest Authentication 👔 Consolet - [Co	nsele R., 🛛 🖉 🖉 🐼 👯 🕅 🕅 🕅 🕅

8. ファイル メニューで Console をクリックし、Add/Remove スナップインを選択します。 9. Add をクリックし、スナップインを追加します。

Add/Remove Snap-in	? ×
Standalone Extensions	
Use this page to add or remove a stand-alone snap-in from the console	e.
Snap-ins added to: Console Root	
Description	
A <u>d</u> d <u>R</u> emove A <u>b</u> out	
ОК СА	ancel

10. スナップインのリストから Certificates を選択し、Add をクリックしします。

ānap-in	Vendor	
💑 .NET Framework 1.1 Configuration	Microsoft Corporation	
Active Directory Domains and Trusts	Microsoft Corporation	
Active Directory Sites and Services	Microsoft Corporation	
炎 Active Directory Users and Compu	Microsoft Corporation	
📺 ActiveX Control	Microsoft Corporation	
🖗 ADSI Edit	Microsoft Corporation	
🛵 Authorization Manager	Microsoft Corporation	
🕵 Certificate Templates	Microsoft Corporation	
Certificates	Microsoft Corporation	
Certification Authority	Microsoft Corporation	-
he Certificates snap-in allows you to br ertificate stores for yourself, a service,	owse the contents of the or a computer.	
he Certificates snap-in allows you to br ertificate stores for yourself, a service,	owse the contents of the or a computer. <u>A</u> dd <u>C</u> lo	se
he Certificates snap-in allows you to br ertificate stores for yourself, a service, puter account を選択し、Next をク	owse the contents of the or a computer. <u>A</u> ddo リックします。	se
he Certificates snap-in allows you to br ertificate stores for yourself, a service, puter account を選択し、Next をク :ificates snap-in	owse the contents of the or a computer. <u>A</u> dd <u>C</u> lo リックします。	se
he Certificates snap-in allows you to br ertificate stores for yourself, a service, puter account を選択し、Next をク ificates snap-in	owse the contents of the or a computer. <u>A</u> dd <u>C</u> o リックします。	se
he Certificates snap-in allows you to br ertificate stores for yourself, a service, puter account を選択し、Next をク ificates snap-in This snap-in will always manage certificates	owse the contents of the or a computer. <u>A</u> dd <u>C</u> lo リックします。 for:	se
he Certificates snap-in allows you to br ertificate stores for yourself, a service, puter account を選択し、Next をク ificates snap-in This snap-in will always manage certificates 〇 <u>My</u> user account	owse the contents of the or a computer. <u>A</u> dd <u>C</u> lo リックします。 for:	se
he Certificates snap-in allows you to br ertificate stores for yourself, a service, puter account を選択し、Next をク fificates snap-in This snap-in will always manage certificates 〇 <u>My</u> user account	owse the contents of the or a computer. <u>A</u> dd <u>C</u> lo リックします。 for:	se

1.00	
	L'ancol
	Lancer
1.0	

<u>N</u>ext >

< <u>B</u>ack

×

12. Local computer を選択し、Finish をクリックします。

ect Computer				
Select the computer you war	nt this snap-in to mana	ige.		
This snap-in will always ma	nage:			
● Local computer: (the	computer this console	is running on)		
C Another computer:				Browse
Allo <u>w</u> the selected co only applies if you sav	mputer to be changed e the console.	d when launching fro	m the commar	id line. This
		< Back	Finish	Cancel

- 13. Close をクリックし、OK をクリックします。
- 14. Certificates (Local Computer) を展開し、Personal folder を右クリックし、All tasks、 Request New Certificate の順に選択します。



15. Welcome to the Certificate Request Wizard で Next をクリックします。



16. Domain Controller 証明書テンプレートを選択し(DC 以外のサーバでコンピュータ証明書 を要求する場合は Computer 証明書テンプレートを選択し)、Next をクリックします。

	Cardificate Taraca
	A certificate type contains preset properties for certificates.
	Select a certificate type for your request. You can access only certificate types that you have permissions for and that are available from a trusted CA.
	Certificate types:
	Directory Email Replication Domain Controller Domain Controller Authentication
	To select a cryptographic service provider and a CA, select Advanced.
	Advanced
	< <u>B</u> ack <u>N</u> ext > Cancel
 正明著	書の名前と説明を入力します。
正明有 Cert	書の名前と説明を入力します。 ificate Request Wizard
正明 i Cert	書の名前と説明を入力します。 ificate Request Wizard Sertificate Friendly Name and Description

Type a friendly name and description for the new certificate.

Eriendly name:

PEAP-Wireless

Description:

IAS Server Certificate - 802.1× Authentication

< <u>B</u>ack

Next >

Cancel

18. Finish をクリックして、	証明書要求ウィザードを完了します	•
---------------------	------------------	---

Certificate Request Wizard



Internet Authentication Service での PEAP-MS-CHAP v2 認証の設定

IAS をインストールし、IAS の証明書を要求できたので、IAS に認証の設定を行います。

次のステップを実行します。

- 1. Start > Programs > Administrative Tools の順にクリックしてから、Internet Authentication Service スナップインをクリックします。
- 2. Internet Authentication Service (IAS) を右クリックし、Register Service in Active Directory をクリックします。

🞾 Internet Authentication Se	reice		킨즈
Elle Action Yers Help			
+ + 1 2 2 2	•		
Elle datan York Lako + II I I I I I I I I I I I I I I I I	(a) (b) (c) (* Anticipation Service [LKG] to authenticate, authentice, and account for dial-up, VPU, wireless and Dhernet connections to your network. You can also configure LKG to Forward speake to any access properties of user accounts in Addre Directory, on the Addre menu, dkl.Register Server in Addre Directory. * Ato read the remote access properties of user accounts in Addre Directory, on the Addre menu, dkl.Register Server in Addre Directory. * Atom addresses accurate in Addresses, and troubleshapting, see Help.	
Register Server in Astric Dectory	Interest Company (Information	A depend (T#2120470)	
	The second secon	A service for the service serv	1.60

3. Register Internet Authentication Service in Active Directory ダイアログボックスが表示される ので、OK をクリックします。これで、IAS が Active Directory 内のユーザを認証できるよう になります。

o enable IAS to authenticate use	n the Active Directory, the computers running IAS must be authorized to read users' dial-in properties from th	e domain
o you wish to authorize this com	er to read users' dial-in properties from the Wireless.com domain?	
	OK Cancel	

1	This computer is now authorized to read users' dial-in properties from domain Wireless.com.
	To authorize this computer to read users' dial-in properties from other domains, you must register this computer to be a member of the RAS/IAS Servers Group in that domain.
	CK CK

- 5. MS IAS サーバに、ワイヤレス LAN コントローラを AAA クライアントとして追加します。 6. [RADIUS Clients] をちクリックト、 [New RADIUS Client] を選択します
- 6. [RADIUS Clients] を右クリックし、[New RADIUS Client] を選択します。

🖓 Internet Authentication Service			
Elle &dian Yew Help			
◆ → 🖪 🖪 🕃 😢 🖩			
Internet Authentication Service (Local) Internet Authentication Service (Local) <t< th=""><th>Nerve Connections to Morocott Routing and Peendre</th><th>Order 1 2</th><th></th></t<>	Nerve Connections to Morocott Routing and Peendre	Order 1 2	
New Clent			
🐮 Start 🧭 😟 Network Connections	PDHC9 Advanget	-[DNS]15WED Poternet Authenticati	🔍 🖓 🛢 🖲 🎆 🍕 🔽 7:13PM

7. クライアント名(ここでは WLC)を入力し、WLC の IP アドレスを入力します。[next] をク リックします。

w RADIUS Client			
Name and Address			
Type a friendly name and eithe	r an IP Address or DNS r	name for the client.	
Eriendly name:	WLC .		
Client address (IP or DNS):	1		
10.77.244.210		⊻erify	
	< <u>B</u> ack	<u>N</u> ext >	Cancel
	1 -		

- 8. 次のページの Client-Vendor で **RADIUS Standard** を選択し、共有秘密鍵を入力し、**Finish** をクリックします。
- 9. WLC が AAA クライアントとして IAS に追加されていることに注意してください。

🖓 Internet Authentication Service					그리프
Elle Action View Help					Ore
◆ → <u>1</u> 1 1 1 1 1 1 1 1 1 1					
Internet Authentication Service (Local)	Priendly Name /	Address	Protocol	Client/Vendor	
Her 'an <u>acceleration</u> III and Remote Access Logging Arrow Access Policies Brief Connection Request Processing	The we	10.77.244.210	RADUS	Rublus Standard	
🐮 Start 🖉 🕵 Network Connections	1 Фака	A drang	nt - [04:2,19400	P Internet Authenticati	

- 10. クライアントのリモート アクセス ポリシーを作成します。
- 11. そのためには、**Remote Access Policies** を右クリックし、**New Remote Access Policy** を選 択します。

Image: The state of the st
Image: Constant of Automatication Service (Local Service) Image: Constant of Automatication
terment Authentication Service (acid) terment Automs (corpore) Terment Automs (corpore)

12. リモート アクセス ポリシー名を入力します。この例では、PEAP という名前を使用します 。次に、[Next] をクリックします。

w Remote Acce	ss Policy Wizard
Policy Configu The wizard o	ration Method can create a typical policy, or you can create a custom policy.
How do you v	vant to set up this policy?
	e wizard to set up a typical policy for a common scenario
◯ <u>S</u> et up	a custom policy
Policy name:	
	Example: Authenticate all VPN connections.

13. 要件に応じてポリシーの属性を選択します。この例では、Wireless を選択します。

Access Method Policy conditions are based on the met	hod used to gain access to the network.
Select the method of access for which yo	ou want to create a policy.
© ⊻PN	
Use for all VPN connections. To c previous page, and select Set up a	reate a policy for a specific VPN type, go back to the a custom policy.
C <u>D</u> ial-up	
Use for dial-up connections that us Digital Network (ISDN) line.	se a traditional phone line or an Integrated Services
Wireless	
Use for wireless LAN connections	only.
C Ethernet	
Use for Ethernet connections, suc	h as connections that use a switch.

14. 次のページで User を選択し、このリモート アクセス ポリシーをユーザのリストに適用します。

w Remote Access Policy Wizard	j
User or Group Access You can grant access to individual users, or you can grant access to sele groups.	cted
Grant access based on the following:	
Group name:	A <u>d</u> d <u>B</u> emove

15. Authentication Methods で、**Protected EAP (PEAP)** を選択し、**Configure** をクリックします。

New Remote Access Policy Wizard		×
Authentication Methods EAP uses different types of security device	es to authenticate users.	Ŷ
Select the EAP type for this policy.		
<u>T</u> ype:		
Protected EAP (PEAP)	5	Configure
	< <u>B</u> ack <u>N</u> ext >	Cancel

16. **Protected EAP Properties** ページで、Certificate Issued ドロップダウン メニューから該当 する証明書を選択し、OK をクリックします。

This server identifies it Select the certificate t	self to callers before the connection hat you want it to use as proof of ide	is completed. :ntity.
Certificate issued	tsweb-lapt.Wireless.com	
Friendly name:	PEAP-Wireless	
Issuer:	Wireless-CA	
Expiration date:	12/16/2008 5:53:02 PM	
🔲 Enable Fast Recon	nect	
Eap Types		
Secured password (Er	AP-MSCHAP v2)	Move Up
		Move Dov
Add	Edit Remove C	K Cancel

New Remote Access Policy W	'izard
8	Completing the New Remote Access Policy Wizard
	You have successfully completed the New Remote Access Policy Wizard. You created the following policy:
	PEAP-Wireless
	Conditions: NAS-Port-Type matches "Wireless - Other OR Wireless - IEEE 802.11"
	Authentication: EAP(Protected EAP (PEAP))
	Encryption: Basic, Strong, Strongest, No encryption
	To close this wizard, click Finish.
	< <u>B</u> ack Finish Cancel

3

18. リモート アクセス ポリシーがリストに追加されました。



19. ポリシーを右クリックして、Properties をクリックします。If a connection request matches the specified conditions の下で Grant remote access permission を選択します。

AP Properties					?
Settings					
Specify the condi	tions that conne	ction reque	ests mu	ist match.	
Policy conditions:					
NAS-Port-Type n	natches "Wirele:	ss - Other C	DR Win	eless - IE	EE 802.11"
4					Þ
<u>ا</u> بده	- J. (D			
<u>Ago</u>	<u>E</u> ak	<u>H</u> emo	ve		
If connection requ	uests match the will be applied t	conditions	specifi	ed in this	policy, the
	will be applied (ection.		
Edit Profile					
Unless individual	access permissi	ons are spe	ecified i	in the use	er profile, this
policy controls ac	cess to the netw	vork.			
If a connection re	quest matches t	the specifie	d cond	litions:	
O Deny remote	access permissio	on			
• Grant remote	access permissi	on			
				888	
			And the second second		
		OK	c	Cancel	Apply

<u>Active Directory へのユーザの追加</u>

この設定では、Active Directory にユーザ データベースが維持されます。

Active Directory のデータベースにユーザを追加するには、次の手順を実行します。

1. Active Directory Users and Computers コンソール ツリーで、**Users** を右クリックし、**New** をクリックして、**User** をクリックします。



2. [New Object – User] ダイアログボックスで、ワイヤレス ユーザの名前を入力します。この 例では、First name フィールドに Client 1、User logon name フィールドに Client 1 を使用 しています。[next] をクリックします。

w Object - User				
Create in:	Wireless.	com/Users		
<u>F</u> irst name:	Client 1		Initials:	
Last name:				
Full name:	Client 1			
User logon name:				
Client1		@Wireless	com	•
User logon name (pre	e- <u>W</u> indows 2	000):		
WIRELESS		Client1		

3. [New Object – User] ダイアログボックスで、[Password] および [Confirm password] フィー ルドに任意のパスワードを入力します。[**User must change password at next logon] チェッ クボックスをオフにし、[Next]** をクリックします。

New Object	User	
g	Create in: Wirele:	ss.com/Users
Password	ŀ	•••••
<u>C</u> onfirm p	issword:	•••••
🗖 User)	just change passwor	rd at next logon
User User	annot change passw	word
🗖 Passy	ord never expires	
	int is disabled	
		< <u>B</u> ack <u>N</u> ext > Cancel
New Object	User] ダイアログ	゚゙ボックスで、[Finish] をクリックします。
New Object	User	
S	Create in: Wirele:	ss.com/Users

Full name: Client 1		
User logon name: Client1		
	Finish Ca	ncel

5. 追加のユーザ アカウントを作成するには、ステップ 2 ~ 4 を繰り返します。

<u>ユーザに無線アクセスを許可する</u>

次のステップを実行します。

- 1. Active Directory Users and Computers コンソール ツリーで、Users フォルダをクリックし、WirelessUser を右クリックして、Properties をクリックし、Dial-in タブに移動します。
- 2. Allow access を選択し、OK をクリックします。

lient 1 Properties	2
Remote control Terminal Service General Address Account Profile Member Of Dial-in Envir	es Profile COM+ Telephones Organization ironment Sessions
Remote Access Permission (Dial-in or VPN)-	
Allow access	
C Deny access	
C Control access through Remote Access	Policy
Callback Options	J
No <u>C</u> allback	
C Set by Caller (Routing and Remote Acce	ess Service only)
C Always Callback to:	
Assign a Static IP Address	
Apply Static Boutes	
Define routes to enable for this Dial-in connection.	Static Routes
ОК	Cancel <u>Apply</u>

<u>Wireless LAN Controller と Lightweight AP の設定</u>

次に、この設定に合せてワイヤレス デバイスを設定します。これには、Wireless LAN Controller(WLC)、Lightweight AP、およびワイヤレス クライアントの設定が含まれます。

<u>MS IAS RADIUS サーバで RADIUS 認証を行うための WLC の設定</u>

まず、MS IAS を認証サーバに使用するように WLC を設定します。ユーザ クレデンシャルを外 部 RADIUS サーバに転送するには、WLC を設定する必要があります。そうすると、外部 RADIUS サーバは、ユーザのクレデンシャルを検証し、ワイヤレス クライアントにアクセス権を 付与します。そのためには、Security > RADIUS Authentication ページで MS IAS サーバを RADIUS サーバとして追加します。

次のステップを実行します。

1. コントローラの GUI から [Security]、[RADIUS]、[Authentication] を選択して、[RADIUS Authentication Servers] ページを表示します。次に、[New] をクリックして、RADIUS サー バを定義します。

3 · 0 · 🗈 🖻	🙆 🔎 📩 🥹 🍰	🖂 🚳					🥂 – 8 ×
CISCO SPOTENO					Save C	onfiguration (Ping.	Logout Retresh
Alter aller	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	RADIUS Authentication Ser	rvers > New				< Back	Apply
AAA General	Server Index (Priority)	1 💌					
RADIUS Accounting Local Net Users	Server IPAddress	10.77.244.198					
MAC Ritering Disabled Clients User Login Policies	Shared Secret Format	ASCII 💌				_	
AP Policies	Shared Secret	•••••					
Access Control Lists	Confirm Shared					1	
IPSec Certificates CA Certificate	Secret					_	
Web Auth Certificate	Key mup						
Wireless Protection Policies	Port Number	1812					
Trusted AP Policies Rogue Policies Standard Signatures	Server Status	Enabled 💌					
Custom Signatures Client Exclusion Policies	Support for RFC 3576	Enabled 💌					
AP ACCIENCEDUCI	Retransmit Timeout	2 seconds					
	Network User	Enable					
	Management	Enable Enable					
	IPSec	🔄 Enable					

2. [RADIUS Authentication Servers] > [New] ページで RADIUS サーバのパラメータを定義しま す。RADIUS サーバ IP アドレス、共有秘密、ポート番号、サーバ ステータスなどのパラメ ータがあります。[Network User] チェックボックスと [Management] チェックボックスでは 、管理ユーザとネットワーク ユーザに RADIUS ベースの認証を適用するかどうかを指定し ます。この例では、MS IAS を 10.77.244.198 という IP アドレスを持つ RADIUS サーバと して使用しています。

3 · 0 🖹 🖻	6 P t	 Ø ∅. 		8					4	- 8
Сіяка Зтатема 	MONITOR	WLANS CO	NTROLLER	WIRELESS 5	ECURITY	MANAGEMENTCC	Save Configurat XMMANDS HELP	ion Ping	Logou	it Refre
Security	RADIUS Au	thentication	Servers					Apply	New.	
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Call Station Credentials Use AES Ke	n ID Type [s Caching sy Wrap	IP Address	×						
Access Control Lists	User N	lanagement	Index	Server Address	Port	IPSec	Admin Statu	s		
IPSec Certificates CA Certificate ID Certificate Web Auth Certificate Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Client Exclusion Policies AP Authentication			1	10.77.244.198	1812	Disabled	Enabled	Edit	Remove	Pina

- 3. [Apply] をクリックします。
- 4. MS IAS サーバが Radius サーバとして WLC に追加され、ワイヤレス クライアントの認証 に使用できるようになりました。

WLAN でのクライアントの設定

ワイヤレス クライアントの接続先の SSID(WLAN)を設定します。この例では、PEAP という 名前の SSID を作成します。

クライアントが EAP ベースの認証(ここでは PEAP-MSCHAPv2)を実行し、AES を暗号化メカ ニズムとして使用するように、レイヤ 2 認証に WPA2 を定義します。他の値はすべてデフォルト のままにします。

注:このドキュメントでは、WLAN を管理インターフェイスにバインドしています。ネットワークに複数の VLAN がある場合、独立した VLAN を作成してそれを SSID にバインドすることができます。WLC に VLAN を設定する方法については、『<u>無線 LAN コントローラでの VLAN の設定</u>例』を参照してください。

WLC に WLAN を設定するには、次の手順を実行します。

- 1. コントローラの GUI で [WLANs] をクリックして、[WLANs] ページを表示します。このペー ジには、コントローラに存在する WLAN の一覧が表示されます。
- 2. 新しい WLAN を作成するには、[New] をクリックします。WLAN の WLAN ID と WLAN SSID を入力し、[Apply] をクリックします。

3 · 🔊 🖹 🖻	0 2 7 0	3· 🕹 🖂 🖏					🦉 – ð ×
Cinco Septeme	HARANA AN				Save C	onfiguration Fing	Logout Refresh
alle alle	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANS	WLANs > New					< Back	Apply
WLANS WLANS	WLAN ID	1 💌	1				
AP Groups VLAN	WLAN SSID	PEAP					

3. 新しい WLAN を作成すると、新しい WLAN に対する [WLAN] > [Edit] ページが表示されま す。このページでは、General Policies、RADIUS Servers、Security Policies、802.1x Parameters など、その WLAN に固有のさまざまなパラメータを定義できます。

SILED STUTLE				Save Gom	garadon Pring Publication
allowedla	MONITOR WLANS CO	WTROLLER WIRELESS	SECURITY MANAGEMEN	T COMMANDS H	HELP
WLANs	WLANs > Edit				< Back Apply
WLANS	WLAN ID	1			
AP Groups VLAN	Profile Name	PEAP			
	WLAN SSID	PEAP			
	General Policies			Security Policies	s
	Radio Policy	All		IPv6 Enable	
	Admin Status	Enabled			
	Session Timeout (secs)	0		Layer 2 Security	WPA1+WPA2
	Quality of Service (QoS)	Silver (best effort)	1		MAC Filtering
	WMM Policy	Disabled 💌		Laver 3 Security	None
	7920 Phone Support	Client CAC Limit CAP	CAC Limit	coper o secondy	Web Policy •
	Broadcast SSID	Enabled			i web rolley
	Aironet IE	Enabled			
	Allow AAA Override	Allow AAA Override Enabled			not be used in combination with
	Client Exclusion	Enabled ** 60		IPsec.	
		Timeout V	Value (secs)	value of zero me	clusion is enabled, a timeout ans infinity(will require
	DHCP Server	Override		administrative ov *** CKIP is not s	erride to reset excluded clients) upported by 10xx APs
	DHCP Addr. Assignment	Required			
	Interface Name	management 💌			
	MFP Version Required	1			
	MFP Signature Generation	Global MFP Disabled)			
	H-REAP Local Switching				
	* H-REAP Local Switching authentications.) not supported with IPSEC,	CRANITE and FORTRESS		

4. WLAN を有効にするには、General Policies の下の Admin Status にチェックマークを入れま

す。AP にビーコン フレームで SSID をブロードキャストさせる場合は、**Broadcast SSID** に チェックマークを入れます。

5. Layer 2 Security で、WPA1+WPA2 を選択します。これで、WLAN で WPA が有効になりま す。ページを下にスクロールし、WPA policy を選択します。この例では、WPA2 と AES 暗 号化を使用しています。[RADIUS Servers] のプルダウン メニューから、適切な RADIUS サ ーバを選択します。この例では、10.77.244.198(MS IAS サーバの IP アドレス)を使用し ています。WLAN ネットワークの要件に基づいて、その他のパラメータを変更できます。

MONITOR W WPA1+WPA2 Parameters	LANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP				
WPA1+WPA2 Parameters	!									
										*
WPA1 Policy WPA2 Policy										
WPA2 Encrypt Auth Key Mgn	tion AES	ТКІР								
ックします	o									
					Save Co	onfiguration	Ping	Logout	Refre	h
MONITOR W	LANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP				
WLANS										
Profile Name	¥ 1	VLAN WLAN S	SID	Adr Sta	nin Secur	ity Policies				
PEAP	1	PEAP		Ena	bled [WPA:	2][Auth(802	.1x)]		Edit B	em
* WLAN IDs 9-1	16 will not be pushed to	1130,1200 and	1240 AP mode	8.						
	WPA2 Encryp Auth Key Mgr ソクします MONITOR W WLANS Profile Name PEAP * WLAN IDS 9-1	WPA2 Encryption FAES Auth Key Mgmt 802.1x ソクします。 MONITOR WLANS CONTROLLER WLANS Profile Name 7 PEAP 1 * WLAN IDS 9-16 will not be pushed to	WPA2 Encryption Auth Key Mgmt 802.1x マ Auth Key Mgmt 802.1x マ ソクします。 MONITOR WLANS CONTROLLER WIRELESS WLANS Profile Name 10 WLAN S PEAP 1 PEAP * WLAN IDS 9-16 will not be pushed to 1130,1200 and	WPA2 Encryption FAES TTKIP Auth Key Mgmt 802.1x IN 2 クします。 MONITOR WLANS CONTROLLER WIRELESS SECURITY WLANS Profile Name WLAN WLAN SSID PEAP 1 PEAP * WLAN IDS 9-16 will not be pushed to 1130,1200 and 1240 AP mode	WPA2 Encryption FAES 「TKIP Auth Key Mgmt B02.1x IV 2 クします。 MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT WLANS Profile Name WLAN SSID Adm 10 WLAN SSID Adm PEAP 1 PEAP Ena * WLAN IDS 9-16 will not be pushed to 1130,1200 and 1240 AP models.	WPA2 Encryption PAES TKIP Auth Key Mgmt 802.1x 3 2 クします。 Xave Co MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS WLANS Profile Name WLAN SSID Admin States Secur PEAP 1 PEAP Enabled [WPA: * WLAN IDS 9-16 will not be pushed to 1130,1200 and 1240 AP models.	WPA2 Encryption FAES TIKIP Auth Key Mgmt B02.1x B 2 クします。 XONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP WLANS Profile Name WLAN SSID Admin Status Security Policies PEAP 1 PEAP Enabled [WPA2][Auth(802) * WLAN IDS 9-16 will not be pushed to 1130,1200 and 1240 AP models.	WPA2 Encryption ALES THEP Auth Key Mgmt B02.1x U 2 クします。 MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP WLANS Profile Name WLAN WLAN SSID Admin Status Security Policies PEAP 1 PEAP Enabled [WPA2][Auth(602.1x)] * WLAN IDS 9-16 will not be pushed to 1130,1200 and 1240 AP models.	WPA2 Encryption Auth Key Mgmt FILE Auth Key Mgmt B02.1x WONTOR Save Configuration MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP WLANS MULAN Profile Name WLAN ID Admin Status Security Policies PEAP In PEAP * WLAN IDS 9-16 will not be pushed to 1130,1200 and 1240 AP models.	WPA2 Encryption Auth Key Memt Image: Control of the public of the p

<u>ワイヤレス クライアントの設定</u>

<u>ワイヤレス クライアントでの PEAP-MS-CHAP v2 認証の設定</u>

次の例では、Cisco Aironet Desktop Utility(ADU)を使用してワイヤレス クライアントを設定す る方法について説明しています。クライアント アダプタの設定を行う前に、使用するファームウ ェアとユーティリティのバージョンが最新であることを確認してください。最新バージョンのフ ァームウェアとユーティリティは、Cisco.com の Wireless ダウンロード ページにあります。

ADU で Cisco Aironet 802.11a/b/g ワイヤレス クライアント アダプタを設定するには、次の手順を実行します。

- 1. Aironet Desktop Utility を開きます。
- 2. Profile Management をクリックし、New をクリックしてプロファイルを定義します。
- 3. General タブでプロファイル名と SSID を入力します。この例では、WLC に設定した SSID(PEAP)を使用します。

Profile Management		? 🔀
General Security Advanc	ed	
- Profile Settings		
Profile Name:	PEAP-MSCHAPv2	
Client Name:	CLIENT1	
Network Names		
SSID1:	PEAP	
SSID2:		
SSID3:		
		Cancel

4. Security タブを選択し、WPA/WPA2/CCKM を選択して、WPA/WPA2/CCKM EAP type で PEAP [EAP-MSCHAPv2] と入力し、Configure をクリックします。

Profile Management		? 🗙
General Security Advanced		
- Set Security Options		
③ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type: FEAP (EAP-MSCHAP V2)	
WPA/WPA2 Passphrase		
◯ 802.1x	802.1x EAP Type: EAP-FAST	
O Pre-Shared Key (Static WEP)		
O None		
Configure	Allow Association to Mixed Cells Profile Locked	
	Limit Time for Finding Domain Controller To: 0 Sec	
Group Policy Delay:	60 🗘 sec	
		Cancel

5. Validate Server Certificate を選択し、Trusted Root Certificate Authorities ドロップダウン メ ニューで Wireless-CA を選択します。

Configure PEAP (EAP-MSCHAP V2)				
Use Machine Information for Domain Logon				
Validate Server Identity				
Trusted Root Certification Authorities				
Wireless-CA 😽				
When connecting, use:				
Certificate				
O User Name and Password				
Select a Certificate				
User Information for PEAP (EAP-MSCHAP V2) Authentication				
User Name: Administrator				
Password.				
Confirm Password:				
Advanced OK Cancel				

6. OK をクリックし、プロファイルを有効にします。注: Protected EAP-Microsoft Challenge Handshake Authentication Protocol Version 2(PEAP-MSCHAPv2)をMicrosoft XP SP2で使用 し、ワイヤレスカードがMicrosoft Wireless Zero Configuration(WZC)で管理されている場合 は、MicrosoftホットフィックスKB885453を適用する必要があります。このホットフィック スにより、PEAP ファスト レジュームに関連した認証上のいくつかの問題が防止されます。

<u>確認とトラブルシューティング</u>

設定が期待通りに動作することを確認するには、ワイヤレス クライアント Client1 上のプロファ イル PEAP-MSCHAPv2 を有効にします。

😰 Cisco Aironet Desktop Utility - Current Profile: PEAP-MSCHAPv2 🛛 🔗 🔀				
Action Options Help				
Current Status Profile Management	Diagnostics			
CISCO SYSTEMS				
nulliumuulliun Profile Name:	PEAP-MSCHAPv2			
Link Status:	Authenticated	Network Type: Infrastructure		
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 64		
Server Based Authentication:	PEAP (EAP-MSCHAP V2)	Data Encryption: AES		
IP Address:	10.77.244.218			
Signal Strength:				
		Advanced		

プロファイル PEAP-MSCHAPv2 が ADU 上で有効になると、クライアントでは 802.11 オープン 認証が実行され、次に PEAP-MSCHAPv2 認証が実行されます。PEAP-MSCHAPv2 認証の成功例 を次に示します。

発生するイベントのシーケンスを理解するには、デバッグ コマンドを使用します。

<u>アウトプット インタープリタ ツール(登録ユーザ専用)(OIT)は、特定の show コマンドをサ</u> <u>ポートします。</u>OIT を使用して、show コマンドの出力の分析を表示します。

ワイヤレス LAN コントローラでの次のデバッグ コマンドが有用です。

- debug dot1x events enable: 802.1x イベントのデバッグを設定
- ・debug aaa events enable: AAA イベントのデバッグを設定
- debug mac addr <mac address>: MAC のデバッグを設定、debug mac コマンドを使用
- ・debug dhcp message enable: DHCP エラー メッセージのデバッグを設定

debug dot1x events enable コマンドと debug client <mac address> コマンドの出力例を次に示します。

debug dot1x events enable

```
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from
    mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to
    mobile 00:40:96:ac:e6:57 (EAP Id 2)
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity Response (count=2) from
    mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
    mobile 00:40:96:ac:e6:57
```

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
 mobile 00:40:96:ac:e6:57 (EAP Id 5)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 6, EAP Type 25)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 7)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 7, EAP Type 25)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
 mobile 00:40:96:ac:e6:57 (EAP Id 8)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 8, EAP Type 25)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
 mobile 00:40:96:ac:e6:57 (EAP Id 9)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
 mobile 00:40:96:ac:e6:57 (EAP Id 11)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
 mobile 00:40:96:ac:e6:57 (EAP Id 12)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 12, EAP Type 25)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Accept for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 13)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending default RC4 key to
 mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending Key-Mapping RC4 key to

mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received Auth Success while in Authenticating state for mobile 00:40:96:ac:e6:57

debug mac addr <MAC Address>

```
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Association received from
  mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 -
  rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0 0 0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
   Change state to START (0)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 START (0)
   Initializing policy
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 START (0)
   Change state to AUTHCHECK (2)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2)
   Change state to 8021X_REQD (3)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 8021X_REQD (3)
   Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for
  mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of
  Mobile Station: 00:40:96:ac:e6:57 (callerId: 48)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to
  station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for
  mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry.
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving
   mobile 00:40:96:ac:e6:57 into Connecting state
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending EAP-
   Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Received EAPOL START from
  mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 EAP State update from
   Connecting to Authenticating for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x -
  moving mobile 00:40:96:ac:e6:57 into Authenticating state
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
  Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
  Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
  Entering Backend Auth Req state (id=4) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)
```

```
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
  Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
  Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
  Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
  Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
  Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Processing Access-Accept for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
  Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending default RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
   8021X_REQD (3) Change state to L2AUTHCOMPLETE (4)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
   L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
   L2AUTHCOMPLETE (4) Change state to RUN (20)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
   (20) Reached PLUMBFASTPATH: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
  (20) Replacing Fast Path rule
 type = Airespace AP Client
 on AP 00:0b:85:51:5a:e0, slot 0, interface = 2
```

```
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
Card = 0 (slot 0), InHandle = 0x0000000,
OutHandle = 0x00000000, npuCryptoFlag = 0x0000
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Successfully plumbed mobile rule (ACL ID 255)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Reached RETURN: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend
Auth Success state (id=12) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received Auth Success
while in Authenticating state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x -
moving mobile 00:40:96:ac:e6:57 into Authenticated state
```

注:PEAP認証用のCisco Secure ACSで認証するためにMicrosoftサプリカントを使用すると、ク ライアントが正常に認証されない可能性があります。最初の接続は正しく認証されるのに、後続 の高速接続の認証でうまく接続が行われません。これは既知の問題です。この問題の詳細と修正 方法は<u>ここ</u>から利用できます。

関連情報

- ACS 4.0 と Windows 2003 を使用した Cisco Unified Wireless Network 環境での PEAP
- EAP 認証と WLAN コントローラ(WLC)の設定例
- <u>ワイヤレス LAN コントローラ (WLC) のソフトウェア アップグレード</u>
- <u>Cisco 4400 シリーズ Wireless LAN Controller 設定ガイド</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。