# ACS 5.1およびWindows 2003 Serverを使用した UWN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 設定 <u>ネットワーク図</u> IIS、Certificate Authority、DNS、DHCP を使用する Windows Enterprise 2003 のセットアップ ( CA ) CA (democa) Cisco 1121 Secure ACS 5.1 CSACS-1121 シリーズ アプライアンスを使用したインストール ACS サーバのインストール Cisco WLC5508 コントローラの設定 WPAv2 および WPA に必要な設定の作成 PEAP 認証 証明書テンプレート スナップインのインストール ACS Web サーバ用の証明書テンプレートの作成 新しい ACS Web サーバ証明書テンプレートの有効化 ACS 5.1 証明書のセットアップ エクスポート可能な ACS 用証明書の設定 ACS 5.1 ソフトウェアでの証明書のインストール Active Directory の ACS ID ストアの設定 ACS への AAA クライアントとしてのコントローラの追加 ワイヤレス用 ACS アクセス ポリシーの設定 ACS アクセス ポリシーとサービス ルールの作成 Windows の自動機能を使用した PEAP 用クライアントの設定 基本的なインストールと設定の実行 ワイヤレス ネットワーク アダプタのインストール ワイヤレス ネットワーク接続の設定 ACS を使用したワイヤレス認証のトラブルシューティング ACS サーバでの PEAP 認証の失敗 関連情報

概要

このドキュメントでは、ワイヤレス LAN コントローラ、Microsoft Windows 2003 ソフトウェア 、および Cisco Secure Access Control Server (ACS) 5.1 で、Protected Extensible Authentication Protocol (PEAP)と Microsoft Challenge Handshake Authentication Protocol (MS-CHAP; Microsoft チャレンジ ハンドシェイク認証プロトコル)バージョン 2 を使用 して、セキュアなワイヤレス アクセスを設定する方法について説明します。

**注**:セキュアワイヤレスの導入については、<u>Microsoft Wi-Fi Webサイト</u>、および<u>Cisco SAFEワイ</u> <u>ヤレスブループリント</u>を参照してください。

# <u>前提条件</u>

<u>要件</u>

ここでは、インストール担当者が Windows 2003 と Cisco ワイヤレス LAN コントローラのイン ストールに関する基本的な知識を持っていることを前提とし、このドキュメントではテストを実 行するための特定の設定についてのみ説明しています。

Cisco 5508 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>Cisco 5500 シリー</u> <u>ズ ワイヤレス コントローラ インストレーション ガイド</u>』を参照してください。Cisco 2100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>クイックスタートガイド : Cisco</u> <u>2100シリーズワイヤレスLANコントローラ</u>』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。

ここでは、PEAP 認証用のユーザ証明書とワークステーション証明書の自動登録を設定できるようにするために、Windows Server 2003 Enterprise Edition SP 1 を使用しています。証明書の自動登録と自動更新を使用すると、証明書の期限管理と更新を自動化できるため、証明書の配布が容易になると同時に、セキュリティも向上します。

#### <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。

- 7.0.98.0 が稼働する Cisco 2106 または 5508 シリーズ コントローラ
- Cisco 1142 Lightweight Access Point Protocol(LWAPP; Lightweight アクセス ポイント プロトコル)AP
- Windows 2003 Enterprise (Internet Information Server (IIS)、Certificate Authority (CA; 認 証局)、DHCP、Domain Name System (DNS; ドメイン ネーム システム) がインストール されているもの)
- Cisco 1121 Secure Access Control System Appliance (ACS) 5.1
- Windows XP Professional SP(および最新の Service Pack)と、無線ネットワーク インター フェイス カード(NIC)(CCX v3 をサポートしているもの)またはサード パーティのサプ リカント
- Cisco 3750 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。

## 設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供して 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。

#### シスコのセキュア ワイヤレス ラボのトポロジ

# Access Point Cisco 5508 Controller Cisco 3750 Cisco 3750 Cisco 3750 Cisco 1121 ACS 5.1

このドキュメントの第1の目的は、ACS 5.1 と Windows 2003 Enterprise サーバを使用する Unified Wireless Network 環境で PEAP を実装する手順を説明することです。特に、クライアントの登録とサーバからクライアントへの証明書の取得を自動化する、クライアントの自動登録の 機能に重点を置いています。 注: Temporal Key Integrity Protocol(TKIP)/Advanced Encryption Standard(AES)を使用するWi-Fi Protected Access(WPA)/WPA2をWindows XP Professional SPに追加するには、『<u>Windows XP</u> <u>Service Pack 2</u>用のWPA2/Wireless Provisioning Services Information Element(WPS IE)アップデ ート』を参照してください。

# <u>IIS、Certificate Authority、DNS、DHCP を使用する Windows</u> Enterprise 2003 のセットアップ(CA)

CA (democa)

CA とは、Windows Server 2003 Enterprise Edition SP2 が稼働していて、次の役割を実行するコンピュータのことです。

- ・IIS を実行する demo.local ドメインのドメイン コントローラ
- ・demo.local DNS ドメインの DNS サーバ
- ・DHCP サーバ
- demo.local ドメインのエンタープライズ ルート CA

CA で、これらのサービスを実行できるように設定するには、次の手順を実行します。

- 1. 基本的なインストールと設定を実行する。
- 2. <u>コンピュータをドメイン コントローラとして設定する。</u>
- 3. ドメインの機能レベルを上げる。
- 4. <u>DHCP をインストールして設定する。</u>
- 5. 証明書サービスをインストールする。
- 6. 証明書を使用するための管理者権限を確認する
- 7. <u>ドメインにコンピュータを追加する。</u>
- 8. <u>コンピュータに無線アクセスを許可する。</u>
- 9. <u>ドメインにユーザを追加する</u>
- 10. <u>ユーザに無線アクセスを許可する。</u>
- 11. <u>ドメインにグループを追加する。</u>
- 12. wirelessusers グループにユーザを追加する
- 13. WirelessUsers グループにクライアント コンピュータを追加する。

基本的なインストールと設定を実行する

次のステップを実行します。

- 1. Windows Server 2003 Enterprise Edition SP2 をスタンドアロン サーバとしてインストール します。
- 2. IP アドレスは *10.0.10.10、*サブネット マスクは *255.255.255.0* で TCP/IP プロトコルを設定 します。

<u>コンピュータをドメイン コントローラとして設定する</u>

次のステップを実行します。

1. [Start] > [Run] を選択して dcpromo.exe と入力し、[OK] をクリックして Active Directory の

インストール ウィザードを開始します。

- 2. [Welcome to the Active Directory Installation Wizard] ページで、[Next] をクリックします。
- 3. [Operating System Compatibility] ページで、[Next] をクリックします。
- 4. [Domain Controller Type] ページで [**Domain Controller for a new Domain**] を選択し、[**Next**] をクリックします。
- 5. [Create New Domain] ページで [**Domain in a new forest**] を選択し、[**Next**] をクリックします。
- 6. [Install or Configure DNS] ページで [No, just install and configure DNS on this computer] を 選択し、[Next] をクリックします。
- 7. [New Domain Name] ページで demo.local と入力して、[Next] をクリックします。
- 8. [NetBIOS Domain Name] ページで、[Domain NetBIOS name] に **demo** と入力して、[Next] をクリックします。
- 9. [Database and Log Folders] ページで、[Database folder] と [Log folder] のディレクトリはデ フォルトのまま、[Next] をクリックします。

Directory Installation Wizard		
atabase and Log Folders Specify the folders to contain the Active Directory database and log files.		
For best performance and recoverability, store the database and the log on separate hard disks.		
Where do you want to store the Active Directory database?		
Database folder:		
C:\WINDOWS\NTDS		Bjowse
Where do you want to store the Active Dir Log folder:	ectory log?	
C:\WINDOWSWTDS		Browse

10. [Shared System Volume] ページで、デフォルトのフォルダ場所が正しいことを確認して、 [Next] をクリックします。

Active Directory Installation Wizard		
Shared System Volume Specify the folder to be shared as the system volume.		
The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.		
The SYSVOL folder must be located on an NTFS volume.		
Enter a location for the SYSVOL folder.		
Eolder location:		
CAWINDOWSASYSVOL Browse		
< <u>B</u> ack <u>N</u> ext> Cancel		

11. [Permissions] ページで、[Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems] が選択されていることを確認して、[Next] をクリックしま

Active Directory Installation Wizard		
Permissions Select default permissions for user and group objects.		
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.		
C Permissions compatible with pre-Windows 2000 server operating systems		
Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.		
Anonymous users can read information on this domain.		
Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems		
Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.		
< <u>B</u> ack <u>N</u> ext> Cancel		

12. [Directory Services Restore Mode Administration Password] ページで、パスワードのボッ クスは空白のままにして、[Next] をクリックします。

す。

13. [Summary] ページで情報を確認して [Next] をクリックします。

Active Directory Installation Wizard	×
Summary Review and confirm the options you selected.	R
You chose to:	
The new domain name is example.com. This is also the name of the new forest.	
The NetBIOS name of the domain is EXAMPLE	
Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL	
The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server.	
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 Back. To begin the operation, click Next.	
< <u>B</u> ack <u>N</u> ext> Can	cel

- 14. Active Directory のインストールが完了したら、[Finish] をクリックします。
- 15. コンピュータの再起動を指示するプロンプトが表示されたら、[Restart Now] をクリックします。

<u>ドメインの機能レベルを上げる</u>

- 1. [Administrative Tools] フォルダから [Active Directory Domains and Trusts] スナップインを開き([Start] > [Programs] > [Administrative Tools] [Active Directory Domains and Trusts])、 ドメイン コンピュータの **CA.demo.local** を右クリックします。
- 2. [Raise Domain Functional Level] をクリックし、[Raise Domain Functional Level] ページで [Windows Server 2003] を選択します。



3. [Raise] をクリックし、[OK] をクリックしてから、もう一度 [OK] をクリックします。

#### DHCP をインストールして設定する

- 1. コントロール パネルの [**プログラムの追加と削除**] を使用して、Dynamic Host Configuration Protocol (DHCP) を Networking Service コンポーネントとしてインストールします。
- 2. [Administrative Tools] フォルダから [DHCP] スナップインを開き([Start] > [Programs] > [Administrative Tools] [DHCP])、DHCP サーバの **CA.demo.local** を強調表示します。
- 3. [Action] をクリックしてから [Authorize] をクリックし、DHCP サービスを許可します。
- 4. コンソール ツリーで CA.demo.local を右クリックして、[New Scope] をクリックします。
- 5. [New Scope] ウィザードの [Welcome] ページで、[Next] をクリックします。
- 6. [Scope Name] ページで、[Name] フィールドに CorpNet と入力します。

New Scope Wizard	
Scope Name You have to p providing a de	rovide an identifying scope name. You also have the option of scription.
Type a name a how the scope	and description for this scope. This information helps you quickly identify a is to be used on your network.
N <u>a</u> me:	CorpNet
Description:	
	< <u>B</u> ack <u>N</u> ext > Cancel

7. [Next] をクリックし、次のようにパラメータを入力します。[Start IP address]: 10.0.20.1[End IP address]: 10.0.20.200Length - 24サブネットマスク: 255.255.255.0

New Scope Wizard		
IP Address Range You define the scope address range by identifying a set of consecutive IP addresses.		
Enter the range of addresses that the scope distributes.		
Start IP address: 10 . 0 . 20 . 1		
End IP address: 10 . 0 . 20 . 200		
A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.		
Length: 24		
Sybnet mask: 255 . 255 . 0		
< <u>B</u> ack <u>N</u> ext > Cancel		

8. [Next] をクリックし、除外するアドレスの [Start IP address] に **10.0.20.1**、[End IP address] に *10.0.20.100* と入力します。次に、[Next] をクリックします。これにより、10.0.20.1 ~ 10.0.20.100 の範囲の IP アドレスが予約されます。この予約 IP アドレスは、DHCP サーバ から割り当てられることはありません。

v Scope Wizard	
Add Exclusions Exclusions are ad server.	dresses or a range of addresses that are not distributed by the
Type the IP addre address, type an a	ess range that you want to exclude. If you want to exclude a single address in Start IP address only.
Start IP address:	End IP address:
10 . 0 . 20	. 1 10.0.20.100 Add
Excluded address	range:
	Remo <u>v</u> e
	< Back Next > Cancel

- 9. [Lease Duration] ページで [Next] をクリックします。
- 10. [Configure DHCP Options] ページで [Yes, I want to configure these options 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 scope.	options before clients can use the	
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?		
Mes, I want to configure these options now		
No, I will configure these options later		
	< <u>B</u> ack <u>N</u> ext > Cancel	

11. [Router (Default Gateway)] ページで、デフォルト ルータ アドレスの *10.0.20.1* を追加し、 [Next] をクリックします。

New Scope Wizard		
Router (Default Gateway) You can specify the routers, or default gateways, to be distributed by this scope.		
To add an IP address for a router used by clients, enter the address below.		
I <u>P</u> address:		
10.0.20.1 Add		
<u>B</u> emove		
Шр		
D <u>o</u> wn		
< <u>B</u> ack <u>N</u> ext > Cancel		

12. [Domain Name and DNS Servers] ページで、[Parent domain] フィールドに *demo.local*、 [IP address] フィールドに *10.0.10.10* と入力し、[Add] をクリックしてから [Next] をクリッ クします。

New Scope Wizard			
Domain Name and DNS Servers The Domain Name System (DNS) maps and translates domain names used by clients on your network.			
You can specify the parent domain you want the client computers on your network to use for DNS name resolution.			
Parent do <u>m</u> ain: demo.local			
To configure scope clients to use DNS server: servers.	s on your network, enter the IP ad	dresses for those	
<u>S</u> erver name:	I <u>P</u> address:		
		A <u>d</u> d	
R <u>e</u> solve	10.0.10.10	<u>R</u> emove	
		Up	
		Down	
	1	Dāmu	
	< <u>B</u> ack <u>N</u> ext >	Cancel	

- 13. [WINS Servers] ページで **[Next]** をクリックします。
- 14. [Activate Scope] ページで、[Yes, I want to activate this scope now] を選択し、[Next] をクリックします。

New Scope Wizard	
Activate Scope Clients can obtain address leases only if a scope is activ	rated.
Do you want to activate this scope now?	
Yes, I want to activate this scope now	
O No, I will activate this scope later	
< <u>B</u> ack	Next > Cancel

15. [New Scope Wizard] ページが完了したら、[Finish] をクリックします。

#### <u>証明書サービスをインストールする</u>

次のステップを実行します。

**注:証明書サ**ービスをインストールする前にIISをインストールする必要があります。また、ユー ザはEnterprise Admin OUの一部である必要があります。

- 1. コントロール パネルで [Add or Remove Programs] を開き、[Add/Remove Windows Components] をクリックします。
- 2. [Windows Components Wizard] ページで [Certificate Services] を選択し、[Next] をクリック します。
- 3. [CA Type] ページで [Enterprise root CA] を選択し、[Next] をクリックします。
- 4. [CA Identifying Information] ページで、[Common name for this CA] ボックスに *democa* と入 力します。その他の情報もオプションで入力できます。次に [**Next**] をクリックし、 [Certificate Database Settings] ページはデフォルトのまま使用します。
- 5. [next] をクリックします。インストールが完了したら、[Finish] をクリックします。
- 6. IIS のインストールに関する警告メッセージを読んでから、[OK] をクリックします。

<u>証明書を使用するための管理者権限を確認する</u>

次のステップを実行します。

1. [Start] > [Administrative Tools] > [Certification Authority] を選択します。

- 2. democa CA を右クリックし、[Properties] をクリックします。
- 3. [Security] タブの [Group or User names] リストで、[Administrators] をクリックします。
- 4. [Permissions for Administrators] リストで、次のオプションが [Allow] に設定されていること を確認します。Issue and Manage CertificatesManage CARequest Certificates[Deny] に設定 されている、またはチェックマークが入っていないオプションがある場合は、権限を [Allow] に設定します。

ca.demo.local Properties		? ×	
General   Policy Module   Exit Mod Certificate Managers Restrictions   Auditir	lule   Extension ng   RecoveryAg	ns Storage jents Security	
<u>G</u> roup or user names: Administrators (DEMO\Administrators) Authenticated Users Domain Admins (DEMO\Domain Admins) Enterprise Admins (DEMO\Enterprise Admins)			
Permissions for Administrators	A <u>d</u> d	<u>R</u> emove Deny	
Read Issue and Manage Certificates Manage CA Request Certificates			
OK	Cancel	Apply	

5. [OK] をクリックして democa CA の [Properties] ダイアログボックスを閉じ、続いて [Certification Authority] を終了します。

#### <u>ドメインにコンピュータを追加する</u>

次のステップを実行します。

**注**:コンピュータがすでにドメインに追加されている場合は、「<u>ドメインへのユーザの追加</u>」に 進みます。

1. [Active Directory Users and Computers] スナップインを開きます。

- 2. コンソール ツリーで demo.local を展開します。
- 3. [Computers] を右クリックして [New] をクリックし、[Computer] をクリックします。
- 4. [New Object Computer] ダイアログボックスで、[Computer name] フィールドにコンピュ ータの名前を入力し、[Next] をクリックします。この例では、*Client* というコンピュータ名

w Object - Computer		
Create in: demo.local/Us	ers	
Computer name:		
client		
Computer name (pre-Windows 2000):		
CLIENT		
The following user or group can join the User or group:	s computer to a dom	nain.
Default: Domain Admins		<u>C</u> hange
Assign this computer account as a	pre-Windows 2000	computer
Assign this computer account as a	backup domain con	troller
	,	
	< <u>B</u> ack <u>N</u> e	ext > Cancel

を使用します。

- 5. [Managed] ダイアログボックスで [Next] をクリックします。
- 6. [New Object Computer] ダイアログボックスで [Finish] をクリックします。
- 7. さらにコンピュータ アカウントを作成する場合は、ステップ3~6を繰り返します。

<u>コンピュータに無線アクセスを許可する</u>

- [Active Directory Users and Computers] コンソール ツリーで [Computers] フォルダをクリックし、ワイヤレス アクセスを許可するコンピュータを右クリックします。この例では、ステップ 7 で追加した [Client] というコンピュータを使用する手順を示します。[Properties] をクリックし、[Dial-in] タブに移動します。
- 2. [Remote Access Permission] で、[Allow access] を選択し、[OK] をクリックします。

client Properties ?	×
General Operating System Member Of Location Managed By Dial-in	L
Remote Access Permission (Dial-in or VPN)	
Allow access	
C Deny access	
C Control access through Remote Access Policy	
Callback Options	
Set by Caller (Routing and Remote Access Service only)	
C Always Callback to:	
Assign a Static IP Address	
Apply Static Boutes	
Define routes to enable for this Dial-in Static Routes	
OK Cancel <u>Apply</u>	

<u>ドメインにユーザを追加する</u>

- 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 *wirelessuser*、[User logon name] フィールドに *wirelessuser* という名前を使用しています。[next] をクリックします。

New Object - User 🛛 🔀
Create in: demo.local/Users
<u>F</u> irst name: <u>Initials:</u>
Last name:
Full name: wirelessuser
User logon name:
wirelessuser @demo.local
User logon name (pre- <u>W</u> indows 2000):
DEMO\ wirelessuser
< <u>B</u> ack <u>N</u> ext > Cancel

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	×
Create in: demo.local/Users	
Password:     •••••••       Confirm password:     •••••••	
<ul> <li>User must change password at next logon</li> <li>User cannot change password</li> <li>Password never expires</li> </ul>	
Account is disabled	
< <u>B</u> ack <u>N</u> ext > Ca	incel

- 4. [New Object User] ダイアログボックスで、[Finish] をクリックします。
- 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>

- 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. [Remote Access Permission] で、[Allow access] を選択し、[OK] をクリックします。

irelessuser	Properties	5			?
Remote General	Address	Termi Account	nal Servic Profile	es Profile   Telephones	COM+ Organization
Remote A	Ur Access Permi	ssion (Dial-in	or VPN)	ronment	Sessions
C Deny	access	ough Remote	e Access	Policy	
□ <u>U</u> erify □ Callback	Caller-ID: Options		Γ		
○ No <u>C</u> ○ <u>S</u> et by	allback y Caller (Rou	ting and Rer	note Acce	ss Service only)	
C Alway	es Callback to	0:	۲ ۲		
	n a Static IP / Static <u>R</u> oute	s	1		•
Define r connect	outes to enal tion.	ble for this D	ial-in	Static Royt	.es
		(	DK	Cancel	Apply

<u>ドメインにグループを追加する</u>

- 1. [Active Directory Users and Computers] コンソール ツリーで、[Users] を右クリックして [New] をクリックし、[Group] をクリックします。
- 2. [New Object Group] ダイアログボックスで、[Group name] フィールドにグループの名前を 入力し、[OK] をクリックします。このドキュメントでは、*wirelessusers* というグループ名 を使用します。

w Object - Group	×
Create in: demo	o.local/Users
Group name:	
wirelessusers	
·	
Group name (pre-Windows 20	000):
wirelessusers	
Group scope	Group type
C Domain local	Security
Global	C Distribution
C Universal	
C Thurster	
	OK Cancel

<u>wirelessusers グループにユーザを追加する</u>

- 1. [Active Directory Users and Computers] の詳細ペインで、グループ [*WirelessUsers*] をダブ ルクリックします。
- 2. [Members] タブに移動し、**[Add]** をクリックします。
- 3. Select Users, Contacts, Computers, or Groups ダイアログボックスで、グループに追加する ユーザの名前を入力します。この例では、ユーザ *wirelessuser* をグループに追加する手順を 説明しています。[OK] をクリックします。

Select Users, Contacts, or Computers	? ×
Select this object type:	
Users or Other objects	Object Types
Erom this location:	
demo.local	Locations
Enter the object names to select (examples):	
wirelessuser	<u>C</u> heck Names

4. [Multiple Names Found] ダイアログボックスで [OK] をクリックします。wirelessuser のユー ザ アカウントが、wirelessusers のグループに追加されます。

wirelessusers Proper	ties	? ×
General Members	Member Of Managed By	
Members:		
Name	Active Directory Folder	
Administrator	demo.local/Users demo.local/Users	
Milelessuser	demonocaty o sets	
1		
Add	Bemove	
	OK Cancel	Applu 1
		OPPY

5. [OK] をクリックして、wirelessusers のグループに対する変更を保存します。 6. さらにユーザをグループに追加する場合は、この手順を繰り返します。

wirelessusers グループにクライアント コンピュータを追加する

- このドキュメントの「<u>wirelessusers グループにユーザを追加する</u>」のステップ1~2を繰り返します。
- 2. [Select Users, Contacts, or Computers] ダイアログボックスで、グループに追加するコンピ ュータの名前を入力します。この例では、*client* という名前のコンピュータをグループに追 加する手順を説明しています。

Select this object type:	
Users or Other objects	Object Types
From this location:	
demo.local	Locations
nter the object names to select (examples):	
inter the object names to select ( <u>examples)</u> : client	<u>C</u> heck Names
Enter the object names to select ( <u>examples)</u> : client	<u>C</u> heck Names
Enter the object names to select ( <u>examples)</u> : client	<u>C</u> heck Names

3. [Object Types] をクリックし、[Users] チェックボックスをオフにして、[Computers] にチェ ックマークを入れます。

Object Types	? ×
Select the types of objects you want to find.	
Object types:	
V Other objects	
Computers	
	OK Cancel

4. [OK] を 2 回クリックします。CLIENT のコンピュータ アカウントが、wirelessusers のグル

Members       Member Of       Managed By         Members:       Active Directory Folder         Image: Administrator       demo.local/Users         Image: Client       demo.local/Computers         Image: Wirelessuser       demo.local/Users	
Add Records	
Name       Active Directory Folder	
Administrator demo.local/Users client demo.local/Computers wirelessuser demo.local/Users	
Scient demo.local/Computers wirelessuser demo.local/Users	
wirelessuser demo.local/Users	
Add	
Add Remove	
Add Remove	
Mon" Ticupac	
OK Carrel 4	

ープに追加されます。

5. さらにコンピュータをグループに追加するには、この手順を繰り返します。

# Cisco 1121 Secure ACS 5.1

#### <u>CSACS-1121 シリーズ アプライアンスを使用したインストール</u>

CSACS-1121 アプライアンスは、ACS 5.1 ソフトウェアと一緒にプリインストールされています 。このセクションでは、ACS をインストールする前に実行する必要のある、インストール プロ セスおよびタスクの概要を説明します。

- 1. CSACS-1121 をネットワークおよびアプライアンス コンソールに接続します。第 4 章「<u>ケ</u> <u>ーブルの接続」を参照してください。</u>
- 2. CSACS-1121 アプライアンスの電源を入れます。第 4 章「<u>CSACS-1121 シリーズ アプライ</u> アンスの電源投入」を参照してください。
- 3. CLI プロンプトで setup コマンドを実行して、ACS サーバの初期設定を行います。「セット アップ プログラムの実行」を参照してください。

#### ACS サーバのインストール

このセクションでは、CSACS-1121 シリーズ アプライアンスに ACS サーバをインストールする プロセスについて説明します。

- <u>セットアップ プログラムの実行</u>
- インストールプロセスの検証
- インストール後のタスク

Cisco Secure ACS サーバのインストールの詳細については、『<u>Cisco Secure Access Control</u> <u>System 5.1 のインストールとアップグレード ガイド</u>』を参照してください。

<u>Cisco WLC5508 コントローラの設定</u>

<u>WPAv2 および WPA に必要な設定の作成</u>

次のステップを実行します。

**注:コント**ローラがネットワークに基本的な接続でき、管理インターフェイスへのIP到達可能性が正常であると想定します。

1. ブラウザで https://10.0.1.10 を開いて、コントローラにログインします。



- 2. [Login] をクリックする。
- 3. デフォルト ユーザの admin とデフォルト パスワードの admin を使用してログインします。
- 4. [Controller] メニューから、VLAN のマッピング用の新しいインターフェイスを作成します。
- 5. [Interfaces] をクリックします。
- 6. [New] をクリックします。
- 7. [Interface name] フィールドに *Employee* と入力します(このフィールドには、任意の値を 入力できます)。
- 8. [VLAN ID]フィールドに20と入力します(このフィールドには、ネットワーク内で伝送され る任意のVLANを指定できます)。
- 9. [Apply] をクリックします。
- 10. 次の [Interfaces > Edit] ウィンドウに示すとおりに、情報を設定します。[Interface IP Address]: **10.0.20.2**[Netmask]: **255.255.255.0**[Gateway]: **10.0.10.1**[Primary DHCP]: **10.0.10.10**

սիսիս				S	a <u>v</u> e Configuratio	in   <u>P</u> ing	Logou	t   <u>R</u> efre
CISCO MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMEN	r c <u>o</u> m	MANDS	HELP
Controller	In	terfaces > Edit			<	Back	Ap	oply
Controller General Inventory Interfaces Multicast Network Routes Internal DHCP Ser Mobility Managem Ports NTP CDP Advanced	ver ent Co Ph Di Ac	terfaces > Edit eneral Informat Interface Name MAC Address onfiguration Guest Lan Quarantine Quarantine Vian Id nysical Informat Quarantine Vian Id nysical Informat Port Number Backup Port Active Port Enable Dynamic AP terface Address VLAN Identifier IP Address Netmask Gateway HCP Information Secondary DHCP Services	ion em 00: 00: 0 tion	ployee 24:97:69:4d:e 2 0 0 20 10.0.20.2 255.255.255. 10.0.20.1		Back	Ap	ylq
		ACL Name		none 💌				
	No ter so	te: Changing the In mporarily disabled a me clients.	terface param and thus may r	eters causes t esult in loss of	he WLANs to be f connectivity for	-		

- 11. [Apply] をクリックします。
- 12. [WLANs] タブをクリックします。
- 13. [Create New] を選択して、[Go] をクリックします。
- 14. [Profile Name] を入力し、[WLAN SSID] フィールドに Employee と入力します。

սիսիս				S	a <u>v</u> e Configuration	Ping   I	Logout   <u>R</u> efre
CISCO MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMAN	NDS HELP
WLANs	W	LANs > New			< Ba	ack	Apply
WLANs     WLANs		Туре	E	WLAN 💌			
Advanced		Profile Name	1	Employee			
		SSID	1	Employee			
		ID	E	1 💌			

15. WLAN の ID を選択し、[Apply] をクリックします。

16. [WLANs > Edit] ウィンドウが表示されたら、この WLAN の情報を設定します。**注:このラ** 

ボでは、WPAv2が選択されたレイヤ2暗号化方式です。この SSID に関連付ける TKIP-MIC クライアントで WPA を使用させるには、802.11i AES 暗号化方式をサポートしていないク ライアントで、[WPA compatibility mode] と [Allow WPA2 TKIP Clients] のチェックボック スをオンにします。

- 17. [WLANs > Edit] 画面で [General] タブをクリックします。
- 18. [Status] の [Enabled] チェックボックスがオンになっており、適切な [Interface] (employee) が選択されていることを確認します。また、[Broadcast SSID] の [Enabled] チェックボックスがオンになっていることも確認します。

	VLANS CO	ITROLLER	WIRELESS	SECURITY	a <u>v</u> e Configuration MANAGEMENT	Eing COMM	Logout <u>R</u> efre
WLANs	WLANs	> Edit		Feeduary	< Bi	ack	Apply
WLANs WLANs	Gener	al Sec	urity Qos	S Advanc	ed		
Advanced	Prof	le E	Employee				
	Тур	• •	WLAN				
	SSI	ο ε	Employee				
	Stat	us [	Enabled				
	Sec Poli	urity [ ies [ cł	[WPA2][Auth( Modifications do hanges.)	802.1X)] ne under secu	rity tab will appear	after app	lying the
	Rad	o Policy	All	•			
	Inte	rface 🧧	employee				
	Bro	dcast	Enabled				

- 19. [Security] タブをクリックします。
- 20. [Layer 2] サブメニューの [Layer 2 Security] で、[WPA + WPA2] を選択します。WPA2 暗 号化の場合、TKIP クライアントを許可するには、[AES + TKIP] を選択します。
- 21. 認証方式には 802.1x を選択します。

WLANs > Edit						
General	Security	QoS	Advance	ed		
Layer 2	Layer 3	AAA Se	ervers			
Layer 2 WPA+WPA	Layer 2 Security  WPA+WPA2 MAC Filtering WPA+WPA2 Parameters					
WPA Po	licy					
WPA2 P	WPA2 Policy					
WPA2 E	WPA2 Encryption AES TKIP					
Auth Ke	ey Mgmt	802.	1X	*		

- 22. レイヤ 3 サブメニューは不要のため、スキップします。RADIUS サーバを設定したら、 [Authentication] メニューから適切なサーバを選択できるようになります。
- 23. 特別な設定が必要でない限り、[QoS] タブおよび [Advanced] タブはデフォルトのままにし ておきます。
- 24. [Security] メニューをクリックし、RADIUS サーバを追加します。
- 25. [RADIUS] サブメニューで、[Authentication] をクリックします。次に、[New] をクリックします。
- 26. RADIUS サーバの IP アドレス(10.0.10.20)を追加します。このアドレスは、前の手順で 設定した ACS サーバのものです。
- 27. 共有キーが、ACS サーバで設定されている AAA クライアントと一致していることを確認 します。[Network User] チェックボックスがオンになっていることを確認し、[Apply] をク リックします。

սիսիս		Save Configuration   Ping   Logout Befree
CISCO MONITOR WL	ANS <u>C</u> ONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	RADIUS Auther	ntication Servers > New < Back Apply
<ul> <li>AAA         General         <ul> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> </ul> </li> <li>TACACS+         <ul> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> </ul> </li> </ul>	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap R	
Local EAP	Server Status	Enabled 💌
Priority Order	Support for REC 3576	Enabled 💌
Certificate	Server Timeout	2 seconds
Access Control Lists	Network User	Enable
<ul> <li>Wireless Protection</li> <li>Policies</li> </ul>	Management	Enable
▶ Web Auth	IPSec	Enable Enable
Advanced		

28. これで基本設定が完了し、PEAP のテストが実行できるようになりました。

# <u>PEAP 認証</u>

MS-CHAP バージョン 2 を使用した PEAP の場合、ACS サーバの証明書は必要ですが、ワイヤレ ス クライアントの証明書は不要です。ACSサーバのコンピュータ証明書の自動登録を使用すると 、導入を簡素化できます。

コンピュータ証明書とユーザ証明書の自動登録を実行するように CA サーバを設定するには、このセクションの手順を実行します。

注: MicrosoftはWindows 2003 Enterprise CAのリリースに伴いWebサーバテンプレートを変更し たため、キーはエクスポートできなくなり、オプションはグレー表示されます。サーバ認証に使 用でき、ドロップダウンで使用できるキーをエクスポート可能にマークできる機能を備えた証明 書サービスでは、これ以外の証明書テンプレートは提供されていないため、これを実行する新し いテンプレートを作成する必要があります。 **注**:Windows 2000ではエクスポート可能なキーを使用できます。Windows 2000を使用する場合 は、これらの手順に従う必要はありません。

<u>証明書テンプレート スナップインのインストール</u>

次のステップを実行します。

- 1. [Start] > [Run] の順に選択し、mmc と入力して、[OK] をクリックします。
- 2. [File] メニューで [Add/Remove Snap-in] をクリックし、[Add] をクリックします。
- 3. [Snap-in] の下にある [Certificate Templates] をダブルクリックし、[Close] をクリックしてか ら [OK] をクリックします。
- 4. コンソール ツリーで [Certificate Templates] をクリックします。詳細ペインに、すべての証 明書テンプレートが表示されます。
- 5. ステップ 2 ~ 4 を省略するには、*certtmpl.msc* と入力し、[Certificate Templates] スナップ インを開きます。

🌇 MyConsole - [Console Root\Certificate Templates]							
Elle Action View Favorites Window Help							
← → 🗈 🖬 😭 😫 😤							
Console Root	Template Display Name	Minimum Supported CAs					
Certificate Templates	Exchange Signature Only	Windows 2000					
	Exchange User	Windows 2000					
	20 IPSec	Windows 2000					
	IPSec (Offline request)	Windows 2000					
	Key Recovery Agent	Windows Server 2003, En					
	RAS and IAS Server	Windows Server 2003, En					
	Root Certification Authority	Windows 2000					
	Router (Offline request)	Windows 2000					
	Smartcard Logon	Windows 2000					
	Smartcard User	Windows 2000					
	Subordinate Certification Authority	Windows 2000					
	Trust List Signing	Windows 2000					
	User User	Windows 2000					
	User Signature Only	Windows 2000					
	Web Server	Windows 2000					
	Workstation Authe Duplicate Template	Windows Server 2003, En 👻					
	All Tasks						
Using this template as a base, creates a	a template that supports Properties						

ACS Web サーバ用の証明書テンプレートの作成

- 1. [Certificate Templates] スナップインの詳細ペインで、[Web Server] テンプレートをクリックします。
- 2. [Action] メニューで [Duplicate Template] をクリックします。

Properties of New T	emplate	? ×
Issuance Requirem General	ents Superseded Templates Request Handling	Extensions Security Subject Name
Template display no Copy of Web Serve Minimum Supported After you apply char name.	ame: ed d CAs: Windows Server 2003, inges to this tab, you can no lor	Enterprise Edition nger change the template
Iemplate name: Copy of Web Serv Validity period: 2 years	er <u>R</u> enewal perio	d:
Publish certifica     Do not auto     Directory	te in Active Directory matically reenrol if a duplicate of	ertificate exists in Active
	ОК	Cancel Apply

3. [Template display name] フィールドに、ACS と入力します。

operties of New 1	remplate		?
Issuance Requirem General	ents   Superseded Templates   Request Handling	Extensions Subject N	Securit Iame
Template display r	iame:		
JALS			
Minimum Supporte	d CAs: Windows Server 2003, E	nterprise Edition	n
After you apply ch name.	anges to this tab, you can no long	er change the	template
Template name:			
ACS			
Validity period:	Eenewal period:	-	
E Publish certific	ate in Active Directory	ditende evide i	e Antine
Directory	maxaay reenroi ir a ouplicate ce	rundate exists i	THEORINE

4. [Request Handling] タブに移動し、[Allow private key to be exported] にチェックを入れます

。また、[Purpose] ドロップダウン メニューで [Signature and Encryption] が選択されている

operties of Ne	w Template	?			
Issuance Requi General	irements   Superseded Templates Request Handling	Extensions Securit Subject Name			
Purpose:	Signature and encryption	•			
	Archive subject's encryption pr	rivate key			
	🔲 Include symmetric algorithms a	llowed by the subject			
	Delete revoked or expired certi	ficates (do not archive)			
Minimum key s	ize: 1024 🔻				
	te key to be evported				
1. Saion bung	te key to be exported				
Do the followin associated with	g when the subject is enrolled and w h this certificate is used:	hen the private key			
C Enroll subje	ect without requiring any user input				
C Prompt the	user during enrollment				
C Prompt the private key	user during enrollment and require units used	ser input when the			
To choose which cryptographic service providers <u>C</u> SPs					
		annal Anch			
		and Shha			

ことを確認します。

5. [Requests must use one of the following CSPs] を選択し、[Microsoft Base Cryptographic Provider v1.0] にチェックマークを入れます。その他の CSP のチェックマークはすべて外して、[OK] をクリックします。

CSP Selection ? 🗙						
Choose which cryptographic service providers (CSPs) can be used in requests:						
C Requests can use any CSP available on the subject's computer						
Requests must use one of the following CSPs:						
<u>C</u> SPs:						
Gemplus GemSAFE Card CSP v1.0						
Infineon SICRYPT Base Smart Card CSP						
✓Microsoft Base Cryptographic Provider v1.0						
Microsoft Base DSS and Diffie-Hellman Cryptographic Provider						
Microsoft DH SChannel Cryptographic Provider						
Microsoft Enhanced Cryptographic Provider v1.0						
Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Prov						
Microsoft Enhanced RSA and AES Cryptographic Provider						
Microsoft BSA SChannel Cryntographic Provider						
OK Cancel						
OK Cancel Apply						

6. [Subject Name] タブに移動し、[Supply in the request] を選択して [OK] をクリックします。

	emplate	1
Issuance Requireme	ents Superseded Templates	s   Extensions   Security
General	Request Handling	Subject Name
Supply in the re	equest	
Select this opti not have acces Autoenrollment	on to allow a variety of subject ss to the domain of which the s is not allowed if you choose th Active Directory information	name formats or if you do subject is a member. his option.
Select this option simplify certificate Subject name for	n to enforce consistency amon e administration. imat:	g subject names and to
None		<b>V</b>
🗖 Include e-ma	ail name in subject name	
Include this infor	mation in alternate subject nam	ne:
monore das anot		
E-mail name		
E-mail name		
E-mail name	al name (UPN)	
E-mail name     DNS name     User prinicip     Service prine	al name (UPN) cipal name (SPN)	
E-mail name     DNS name     User prinicip     Service princ	al name (UPN) cipal name (SPN)	

- [Security] タブに移動して、[Domain Admins Group] を選択し、[Allowed] の下部にある [Enroll] オプションにチェックマークが入っていることを確認します。注:このActive Directory情報から構築することを選択した場合は、[User principal name (UPN)] のみをオン にし、[Include email name in subject name and E-mail name]をオフにします。これは、 Active Directory Users and Computersスナップインでワイヤレスユーザアカウントに電子メ ール名が入力されていないためです。これらの2つのオプションを無効にしなかった場合は 、自動登録による電子メールの使用が試行され、その結果、自動登録のエラーが発生します。
- 8. 証明書が自動的にプッシュされてしまうことを防止する必要がある場合は、追加のセキュリ ティ対策が用意されています。これらの機能は、[Issuance Requirements] タブにあります 。このドキュメントでは、詳細は説明しません。

operties of New Templ	ate		?
General   Issuance Requirements	Request Handling Superseded Templ	Sub lates   Extensi	oject Name ions   Security
Require the following for a	enrollment: er approval		
This number of author	rized signatures:	0	
If you require more th	ian one signature, au	utoenrollment is	not allowed.
Edicy type required in	signature:		
Application policy:			×
I <u>s</u> suance policies:			
			Add Remove
Require the following for r Same criteria as for er C Valid existing certifica	nroliment te	Cancel	Apply

9. [OK] をクリックしてテンプレートを保存し、[Certificate Authority] スナップインからこのテ ンプレートを発行するようにします。

<u>新しい ACS Web サーバ証明書テンプレートの有効化</u>

- 1. [Certification Authority] スナップインを開きます。「<u>ACS Web サーバ用の証明書テンプレー</u> <u>トの作成</u>」セクションのステップ 1 ~ 3 を実行し、[Certificate Authority] オプションを選択 し、[Local Computer] オプションを選択して [Finish] をクリックします。
- 2. [Certificate Authority] コンソール ツリーで、**ca.demo.local** を展開し、[Certificate Templates] を右クリックします。
- 3. [New] > [Certificate Template to Issue] に移動します。

🔯 Certification Authority							
<u>File Action View Help</u>							
	1 😫 💵						
i Certification Authority (Loc	:al)	Name					
🖻 😰 ca.demo.local		🔯 Direc	tory Email Replication				
Revoked Certificat	es	Dom 🔯	ain Controller Authentication				
Issued Certificates	;	🔯 EFS I	Recovery Agent				
Pending Requests		🙀 Basic EFS					
Failed Requests		Controller					
	Manage		Server				
			huter				
	<u>N</u> ew	<u> </u>	Certificate Template to Issue				
	View	•	rdinate Certification Authority				
			histrator				
Refresh							
	Export L	įst					
	<u>H</u> elp						

#### 4. ACS Certificate Template をクリックします。

Name	Intended Purpose	
R ACS	Server Authentication	
Authenticated Session	Client Authentication	
🙀 CA Exchange	Private Key Archival	
CEP Encryption	Certificate Request Agent	
🙀 Code Signing	Code Signing	_
2 Cross Certification Authority	<alb< td=""><td></td></alb<>	
🗱 Enrollment Agent	Certificate Request Agent	
🗱 Enrollment Agent (Computer)	Certificate Request Agent	
Exchange Enrollment Agent (Offline request)	Certificate Request Agent	
🗱 Exchange Signature Only	Secure Email	
Exchange Liser	Secure Email	·

- 5. [OK] をクリックし、[Active Directory Users and Computers] スナップインを開きます。
- 6. コンソール ツリーで [Active Directory Users and Computers] をダブルクリックし、 demo.local を右クリックして [Properties] をクリックします。


7. [Group Policy] タブで、[Default Domain Policy] をクリックし、次に [Edit] をクリックします 。これにより、Group Policy Object Editor スナップインが開きます。

demo.local Properties		? ×			
General Managed By Group Policy					
To improve Group Policy management, upgrade Management Console (GPMC). Current Group Policy Object Links for	to the Group Po or demo	olicy			
Group Policy Object Links	No Override	Disabled			
Group Policy Objects higher in the list have the h This list obtained from: AD2003.demo.local	nighest priority.				
New     Add     Edit       Options     Delete     Properties		Up Do <u>w</u> n			
Elock Policy inheritance					
Close	Cancel	Apply			

8. コンソール ツリーで、[Computer Configuration] > [Windows Settings] > [Security Settings] > [Public Key Policies] を展開して、[Automatic Certificate Request Settings] を選択します。



- 9. [Automatic Certificate Request Settings] を右クリックして、[New] > [Automatic Certificate Request] を選択します。
- 10. [Welcome to the Automatic Certificate Request Setup Wizard] ページで [**Next**] をクリック します。
- 11. [Certificate Template] ページで [Computer] をクリックし、[Next] をクリックします。

Automatic Certificate Request Setup V	Yizard 🗙
Certificate Template The next time a computer logs on, a provided.	certificate based on the template you select is
A certificate template is a set of prede computers. Select a template from the Certificate templates:	efined properties for certificates issued to e following list.
Name	Intended Purposes
Computer Domain Controller Enrollment Agent (Computer) IPSec	Client Authentication, Server Authenticatior Client Authentication, Server Authenticatior Certificate Request Agent IP security IKE intermediate
•	<b>&gt;</b>
	< <u>B</u> ack <u>N</u> ext > Cancel

12. Automatic Certificate Request Setup Wizard ページが完了したら、[Finish] をクリックしま す。[Group Policy Object Editor] スナップインの詳細ペインに、コンピュータ証明書の種類 が表示されます。

Group Policy Object Editor							
Elle Action View Help							
S Default Domain Policy [AD2003.demo.local] Policy	Automatic Certificate Request						
E-B Computer Configuration	Computer						
Software Settings							
- Windows Settings							
<ul> <li>Scripts (Startup/Shutdown)</li> </ul>							
E-B Security Settings							
Account Policies							
Local Policies							
🖭 🚽 Event Log							
Restricted Groups							
E System Services							
Registry							
🕖 🤷 File System							
Wireless Network (IEEE 802.11) Policies							
Public Key Policies							
Automatic Certificate Request Settings							
Enterprise Trust							
Software Restriction Policies							
IP Security Policies on Active Directory (demo.local)							
Administrative Templates							
E User Configuration							
Software Settings							
Windows Settings							
⊡ Administrative Templates							

- 13. コンソール ツリーで、[User Configuration] > [Windows Settings] > [Security Settings] > [Public Key Policies] を展開します。
- 14. 詳細ペインで [Auto-enrollment Settings] をダブルクリックします。

🚡 Group Policy Object Editor						
<u>Eile Action View H</u> elp						
🗊 Default Domain Policy [AD2003.demo.local] Policy	Object Type					
🗄 🜆 Computer Configuration	Enterprise Trust					
🖻 🚛 User Configuration	Autoenrollment Settings					
🗄 📲 Software Settings						
🗄 📲 Windows Settings						
Remote Installation Services						
🗐 Scripts (Logon/Logoff)						
🖻 😳 Security Settings						
🖻 📥 Public Key Policies						
Enterprise Trust						
🕀 💼 Software Restriction Policies						
En Folder Redirection						
🗄 🖓 Internet Explorer Maintenance						
🖅 🧰 Administrative Templates						

15. [Enroll certificates automatically] を選択し、[Renew expired certificates, update pending certificates and remove revoked certificates] と [Update certificates that use certificate templates] にチェックマークを入れます。

Autoenrollment Settings Properties
General
Enroll user and computer certificates automatically
<ul> <li>Do not enroll certificates automatically</li> <li>Enroll certificates automatically</li> </ul>
Renew expired certificates, update pending certificates, and remove revoked certificates
Update certificates that use certificate templates
UK Cancel Apply

16. [OK] をクリックします。

# <u>ACS 5.1 証明書のセットアップ</u>

### エクスポート可能な ACS 用証明書の設定

**注**:ACSサーバは、WLAN PEAPクライアントを認証するために、エンタープライズルートCAサ ーバからサーバ証明書を取得する必要があります。 **注**:証明書の設定プロセス中にIISマネージャが開いていないことを確認してください。キャッシュされた情報に問題が発生するためです。

- 1. Admin 権限を持っているアカウントで、ACS サーバにログインします。
- 2. [System Administration] > [Configuration] > [Local Server Certificates] に移動します。[Add] をクリックします。

> CA My Workspace	Conte		desinistration - Cont		ine a Local Pressor C	antification is		and final and	Contraction of the second s
· da Network Dessures	System Administration > Configuration > Local Server Certificates > Local Certificates								
Network Resources	Loc	cal	Certificates				Show	ning 1-1 of 1 50 💌	per page Go
<ul> <li>Weight Users and Identity Stores</li> </ul>	Fil	ter:			Match if.		*	Go 🔻	
Policy Elements	F		Friends Hama		lanuad Ta	in and D	_	Mallel From	Valid To (T)
Access Policies			Friendly Name	-	Issued 10	Issued B	y	valid From	Valid To (Ex
Monitoring and Reports			<u>acs</u>		acs	acs		04:29 20.09.2010	04:29 20.09
🔹 💐 System Administration									
<ul> <li>Administrators         Accounts         Roles         <ul> <li>Settings</li> </ul> </li> <li>Users         Authentication Settings</li> <li>Operations         Distributed System Management         Software Repositories         Centralized Software Updates         Scheduled Backups</li> <li>Local Operations</li> <li>Configuration         <ul> <li>Global System Options</li> <li>Dictionaries</li> <li>Local Server Certificates             <ul> <li>Local Server Certificates</li> <li>Outstanding Signing Requests</li> <li>Log Configuration</li> <li>Licensing</li> </ul> </li> <li>Downloads         Migration Utility         User Change Password</li> </ul></li></ul>									
Sample Python Scripts	Ad	d	Edit Delete	[	Export		1	Page 1	of 1

3. サーバ証明書の作成方法は、[Generate Certificate Signing Request] を選択します。[next] を クリックします。



4. 次の例のように証明書のサブジェクトとキーの長さを入力して、[Finish] をクリックします 。[Certificate Subject] : **CN=acs.demo.local**[Key

Length] : 1024



5. ACS で、証明書署名要求が生成されたことを通知するプロンプトが表示されます。[OK] を クリックします。

Windows Internet Explorer						
⚠	A server certificate signing request has been generated and can be viewed in the "Outstanding Signing Requests" list.					
	ок					

 [System Administration] で、[Configuration] > [Local Server Certificates] > [Outstanding Signing Requests] に進みます。注:この手順を実行する理由は、Windows 2003ではエクス ポート可能なキーを使用できないため、エクスポート可能なキーを使用するために事前に作 成したACS証明書に基づいて証明書要求を生成する必要があるためです。



7. [Certificate Signing Request] のエントリを選択して、[Export] をクリックします。

![](_page_46_Picture_0.jpeg)

8. ACS 証明書の .pem ファイルをデスクトップに保存します。

Save As					? ×
Save in:	Desktop		. 00	P 📑	
My Recent Documents Desktop My Documents My Computer	My Documents My Computer	aces			
My Network	File name:	ACS_ctr		•	Save
Places	Save as type:	.pem Document			Cancel

## <u>ACS 5.1 ソフトウェアでの証明書のインストール</u>

次のステップを実行します。

1. ブラウザを開き、CA サーバ URL http://10.0.10.10/certsrv に接続します。

	- 47 × U
	<u>a</u>
oes not currently ocess of being up you still experier site administrato rator and feel you lease see "Enable Connect to cade Connecting to ca H User name: Bassword:	y have a pgraded and ence the or.
	oes not currently ocess of being u i you still experie site administrato rator and feel yo lease see "Enab State Connect to ca.d Connecting to ca User name: Password:

2. [Microsoft Certificate Services] ウィンドウを表示します。[Request a certificate] を選択しま

![](_page_47_Picture_2.jpeg)

3. クリックして [Advanced certificate request] を送信します。

す。

![](_page_48_Figure_0.jpeg)

4. [Advanced Certificate Request] で、[Submit a certificate request using a base-64encoded...] をクリックします。

![](_page_48_Picture_2.jpeg)

5. ブラウザのセキュリティで許可されている場合は、[Saved Request] フィールドで前の ACS 証明書の要求ファイルをブラウズして挿入します。

Microsoft Certific	ate Services ca.demo.local Ho	me
Submit a Certi	ficate Request or Renewal Request	
To submit a sav #10 certificate r source (such as	red request to the CA, paste a base-64-encoded CMC or PKCS request or PKCS #7 renewal request generated by an external a Web server) in the Saved Request box.	
Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	≍ Browse for a file to insert.	
Certificate Temp	late:	
	Administrator	
Additional Attribu	ites:	
Attributes:	x X	
	Submit >	

6. ブラウザのセキュリティ設定によっては、ディスクのファイルにアクセスできない場合があります。その場合は、[OK] をクリックして手動で貼り付けます。

Windows	Windows Internet Explorer						
1	Your web browser security settings prohibit this page from accessing your disk. Either paste the data into this page manually, or add this page to your browser's list of trusted sites.						
	ОК						

7. 前の ACS エクスポートから ACS \*.pem ファイルを探します。テキスト エディタ(Notepad など)を使用して、ファイルを開きます。

ACS_csr PEM File 1 KB	
<b>Open</b> Edit	
Open With 🕨	🝺 Notepad
Send To 🕨	🏉 Internet Explorer
Cut	Choose Program
Copy Create Shortcut	-
Delete	
Rename	_
Properties	

8. ファイルの内容をすべて選択して、[Copy] をクリックします。

📕 ACS_csr - Notepad	
File Edit Format Viev	v Help
BEGIN CERTI	Undo
	Cut
	Copy States

9. [Microsoft Certificate Services] ウィンドウに戻ります。コピーした内容を [Saved Request]

Microsoft Certific	ate Servi	ces ca	a.demo.loca
Submit a Certi	ficate F	Reques	t or Rene
To submit a say	ved reau	uest to th	ne CA, pa
renewal reques	t genera	ated by a	an externa
Saved Request:			
Base-64-encoded		Undo	
(CMC or		Cut	
PKCS #10 or PKCS #7):		Copy	
,	4	Delete	
	Browse	Select Al	ett.
Certificate Templ	late:		
	Adminis	trator	

フィールドに貼り付けます([Paste])。

10. [Certificate Template] として [ACS] を選択して、[Submit] をクリックします。

Saved Request:	
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	YIZIAYb4QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUA DXoioRABct447w077+uAk8crn26oaEhcfG/ZR15X ONZQ5xnrK23yxEdQNvSFC30mzRZEbQq4s5MvPEZZ /MWqXej3NjpicpAgiV8CSwNd END CERTIFICATE REQUEST
Certificate Temp	ACS
Attributes:	× *
	Submit >

11. 証明書が発行されたら、[Base 64 encoded] を選択して、[Download certificate] をクリック

Certificate Issued	
The certificate you request	ed was issued to you.
C DER encode	ed or Gase 64 encoded
Download certs	ficate
Download certi	ticate chain
	File Download - Security Warning
	Do you want to open or save this file?
	Name: certnew.cer
	From: ca
	One Swe 1
	While files from the laternat can be useful this file tone of
	potentially harm your computer. If you do not trust the sou

12. [Save] をクリックして、証明書をデスクトップに保存します。

![](_page_52_Picture_0.jpeg)

13. [ACS] > [System Administration] > [Configuration] > [Local Server Certificates] に移動しま す。[Bind CA Signed Certificate] を選択して、[Next] をクリックします。

![](_page_52_Picture_2.jpeg)

14. [Browse] をクリックして、保存した証明書を探します。

<ul> <li>Select server certificate creation method</li> <li>Bind CA S</li> </ul>	igned Certificate
Step 2 -Bind CA Signed Certificate	
Certificate File:	Browse
Protocol	
EAP: Used for EAP protocols that use SSL/TLS tunn	eling
Management Interface: Used to authenticate the well	b server (GUI)
Override Policy	
A certificate being imported may be determined to alread Subject or Issuer and serial number as an existing certifi "Replace Certificate" option will allow the certificate contre existing protocol selections for the certificate.	ly exist in ACS when it has either the same icate. In such a case, selection of the ents to be replaced while retaining the
Replace Certificate	

15. CA サーバにより発行された ACS 証明書を選択して、[Open] をクリックします。

Choose file					2	×
Look in:	Desktop		•	+ 🖻 💣	-	
My Recent Documents Desktop My Documents My Computer	My Documents My Computer My Network Pla ACS_cert ACS_csr	1085				
My Network	File name:	ACS, cert		•	Open	1
Places	Files of type:	All Files (".")			Cancel	

16. また、[Protocol] の [EAP] チェックボックスをオンにして、[Finish] をクリックします。

![](_page_54_Picture_0.jpeg)

17. ACS の [Local Certificate] に、CA により発行された ACS 証明書が表示されます。

System /	system Administration > Configuration > Local Server Certificates > Local Certificates							
Local Certificates Showing 1-2 of 2 50 💌								
Filter	:		Match if:	•	Go 🔻			
	Friendly Name	•	Issued To	Issued By	Valid From			
	acs		acs	acs	04:29 20.09.2010			
	acs.demo.local		acs.demo.local	ca.demo.local	10:39 22.09.2010			

#### <u>Active Directory の ACS ID ストアの設定</u>

次のステップを実行します。

- 1. ACS に接続して、Admin アカウントにログインします。
- 2. [Users and Identity Stores] > [External Identity Stores] > [Active Directory] に移動します。

![](_page_55_Picture_0.jpeg)

3. [Active Directory Domain] に *demo.local* と入力し、サーバのパスワードを入力して、[Test Connection] をクリックします。[OK] をクリックして続行します。

General Directory Gro	ps Directory Attributes	
Connection Details		
Active Directory Domai Name:	demo.local	
Please specify the crede	tials used to join this machine to the Active Directory Domain:	
OUsername:	administrator	
O Password		
reachable.	Test Connection	ory Donna
click on 'Save Changes' nave successfully conne	Test Connection	on. Once y
reachable. Click on 'Save Changes' have successfully conne to be available for use in	Test Connection  Connect to the Active Directory Domain and save this configuration  Connect to the Domain, yo  Windows Internet Explorer  Connection test to 'demo.local' success	on. Once y
Click on 'Save Changes' have successfully conne to be available for use in End User Authenticatio	Test Connection Connect to the Active Directory Domain and save this configuration to the Domain, your Windows Internet Explorer Connection test to 'demo.local' succe Settings	on. Once y
Click on 'Save Changes' have successfully conne to be available for use in End User Authenticatio F Enable password	Test Connection  Connect to the Active Directory Domain and save this configuration  Connection test to 'demo.local' succes  Settings  hange OK	on. Once y x ibut eded.
Click on 'Save Changes' have successfully conne to be available for use in End User Authenticatio I Enable password Enable machine a	Test Connection  Connect to the Active Directory Domain and save this configuration  Connection test to 'demo.local' succe  Settings  thange thentication	on. Once y

4. [Save Changes] をクリックします。

![](_page_56_Picture_0.jpeg)

**注**: ACS 5.x統合手順の詳

細については、『<u>ACS 5.x以降:Microsoft Active Directoryとの統合の設定例</u>』を参照してく ださい。

### ACS への AAA クライアントとしてのコントローラの追加

次のステップを実行します。

1. ACS に接続して、[Network Resources] > [Network Devices and AAA Clients] に移動します

► 🛠 My Workspace	Network Resources > Network Devices an
<ul> <li>Network Resources</li> </ul>	Network Devices
<ul> <li>Network Device Groups Network Devices and AAA Clients</li> </ul>	Filter: Match
Default Network Device External RADIUS Servers	Name • IP/Mask N
<ul> <li>Jusers and identity Stores</li> </ul>	No data to display
Policy Elements	
Access Policies	
Monitoring and Reports	
<ul> <li>System Administration</li> </ul>	
	Create Duplicate Edit 0

。[Create] をクリックします。

2. 次のフィールドを入力します。[Name] : **wlc**[IP] : **10.0.1.10**[RADIUS] チェックボックス : **オ** ン[Shared

Description:	100		
Location	All Locations		Select
Device Type	All Device Types		Select
IP Address Single IP Address IP: 10.0.1.10	C IP Range (s)	Authentication Options TACACS+ Shared Secret Single Connect Device C Legacy TACACS+ Sin TACACS+ Draft Comp Support RADIUS RADIUS Shared Secret Cisco TrustSec Vuse Device ID for Trust Device ID: Password: TrustSec Advanced Set	e Igle Connect Sup pliant Single Con Sec identification

Secret] : cisco

3. 完了したら、[Submit] をクリックします。[ACS Network Devices] リストで、コントローラ がエントリとして表示されます。

My Workspace	Network	Resources	i > Ne	twork Devices an	d AAA Clients	
Network Resources	Netw	vork Devic	es			Showing 1-1 of 1
Network Device Groups     Network Devices and AAA Clients	Filte	r 🗌		Match	it:	Go ▼
Default Network Device External RADIUS Servers		Name	•	IP / Mask	NDG:Location	NDG:Device Type
B Users and Identity Stores		wic		10.0.1.10/32	All Locations	All Device Types
Policy Elements						
Access Policies						
Monitoring and Reports						

## <u>ワイヤレス用 ACS アクセス ポリシーの設定</u>

次のステップを実行します。

1. ACS で、[Access Policies] > [Access Services] に移動します。

![](_page_59_Figure_0.jpeg)

2. [Access Services] ウィンドウで、[Create] をクリックします。

Access Services Showing 1-2 of 2  Filter: Match if: Default Device Administration Genetity Default Device Administration Genetity Default Network Access Net	Access P	olicies > Access Services			
Filter:       Match it:       Image: Comparison of the service Type       Included Policies       Description         Default Device Admin       Device Administration       Identity       Default Device         Default Network Access       Network Access       Identity       Authorization       Default Network         Default Network Access       Network Access       Identity       Authorization       Default Network         Create       Duplicate       Edit       Default       Default       Network       Identity	Acces	s Services		Showing 1-2 of 2	50 💌 per p
Image: Name       Service Type       Included Policies       Description         Default Device Admin       Device Administration       Identity       Default Device         Default Network Access       Network Access       Identity       Default Network         Identity       Authorization       Default Network       Default Network         Identity       Authorization       Default Network	Filter:	Match it	t 💌	Go 🔻	
Default Device Admin     Device Administration <u>Identity     Authorization     Default Network Access     Network Access     <u>Identity     Authorization     Default Net     Default Network Access     Lidentity     Default Network     Default Network Access     Lidentity     Default Network     Default Network Access     Lidentity     Default Network     Default N</u></u>		Name 🔺	Service Type	Included Policies	Description
		Default Device Admin	Device Administration	Identity Authorization	Default Devi
Create Duplicate Edit Delete		Default Network Access	Network Access	Identity Authorization	Default Netv
Create Duplicate Edit Delete Mage 1 of 1	1				1
	Creat	te Duplicate Edit	Delete	Page	1 of 1

3. アクセス サービスを作成して、名前(例:WirelessAD)を入力します。[Based on service

```
template] を選択して、[Select] をクリックします。
```

Access Policies > Access Services > Cr	eate
General Allowed Protocols	
Step 1 - General	
General	
• Name: WirelessAD	
Description:	
Access Service Policy Structure	e
Based on service template	Select
C Based on existing service	Select
C User Selected Service Type	Network Access

4. [Webpage Dialog] で、[Network Access – Simple] を選択します。[OK] をクリックします。

Acce	ess Services		Showing 1-4
Filte	r: 💌 Match if: 🔍	Go 🔻	
	Name 🔺	Service Type	Description
0	Device Admin - Command Auth	Device Administration	
C	Device Admin - Simple	Device Administration	
0	Network Access - MAC Authentication Bypass	Network Access	
•	Network Access - Simple	Network Access	

5. [Webpage Dialog] で、[Network Access – Simple] を選択します。[OK] をクリックします。 テンプレートを選択したら、[Next] をクリックします。

Step 1 - General					
General O Name: WirelessAD					
Description:					
Access Service Policy Structur	e				
<ul> <li>Based on service template</li> </ul>	Network Access - Simple	Select			
C Based on existing service		Select			
O User Selected Service Type	Network Access				

6. [Allowed Protocols] で、[Allow MS-CHAPv2] および [Allow PEAP] チェックボックスをオン

![](_page_61_Picture_0.jpeg)

にします。[Finish] をクリックします。

7. ACS により表示される新しいサービスをアクティブにするかを尋ねるプロンプトで、[Yes] をクリックします。

D				Authorization
n v		WirelessAD	Network Access	Identity Authorization
and Reports				
				<b></b>
Access Service?	created	successfully. Would	I you like to modify the Service	Selection policy to activate
		Ye	s No	

8. 作成およびアクティブ化した新しいアクセス サービスで、[Identity] を展開して選択します。[Identity Source] で、[Select] をクリックします。

![](_page_62_Picture_0.jpeg)

9. ACS に設定した Active Directory に [AD1] を選択し、[OK] をクリックします。

¢	Cisco	Secure ACS	We	bpage Dialog
	Identit	y Store		
	Filter:		٣	Match if: Go 🔻
		Name	-	Description
	С	AD1		
	0	CN Usernan	ne	Predefined Certificate Authentication Profile
	0	DenyAccess		
	0	Internal Hos	ts	
	0	Internal Use	rs	
	0	NAC Profiler		Default Entry for NAC Profiler

10. [Identity Source] が [AD1] であることを確認して、[Save Changes] をクリックします。

Access Policies > Access Services > WirelessAD > Identity					
Single result selection C Rule based result selection					
Identity Source: AD1	Select				
Advanced Options					

## <u>ACS アクセス ポリシーとサービス ルールの作成</u>

次のステップを実行します。

1. [Access Policies] > [Service Selection Rules] に移動します。

						VALUE AND A DESCRIPTION OF A DESCRIPTON OF A DESCRIPTION OF A DESCRIPANTE A DESCRIPANTE A DESCRIPTA DESCRIPTION OF A DESCRIPT
▶ 🛠 My Workspace	Access Policies > Access Services > Service Selection Rules					
Image:	0	Single i	result sele	ection @	Rule based result	selecti
Users and Identity Stores	Ser	vice Se	election P	olicy		
Policy Elements	Filt	er: Sta	atus	Match if	Equals 💌	
👻 🛼 Access Policies	-		-			Cond
<ul> <li>Access Services</li> </ul>			Status	Name	Protocol	Cona
Service Selection Rules     O Default Device Admin	1			Rule-1	match Radius	
Default Network Access	2		Θ	Rule-2	match Tacacs	
<ul> <li>Ø WirelessAD Identity Authorization</li> </ul>						

2. [Service Selection Policy] ウィンドウで [Create] をクリックします。新しいルールに名前を 付けます(例: *WirelessRule*)。[Protocol] のチェックボックスをオンにして、[Radius] と 一致させます。

Cisco Secure ACS Webpage Dialog	
General Name: WirelessRule Status:	Enabled 💌 😬
The Customize button in the I conditions and results are available	ower right area of the policy rules scree ailable here for use in policy rules.
Conditions Protocol: match	Select
Results	
	🖉 Cisco Secure ACS Webpage Di
	Enum Definition
	Enum Name ID
	C Radius 0

Tacacs

1

C

- 3. [Radius] を選択して、[OK] をクリックします。
- 4. [Results] の [Service] に、[WirelessAD] を選択します(前の手順で作成したもの)。

Conditions			
Protocol: ma	itch	<ul> <li>Radius</li> </ul>	Sele

5. 新しいワイヤレス ルールを作成したら、そのルールを選択して一番上に移動([Move])し ます。一番上のルールは、Active Directory を使用したワイヤレス Radius 認証の識別に使用

Ser	vice S	election P	olicy			199369
Filb	er: Sta	atus	Match if: Equa	uls 💌		Clear
		Status	Name	Protocol	Conditions	
3			WirelessRule	match Radius		
1		0	Rule-1	match Radius		
2			Rule-2	match Tacacs		
-1				$\backslash$		
4	-	Default		If no rules detin	ed or no enab	led ru

される最初のルールになります。

## <u>Windows の自動機能を使用した PEAP 用クライアントの設定</u>

この例では、CLIENT は、Windows XP Professional SP2 が稼働し、無線クライアントとして機 能していて、無線 AP 経由でイントラネット リソースにアクセス可能なコンピュータです。 CLIENT をワイヤレス クライアントとして設定するには、このセクションの手順を実行します。

#### 基本的なインストールと設定の実行

次のステップを実行します。

- 1. イーサネット ケーブルを使用して CLIENT をハブに接続し、イントラネット ネットワーク セグメントに接続します。
- 2. CLIENT に、Windows XP Professional SP2 をインストールします。このインストールでは 、demo.local ドメインの CLIENT という名前のメンバー コンピュータとして設定します。

3. Windows XP Professional SP2 をインストールします。このインストールは、PEAP をサポ ートするために必要です。注: Windows XP Professional SP**2で**は、Windowsファイアウォ ールは自動的に有効になります。ファイアウォールは無効にしないでください。

<u>ワイヤレス ネットワーク アダプタのインストール</u>

次のステップを実行します。

- 1. CLIENT コンピュータをシャットダウンします。
- 2. CLIENT コンピュータとイントラネット ネットワーク セグメントの接続を解除します。
- 3. CLIENT コンピュータを再起動し、ローカル管理者アカウントを使用してログインします。
- ワイヤレス ネットワーク アダプタをインストールします。注:ワイヤレスアダプタ用の製 造元の設定ソフトウェアはインストールしないでください。ワイヤレス ネットワーク アダ プタ ドライバのインストールには、Add Hardware Wizard を使用します。また、プロンプ トが表示された場合は、製造元から提供された CD、または Windows XP Professional SP2 用の最新ドライバが入っているディスクを挿入します。

#### ワイヤレス ネットワーク接続の設定

次のステップを実行します。

- 1. ログオフし、demo.local ドメインの WirelessUser アカウントを使用してログインします。
- 2. [Start] > [Control Panel] を選択し、[Network Connections] をダブルクリックして、[Wireless Network Connection] を右クリックします。
- 3. [Properties] をクリックし、[Wireless Networks] タブに移動して、[Use Windows to configure my wireless network settings] にチェックマークが入っていることを確認します。

👃 Wireless Network Connection Pr	roperties <b>?</b> X
General Wireless Networks Advan	ced
Use Windows to configure my wi	eless network settings
Available networks:	
To connect to, disconnect from, or about wireless networks in range, or	find out more information lick the button below.
	View Wireless Networks
Preferred networks: Automatically connect to available below:	networks in the order listed Move up Move down
Add Remove	Properties work Advanced
	OK Cancel

4. [Add] をクリックします。

- 5. [Association] タブで、[Network name (SSID)] フィールドに *Employee* と入力します。
- 6. [Network Authentication] に [WPA] を選択して、[Data encryption] が [TKIP] に設定されてい

Wireless network propertie	s ?X
Association Authentication	Connection
Network name (SSID):	Employee
Wireless network key	
This network requires a ke	y for the following:
Network Authentication:	WPA 💌
Data encryption:	TKIP
Network key:	
Confirm network key:	
Key index (advanced):	
The key is provided for	r me automatically
This is a computer-to-con access points are not us	mputer (ad hoc) network; wireless ed
	OK Cancel

ることを確認します。

- 7. [Authentication] タブをクリックします。
- 8. EAP type で **Protected EAP (PEAP)** を使用するように設定されていることを確認します。設定されていない場合は、ドロップダウン メニューから選択します。
- 9. ログイン前にマシンの認証を実行する場合は(この場合、ログイン スクリプトやグループ ポリシー プッシュを適用できます)、[Authenticate as computer when computer information is available] にチェックマークを入れます。

Wireless net	work properties	?×
Association	Authentication Connection	
Select this wireless Eth	option to provide authenticated network access for hemet networks.	
☑ Enable	IEEE 802.1x authentication for this network	
EAP type:	Protected EAP (PEAP)	
Authen availab	Propertie ticate as computer when computer information is le ticate as guest when user or computer information is able	25
	OK Ca	ncel

- 10. [Properties] をクリックします。
- 11. PEAP には、クライアントによるサーバの認証が含まれているため、[Validate server certificate] がチェックされていることを確認します。また、[Trusted Root Certification Authorities] メニューで、ACS 証明書として発行された CA にチェックマークが付いていることを確認します。
- 12. [Select Authentication Method] に [Secured password (EAP-MSCHAP v2)] を選択します。 これは内部認証として使用されます。

Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
C&W HKT SecureNet CA Root CA 1 Ca.demo.local Certiposte Classe A Personne Certiposte Serveur Certisign - Autoridade Certificadora - AC2 Certisign - Autoridade Certificadora - AC4
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Enable Fast Reconnect
OK Cancel

- 13. [Enable Fast Reconnect] チェックボックスがオンになっていることを確認します。次に、 [OK] を 3 回クリックします。
- 14. システムトレイのワイヤレス ネットワーク接続のアイコンを右クリックして、[View Available Wireless Networks] をクリックします。
- 15. Employee のワイヤレス ネットワークをクリックし、[Connect] をクリックします。接続が 成功した場合は、ワイヤレス クライアントに [Connected] と表示されます。

![](_page_68_Picture_4.jpeg)

- 16. 認証が成功したら、Network Connections を使用して、ワイヤレス アダプタの TCP/IP 設 定を確認します。ワイヤレス アダプタには、10.0.20.100 ~ 10.0.20.200 の範囲内のアドレ スが、DHCP スコープ、または CorpNet ワイヤレス クライアント用に作成したスコープか ら割り当てられます。
- 17. 機能をテストするため、ブラウザを開いて、http://10.0.10.10(または、CA サーバの IP ア ドレス)を表示します。

## ACS を使用したワイヤレス認証のトラブルシューティング

次のステップを実行します。

1. [ACS] > [Monitoring and Reports] に移動して、[Launch Monitoring & Report Viewer] をクリ

![](_page_69_Figure_2.jpeg)

ックします。

2. 別の ACS ウィンドウが開きます。[Dashboard] をクリックします。

![](_page_69_Picture_5.jpeg)

3. [My Favorite Reports] セクションで、[Authentications – RADIUS – Today] をクリックします

y Favorite Reports	
Favorite Name	Report Name
ACS - Configuration Audit - Today	ACS Instance>ACS_Configuration_Audi
ACS - System Errors - Today	ACS Instance>ACS_System_Diagnostics
Authentications - RADIUS - Today	AAA Protocol>RADIUS_Authentication

4. ログにすべての RADIUS 認証が表示され、[Pass] または [Fail] が示されます。ログに記録さ れているエントリで、[Details] 列の**虫眼鏡のアイコン**をクリックします。

AAA Protocol > RADI	US Authentication					
Authentication Status : Date :	Pass or Fail September 22, 2010	Last 30	Minutes   Last Hour   L	<u>ast 12 Hours</u>   Today	Yesterday   Last	7 Days   Last 30 Days )
Generated on September	22, 2010 5:51:34 PM	PDT				
Reload						
✓=Pass ¥=Fail 🍳	-Click for details	=Mouse	over item for additio	nal information		
Logged At	RADIUS NAS Status Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method
Sep 22,10 5:51:17.843 F	M 🗸	9	wirelessuser	00-21-5c-69-9a-39	WirelessAD	PEAP (EAP-MSCHAPv2)

5. [RADIUS Authentication Detail] に、ログに記録されている試行内容の詳細情報が表示されま

AAA Protocol > RAI	DIUS Authentication Detail
ACS session ID : acs/ Date : Sep	/74551189/31 tember 22, 2010
Generated on Septemb	per 22, 2010 5:52:16 PM PDT
Authentication Summ	ary
Logged At:	September 22,2010 5:51:17.843 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	wirelessuser
MAC/IP Address:	00-21-5c-69-9a-39
Network Device:	wlc : 10.0.1.10 :
Access Service:	WirelessAD
Identity Store:	AD1
Authorization Profiles:	Permit Access
CTS Security Group:	
Authentication Method:	PEAP(EAP-MSCHAPv2)

0

6. ACS サービスの [Hit Count] に、ACS で作成したルールに一致する試行内容の概要を表示で

きます。[ACS] > [Access Policies] > [Access Services] に移動して、[Service Selection

Results Service	Hit Count
WirelessAD	33
Default Network Access	0

Rules] をクリックします。

#### <u>ACS サーバでの PEAP 認証の失敗</u>

ご使用のクライアントが ACS サーバの PEAP 認証に失敗した場合は、ACS の [Report and Activity] メニューの [Failed attempts] オプションに、「NAS duplicated authentication attempt」 エラーメッセージが表示されているかどうかを確認します。

クライアント マシンに Microsoft Windows XP SP2 がインストールされており、Windows XP SP2 が Microsoft IAS サーバ以外のサードパーティ サーバに対して認証を行う場合、このエラー メッセージを受け取る場合があります。特に、Cisco RADIUS サーバ(ACS)で使用する Extensible Authentication Protocol Type:Length:Value(EAP-TLV)フォーマット ID の計算方法が 、Windows XP が使用する方法と異なる場合に起こります。Microsoft では、これを XP SP2 サプ リカントの不具合と特定しています。

ホットフィックスについては、Microsoft に問い合わせいただき、『<u>PEAP authentication is not</u> <u>successful when you connect to a third-party RADIUS server</u>』を参照してください。根本的な問 題は、クライアント側の Windows ユーティリティで、PEAP の [Fast Reconnect] オプションが デフォルトでディセーブルになっているのに対し、サーバ側(ACS)ではデフォルトでイネーブ ルになっていることにあります。この問題を解決するには、ACS サーバ([Global System Options] の下)の [Fast Reconnect] オプションのチェックを外します。または、クライアント側 で [Fast Reconnect] オプションをイネーブルにして問題を解決することもできます。

次の手順を実行して、Windows ユーティリティを使用して Windows XP が稼働しているクライア ントで [Fast Reconnect] をイネーブルにします。

- 1. [Start] > [Settings] > [Control Panel] に移動します。
- 2. [Network Connections] アイコンをダブルクリックします。
- 3. [Wireless Network Connection] アイコンを右クリックして、[Properties] をクリックします。
- 4. [Wireless Networks] タブをクリックします。
- 5. [Use Windows to configure my wireless network settings] オプションを選択して、Windows でクライアント アダプタを設定できるようにします。
- 6. SSID を設定済みの場合は、SSID を選択して [Properties] をクリックします。設定していない場合は、[New] をクリックして新規の WLAN を追加します。
- 7. [Association] タブで SSID を入力します。[Network Authentication] が [Open] であり、[Data Encryption] が [WEP] に設定されていることを確認します。
- 8. [Authentication] をクリックします。
- 9. [Enable IEEE 802.1x authentication for this network] オプションを選択します。
- 10. [EAP Type] として [PEAP] を選択して、[Properties] をクリックします。
- 11. ページの下部の [Enable Fast Reconnect] オプションを選択します。
## <u>関連情報</u>

- <u>ACS 4.0 と Windows 2003 を使用した Cisco Unified Wireless Network 環境での PEAP</u>
- <u>Web</u> 認証用の Cisco ワイヤレス LAN コントローラ (WLC) および Cisco ACS <u>5.x(TACACS+)の設定例</u>
- <u>Cisco Secure Access Control System 5.1 のインストールとアップグレード 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。