# ACS 4.0 と Windows 2003 を使用した Unified Wireless Network 環境での EAP-TLS

## 内容

概要 前提条件 要件 使用する<u>コンポーネント</u> ネットワーク図 表記法 IIS、Certificate Authority、DNS、DHCP を使用する Windows Enterprise 2003 のセットアップ (DC\_CA) DC CA (wirelessdemoca) Cisco Secure ACS 4.0 を使用する Windows Standard 2003 のセットアップ 基本的なインストールと設定 Cisco Secure ACS 4.0 のインストール <u>Cisco LWAPP</u>コントローラの設定 WPA2/WPA に必要な設定の作成 EAP-TLS 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 4.0 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 4.0 ソフトウェアでの証明書のインストール Windows の自動機能を使用した EAP-TLS 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 ネットワーク接続の設定 関連情報

## <u>概要</u>

このドキュメントでは、Wireless LAN Controller(WLC)、Microsoft Windows 2003 ソフトウェ ア、および Cisco Secure Access Control Server(ACS)4.0 を使用して、Extensible Authentication Protocol-Transport Layer Security(EAP-TLS)によるセキュアな無線アクセスを 設定する方法について説明します。

**注:セキュリテ**ィワイヤレスの展開の詳細については、<u>Microsoft Wi-Fi Webサイト</u> および<u>Cisco</u> <u>SAFE Wireless Blueprintを参照してください</u>。

## <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 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 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> <u>ガイド: Cisco 4400 シリーズ ワイヤレス LAN コントローラ</u>.Cisco 2000 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 2000 シリーズ Wireless</u> LAN Controller.

開始する前に、テスト ラボの各サーバに 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 および AP をインストールし、最新のソフトウェア アップデートが設定されていることを確認し てください。

**重要:**このドキュメントの執筆時点における Windows Server 2003 の最新アップデートは SP1 で、Windows XP Professional の最新ソフトウェアは更新パッチ適用済みの SP2 です。

このドキュメントでは、EAP-TLS 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 SP 1 Enterprise Edition を使用していま す。これについては、このドキュメントの「<u>EAP-TLS 認証</u>」セクションで説明します。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。

- バージョン 3.2.116.21 が稼働する Cisco 2006 または 4400 シリーズ コントローラ
- Cisco 1131 Lightweight Access Point Protocol (LWAPP) 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)
- Access Control Server (ACS) 4.0 が稼働する Windows 2003 Standard
- 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 3560 スイッチ

### <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



このドキュメントの第1の目的は、ACS 4.0 と Windows 2003 Enterprise サーバを使用する Unified Wireless Network 環境で EAP-TLS 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)を搭載したWi-Fi Protected Access(WPA)/WPA2をSPを搭載したWindows XP Professionalに追加するには、『 <u>WPA2/Wireless Provisioning Services Information Element (WPS IE update)』を</u>を参照してくだ さいWindows XP SP2用。

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

DC\_CA ( wirelessdemoca )

DC\_CA とは、Windows Server 2003 Enterprise Edition SP1 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 wirelessdemo.local ドメインのドメイン コントローラ
- ・wirelessdemo.local DNS ドメインの DNS サーバ
- ・DHCP サーバ
- ・wirelessdemo.local ドメインのエンタープライズ ルート CA

DC\_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. DHCP をインストールして設定する。
- 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. <u>wirelessusers グループにユーザを追加する</u>
- 13. WirelessUsers グループにクライアント コンピュータを追加する。

#### ステップ1: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 SP1 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 172.16.100.26、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>ステップ2: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>

- 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 wirelessdemo.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 wirelessdemo と入力して、

Next をクリックします。

9. Database and Log Folders Location 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。

Active Directory Installation Wizard	×
<b>Database and Log Folders</b> Specify the folders to contain the Active Directory database and log file:	
For best performance and recoverability, store the database and the log hard disks.	on separate
Where do you want to store the Active Directory database?	
<u>D</u> atabase folder:	
C:\WINDOWS\NTDS	B <u>r</u> owse
Where do you want to store the Active Directory log? Log folder:	
C:\WINDOWS\NTDS	Br <u>o</u> wse
< <u>B</u> ack <u>N</u> ext>	Cancel

10. Shared System Volume ダイアログボックスで、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
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:
C:\\wINDOWS\SYSVOL B_owse
< <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 をクリックします。

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

<b>ummary</b> Beview and confirm the	options you selected.
You chose to:	
The new domain name i	is example.com. This is also the name of the new forest. 👘 💻
The NetBIOS name of t	he domain is EXAMPLE
Database folder: C:\WIN Log file folder: C:\WIND SYSVOL folder: C:\WIN	NDOWS\NTDS IOWS\NTDS IDOWS\SYSVOL
The DNS service will be will be configured to use	e installed and configured on this computer. This computer this DNS server as its preferred DNS server.
The password of the ne the administrator of this	w domain administrator will be the same as the password of computer.
To change an option, cl	ick Back. To begin the operation, click Next.
	< <u>B</u> ack <u>N</u> ext> Car

- 14. Completing the Active Directory Installation Wizard ページで、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>ステップ3: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 ([スタート] > [管理ツール] > [Active Directory Domains and Trusts])、ドメインコンピュー タDC\_CA.wirelessdemo.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。

Domain name:			1035 <b>-</b>
example.com			
Current domain functional level:			
Windows 2000 native			
Select an available domain funch	ional leviet		
Select an available domain funct Windows Server 2003	ional levet		<u> </u>
Mindows Server 2003 After you raise the domain f an domain functional levels	undional level, it carno undional level, it carno , click, Help.	t be reversed. For	more information
Select an available domain funct Windows Server 2003 After you raise the domain f on domain functional levels	unotional level, it carno , click. Help.	t be reversed. For	more information
Select an available domain funct Windows Server 2003 After you raise the domain f on domain functional levels	unotional level, it carno , click. Help.	t be reversed. For	more information

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。

#### <u>ステップ4:DHCPをインストールして設定する</u>

- 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ます([Start] > [Programs] > [Administrative Tools] > [DHCP])。次に、DHCPサーバDC\_CA.wirelessdemo.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 DC\_CA.wirelessdemo.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。

cope Name You have to p providing a de	provide an identifying scope name. You also have the option of escription.
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:	

- 7. [Next] をクリックし、次のようにパラメータを入力します。開始IPアドレス
  - :172.16.100.1[End IP address]:172.16.100.254長さ: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. <u>Start IP address</u> : 172 . 16 . 100 . 1 <u>End IP address</u> : 172 . 16 . 100 . 254 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 - 24 - 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 172.16.100.1、End IP address に 172.16.100.100 と入力します。次に、[Next] をクリックします。これにより、 172.16.100.1 ~ 172.16.100.100の範囲のIPアドレスが予約されます。これらの予約IPアドレ スはDHCPサーバによって割り当てられることはありません。

#### New Scope Wizard

#### Add Exclusions

Exclusions are addresses or a range of addresses that are not distributed by the server.



Type the IP address rang address, type an address	e that you want to exclude. in Start IP address only.	If you want to exc	clude a single
<u>S</u> tart IP address: 172 . 16 . 100 . 1	End IP address:	Add	
r Ex <u>e</u> luded address range:			
		Remo <u>v</u> e	
1			
	< <u>B</u>	ack <u>N</u> ext	> 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 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

11. Router (Default Gateway) ページで、デフォルト ルータ アドレスの 172.16.100.1 を追加し 、Next をクリックします。

#### Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.



12. Domain Name and DNS Servers ページで、Parent domain フィールドに wirelessdemo.local、IP address フィールドに 172.16.100.26 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	Wizaro	

#### **Domain Name and DNS Servers**

The Domain Name System (DNS) maps and translates domain names used by clients on your network.



arent do <u>m</u> ain: wirelessden	no.local		
o configure scope clients to ervers.	use DNS serve	rs on your network, enter the IP	addresses for tho:
erver name:		I <u>P</u> address:	200 100
			Add
	R <u>e</u> solve	172.16.100.26	Bemove
			<u>U</u> p
			Down
		3. 	

- 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 activated.
Do you want to activate this scope now?
Yes, I want to activate this scope now
No, I will activate this scope later
< <u>B</u> ack <u>N</u> ext> Cancel

15. Completing the New Scope Wizard ページで Finish をクリックします。

<u>ステップ5: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、ユーザーはエン タープライズ管理者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。

You can add or remove components of Windows	
To add or remove a component, click the checkt part of the component will be installed. To see w Details.	box. A shaded box means that only hat's included in a component, click
Components:	
💌 📻 Accessories and Utilities	4.9 MB 🔺
🗹 🕞 Application Server	33.4 MB 🛁
🔽 😫 Certificate Services	1.4 MB
🔲 💻 E-mail Services	1.1 MB
Eax Services	7 9 MB 💻
Description: Installs a certification authority (CA) public key security programs.	to issue certificates for use with
Total disk space required: 3.4 MB	<u>D</u> etails
Space available on disk: 1346.9 MB	

3. [CA Type] ページで [Enterprise root CA] を選択し、[Next] をクリックします。

Windows Components Wizard	×
CA Type Select the type of CA you want to set up.	Ì
<ul> <li>Enterprise root CA</li> <li>Enterprise subordinate CA</li> <li>Stand-alone root CA</li> <li>Stand-alone subordinate CA</li> <li>Description of CA type</li> <li>The most trusted CA in an enterprise. Should be installed before any other CA.</li> </ul>	
< <u>B</u> ack <u>N</u> ext > Cancel	Help

4. CA Identifying information ページで、Common name for this CA ボックスに wirelessdemoca と入力します。必要に応じてその他の詳細オプションを入力し、Next をクリックします。 Certificate Database Settings ページでデフォルトの設定を確認します。

vtificate Database Settings		
Enter locations for the certificate database information.	e, database log, and co	nfiguration
<u>C</u> ertificate database:		
C:\WINDOWS\system32\CertLog		Br <u>o</u> wse
Certificate database log:		
C:\WINDOWS\system32\CertLog		Bro <u>w</u> se
<ul> <li>Store configuration information in a shared folder:</li> <li>Preserve existing certificate database</li> </ul>	hared folder	B <u>r</u> øwse
< <u>B</u> ack	<u>N</u> ext> (	Cancel He

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を読んでから、OK をクリックします。

<u>ステップ6:証明書を使用するための管理者権限を確認する</u>

- 1. [Start] > [Administrative Tools] > [Certification Authority] を選択します。
- 2. wirelessdemoca CA を右クリックし、Properties を選択します。
- 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 CertificatesDeny に設定さ れていたり、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。

relessdemoca Properties		?
General   Policy Module   Exit M Certificate Managers Restrictions   Aud	odule   Extension iting   Recovery Ag	ns   Storage gents Security
Administrators (WIRELESSDEMO) Authenticated Users Domain Admins (WIRELESSDEM) Enterprise Admins (WIRELESSDE	Administrators) D\Domain Admins) MO\Enterprise Admir	ns)
Permissions for Administrators	A <u>d</u> d Allow	<u>R</u> emove Deny
Read Issue and Manage Certificates Manage CA Request Certificates		
OK	1	1

5. OK をクリックして wirelessdemoca CA 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>手順7: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**タが既にドメインに追加されている場合は、「ドメインにユーザを追<u>加する」に</u> <u>進みます</u>。

- 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 wirelessdemo.local を展開します。
- 3. Users 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 を使用します。

New Object - Computer	×
Create in: wirelessdemo.local/Users	
Computer n <u>a</u> me:	
Client	
Computer name (gre-Windows 2000): CLIENT	
The following user or group can join this computer to a domain. <u>U</u> ser or group:	
Default: Domain Admins <u>C</u> hange	
Assign this computer account as a pre-Windows 2000 computer	
< <u>B</u> ack <u>N</u> ext > C	ancel

- 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>ステップ8:コンピュータ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 [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。
- 2. [**Properties**] をクリックし、[Dial-in] タブに移動します。
- 3. Allow access を選択して OK をクリックします。

<u>手順9: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の[First name]フィールドに**WirelessUserと入力**し、 [User logon name]フィールドに**WirelessUserと入力**し、[**Next**]をクリックします。

w Object - User		
robject oser		
	e in: Wirelessdemo. local/Users	
_		
<u>F</u> irst name:	WirelessUser Initials:	
Last name:		
Full name:	WirelessUser	
	,	
User logon name:	e e e e e e e e e e e e e e e e e e e	
<u>Network</u>		
WirelessUser	🛛 🔍 🗠 🦉 🖉	
User logon name	(pre- <u>W</u> indows 2000):	
User logon name	(pre- <u>W</u> indows 2000): 10 \ WirelessUser	
User logon name WIRELESSDEM	(pre- <u>W</u> indows 2000): 10 \ WirelessUser	
User logon name WIRELESSDEM	(pre- <u>W</u> indows 2000): 10 ∖ WirelessUser	
User logon name WIRELESSDEM	(pre- <u>W</u> indows 2000): 10 \ WirelessUser	
User logon name	: (pre- <u>W</u> indows 2000): 10 \ WirelessUser	

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。

ew ubject - User		
Create in: win	elessdemo.local/Users	
Password:	••••	
<u>C</u> onfirm password:	••••	
User <u>m</u> ust change pass	word at next logon	
User cannot change pa	assword	
Pass <u>w</u> ord never expires	\$	
Account is disabled		
	c Danka Marita	Coursel
	<u> K B</u> ack <u>N</u> ext >	Lancel

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> 手順 10: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 を選択して OK をクリックします。

<u>ステップ 11: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。

Group n <u>a</u> me:	
WirelessUsers	
Group name (pre-Windows 20	100):
WirelessUsers	
C Domain local	Security
Global	© <u>D</u> istribution
⊂ <u>U</u> niversal	

<u>ステップ 12: 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, Computers, or Groups	? X
<u>S</u> elect this object type:	
Users, Groups, or Other objects	<u>O</u> bject Types
<u>From this location:</u>	
wirelessdemo.local	Locations
Enter the object names to select ( <u>examples</u> ):	
wirelessuser	<u>C</u> heck Names
	_
<u>A</u> dvanced OK	Cancel

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 Pro	perties	? ×	
General Members	Member Of Managed By		
		1	
<u>M</u> embers:		[	
Name	Active Directory Folder		
🛛 📓 Administrator	r wirelessdemo.local/Users		
🛛 🙎 WirelessUse	r wirelessdemo.local/Users		
		_	
Add	Bemove		
<u></u>	<u>IT</u> ellove		
		PPly	

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。

<u>ステップ 13: WirelessUsers グループにクライアント コンピュータを追加する</u>

- 1. 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>」セクションのステップ 1 と 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 Users, Contacts, Computers, or Groups	? 🗙
<u>S</u> elect this object type:	
Users, Groups, or Other objects	<u>O</u> bject Types
Erom this location:	
wirelessdemo.local	Locations
Enter the object names to select ( <u>examples</u> ):	
client	<u>C</u> heck Names
<u>A</u> dvanced	OK Cancel

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	? X
Select the types of objects you want to find.	
Object types:	
🔽 🐗 Other objects	
Contacts           Image: Contacts           Image: Contacts           Image: Contacts	
🗖 🗹 Users	
	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 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。

## <u>Cisco Secure ACS 4.0 を使用する Windows Standard 2003 のセ</u> ットアップ

Cisco Secure ACS は、Windows Server 2003 Standard Edition SP1 が稼働していて、コントロー ラに RADIUS 認証および認可を提供するコンピュータです。ACS を RADIUS サーバとして設定 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

次のステップを実行します。

- Windows Server 2003 Standard Edition SP1 を、wirelessdemo.local ドメインの ACS という 名前のメンバ サーバとしてインストールします。注:残りの設定では、ACSサーバ名は cisco\_w2003と表示されます。ラボ環境の以降のセットアップでは、ACS あるいは cisco\_w2003 で読み換えてください。
- 2. ローカルエリア接続の場合は、IP アドレスは 172.16.100.26、サブネット マスクは 255.255.255.0、DNS サーバの IP アドレスは 127.0.0.1 で、TCP/IP プロトコルを設定しま す。

<u>Cisco Secure ACS 4.0 のインストール</u>

**注:**Cisco Secure <u>ACS 4.0 for Windowsの設定方法の詳細については、『</u>Cisco Secure ACS 4.0 for Windowsインストールガイド』を参照してください。

- Cisco Secure ACS をインストールするには、ドメイン管理者アカウントを使用して、ACS という名前のコンピュータにログインします。注: Cisco Secure ACSをインストールする コンピュータでのみ実行されるインストールがサポートされます。Windows Terminal Services や、Virtual Network Computing (VNC)などの製品を使用したリモート インスト ールはテストされておらず、サポートされていません。
- 2. コンピュータの CD-ROM ドライブに Cisco Secure ACS CD を挿入します。
- CD-ROM ドライブが Windows の自動再生機能をサポートしている場合は、Cisco Secure ACS for Windows Server ダイアログボックスが表示されます。注:コンピュータに必要な サービスパックがインストールされていない場合は、ダイアログボックスが表示されます。 Windows の Service Pack の適用は、Cisco Secure ACS のインストール前でもインストー ル後でもかまいません。インストールはそのまま続行できますが、インストール完了後に、 必ず、必要な Service Pack を適用してください。これを行わないと、Cisco Secure ACS が 正常に機能しない場合があります。
- 4. 次のタスクのいずれかを実行します。Cisco Secure ACS for Windows Server ダイアログボ ックスが表示された場合は、Install をクリックします。Cisco Secure ACS for Windows Server ダイアログボックスが表示されない場合は、Cisco Secure ACS CD のルート ディレ クトリにある setup.exe を実行します。
- 5. Cisco Secure ACS Setup ダイアログボックスに、ソフトウェア ライセンス契約書が表示されます。
- ソフトウェア ライセンス契約書をお読みください。ソフトウェア ライセンス契約書に同意 する場合は、Accept をクリックします。Welcome ダイアログボックスに、セットアップ プ ログラムに関する基本的な情報が表示されます。
- 7. Welcome ダイアログボックスの情報を読み終わったら、Next をクリックします。
- Before You Begin ダイアログボックスに、インストールを続行する前に完了しておく必要の ある項目が一覧表示されます。Before You Begin ダイアログボックスに表示されている項目 がすべて完了していたら、各項目に対応するボックスにチェックマークを入れて、Next を クリックします。注:[開始前]ボックスに表示されているすべての項目を完了していない場 合は、[キャンセル]をクリックして、[設定の終了]をクリックします。Before You Begin ダイ アログボックスに表示されているすべての項目を完了してから、インストールを再開します

- 9. Choose Destination Location ダイアログボックスが表示されます。Destination Folder にイ ンストール場所が表示されます。このドライブとパスが、Cisco Secure ACS がインストー ルされる場所になります。
- 10. インストール場所を変更する場合は、次の手順を実行します。[Browse] をクリックします。Choose Folder ダイアログボックスが表示されます。Path ボックスに、インストール場所が表示されます。インストール場所を変更します。Path ボックスに新しい場所を入力するか、Drives and Directories リストを使用して新しいドライブとディレクトリを選択します。インストール場所は、コンピュータのローカル ドライブである必要があります。注 :パスにパーセント文字「%」を含むパスは指定しないでください。使用した場合、インストールは問題なく続行されるように見えますが、途中で失敗します。[OK] をクリックします。注記:存在しないフォルダを指定した場合、フォルダの作成を確認するダイアログボックスが表示されます。続行する場合は [Yes] をクリックします。
- 11. Choose Destination Location ダイアログボックスの Destination Folder に、新しいインストール場所が表示されます。
- 12. [next] をクリックします。
- 13. Authentication Database Configuration ダイアログボックスに、ユーザを認証する際のオプションが一覧表示されます。認証は、Cisco Secure ユーザ データベースだけを使用して実行するか、これに加えて Windows ユーザ データベースも使用して実行することができます。注: Cisco Secure ACSをインストールした後、Windowsユーザデータベースに加えて、すべての外部ユーザデータベースタイプの認証サポートを設定できます。
- 14. ユーザの認証に、Cisco Secure ユーザ データベースだけを使用する場合は、Check the Cisco Secure ACS database only オプションを選択します。
- 15. ユーザの認証に、Cisco Secure ユーザ データベースに加えて、Windows Security Access Manager (SAM) ユーザ データベースまたは Active Directory ユーザ データベースを使用 する場合は、次の手順を実行します。Also check the Windows User Database オプション を選択します。Yes, refer to "Grant dialin permission to user" setting チェックボックスが使 用可能になります。注: [Yes, refer to Grant dialin permission to user]チェックボックスは 、ダイヤルインアクセスだけでなく、Cisco Secure ACSによって制御されるすべての形式 のアクセスに適用されます。たとえば、VPN トンネル経由でネットワークにアクセスする ユーザは、ネットワーク アクセス サーバにダイヤルインはしません。しかし、Yes, refer to "Grant dialin permission to user" setting ボックスにチェックマークを入れると、Cisco Secure ACS では、ネットワークに対するユーザ アクセスの可否を判別する場合に Windows ユーザのダイヤルイン権限を適用するようになります。Windows ドメイン ユー ザデータベースで認証されたユーザにつき、各ユーザが Windows アカウントでダイヤル イン権限を持っているときだけにアクセスを許可する場合は、Yes, refer to "Grant dialin permission to user" setting ボックスにチェックマークを入れます。
- 16. [next] をクリックします。
- 17. セットアップ プログラムによって、Cisco Secure ACS がインストールされ、Windows の レジストリが更新されます。
- 18. Advance Options ダイアログボックスに、Cisco Secure ACS の機能がいくつか表示されます。これらの機能は、デフォルトでは無効になっています。これらの機能の詳細については、『Cisco Secure ACS ユーザ ガイド Windows 版 Version 4.0』を参照してください。 注:上記の機能は、Cisco Secure ACS HTMLインターフェイスで有効にした場合にのみ表示されます。インストール後は、Interface Configuration セクションの Advanced Optionsページで、これらの機能を有効または無効にできます。
- 19. 有効にする機能につき、それぞれ対応するボックスにチェックマークを入れます。 20. [next] をクリックします。

- 21. Active Service Monitoring ダイアログボックスが表示されます。注:インストール後、[シ ステムの設定(System Configuration)]セクションの[アクティブサービス管理(Active Service Management)]ページでアクティブサービス監視機能を設定できます。
- 22. Cisco Secure ACS でユーザ認証サービスを監視する場合は、Enable Login Monitoring ボックスにチェックマークを入れます。Script to Execute リストで、認証サービスが失敗した場合に適用するオプションを次の中から選択します。是正措置なし:Cisco Secure ACSはスクリプトを実行しません。注:このオプションは、イベントメール通知を有効にする場合に便利です。リブート:Cisco Secure ACSは、Cisco Secure ACSを実行するコンピュータをリブートするスクリプトを実行します。Restart All:Cisco Secure ACSはすべてのCisco Secure ACSサービスを再起動します。RADIUS/TACACS+の再起動:Cisco Secure ACSは、RADIUSおよびTACACS+サービスのみを再起動します。
- 23. サービス モニタリングでイベントが検出されたときに、Cisco Secure ACS から E メール メッセージを送信させる場合は、Mail Notification ボックスにチェックマークを入れます。
- 24. [next] をクリックします。
- 25. Database Encryption Password ダイアログボックスが表示されます。注:データベース暗 号化パスワードは暗号化され、ACSレジストリに保存されます。このパスワードは、重大 な問題が発生して、データベースに手動でアクセスする必要が発生した場合などに必要に なります。このパスワードは、テクニカルサポートがデータベースにアクセスできるよう に、手元に保存しておいてください。パスワードは、有効期間が終了するごとに変更でき ます。
- 26. データベースの暗号化に使用するパスワードを入力します。パスワードは、最低 8 文字の 長さで、文字と数字の両方を含んでいる必要があります。無効な文字はありません。[next] をクリックします。
- 27. セットアップ プログラムが終了し、Cisco Secure ACS Service Initiation ダイアログボック スが表示されます。
- 28. 適用する Cisco Secure ACS Services Initiation のオプションにつき、それぞれ対応するボ ックスにチェックマークを入れます。各オプションに関連する処理はセットアップ プログ ラムの終了後に有効になります。はい、I want to start the Cisco Secure ACS Service now:Cisco Secure ACSを構成するWindowsサービスを開始します。このオプションを選択 しなかった場合は、コンピュータを再起動するか、CSAdmin サービスを開始するまで、 Cisco Secure ACS HTML インターフェイスは使用できません。Yes, I want Setup to launch the Cisco Secure ACS Administrator from my browser following installation:現在の WindowsユーザアカウントのデフォルトWebブラウザでCisco Secure ACS HTMLインター フェイスを開きます。Yes, I want to view the Readme File:Windowsのメモ帳で README.TXTファイルを開きます。
- 29. [next] をクリックします。
- 30. いずれかのオプションを選択していた場合は、Cisco Secure ACS サービスが開始されます 。Setup Complete ダイアログボックスに、Cisco Secure ACS HTML インターフェイスに 関する情報が表示されます。
- 31. [Finish] をクリックします。**注:設定**の残りの部分は、設定されているEAPタイプのセクションに記載されています。

## <u>Cisco LWAPP コントローラの設定</u>

#### <u>WPA2/WPA に必要な設定の作成</u>

**注:コン**トローラがネットワークに基本的に接続しており、管理インターフェイスへのIP到達可 能性が成功していることを前提としています。

1. https://172.16.101.252 をブラウズして、コントローラにログインします。

Class Systems Lingle - Alkcrosoft Internet Explorer provided by Disco Systems . Inc.
nie Ddi: View Favorices Fools Help
😋 s - z 💿 - 🛋 🗟 🏠 🔎 s all 👷 hearis 🥝 🝰 - 🛬 🖿 - 🔜 🇱 🟮 🙂 🍇
Address 🦨 htt padr 2015 the 2020



- 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、インターフェイスと VLAN のマッピングを作成します。
- 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]ウィンドウが表示されるように、情報を設定します。

ISCO SYSTEMS				
alle, alle,	MONITOR WUNNS CONTR	OLLER WIRELESS SECURITY		
Controller	Interfaces > Edit			
General Inventory	General Information			
Interfaces	Interface Name employee			
Internal DHCP Server	Tutuda an I didua an			
Mobility Management Mobility Groups Mobility Statistics Ports Master Controller Mode Network Time Protocol QoS Profiles	VLAN Icentifier IP Address Netmask Gateway Physical Information Port Number DHCP Information	20 172.16.100.4 255.255.255.0 172.16.100.1		
	Primary DHCP Server Secondary DHCP Server Access Control List	172.16.100.25 0.0.0.0		
	ACL Name	none 💙		

- 11. [Apply] をクリックします。
- 12. WLAN をクリックします。
- 13. [New] をクリックします。
- 14. WLAN SSID フィールドに、Employee と入力します。
- 15. [Apply] をクリックします。
- 16. 次の[WLANs > Edit]ウィンドウが表示されるように、情報を設定します。注:この実習で は、WPA2がレイヤ2暗号化方式として選択されています。この SSID に関連付ける TKIP-MIC クライアントで WPA を使用するようにするには、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 のボ ックスにチェックマークを入れます。

WLANs > Edit

WLAN LD	1			
WLAN 5510	Employee			
Ceneral Policies		Security Policies		
Radio Policy	N 11		W242	
Admin Status	🗹 Enabled	Luyor 2 Seburity	W 142	
Session T meaut (secs)	1830			
Quality of Scrvics (QoB)	Silver (best offert)	Layer 3 Security	Nore	
WMM Policy	Disabled 🛩		web Policy "	
7920 P ione Support	🔲 Client CAC Limit 🔄 🗛 CAC Limit			
Broaccast SSID	💌 Enabled			
Allow AAA Override	🥅 Enabled	* Web Policy cannot be used in combination with IPsec and L2TP.		
Client Exclusion	Enabled ** 60 Timeout Value (secs)	** When blight exclusion zero means infinity(will	on is enabled, a timbout value of Frequire administrative override	
DHCP Server	Over-ida	reset excluded clients)		
DI CP Addr. Assignment	🗹 Required			
Interface Name	emplayee 💌			
Radius Servers				
	Authentication Servers Accounting Servers			
Server 1	TP:172.16.100.25, Port:1812 💙 none 💙			
Server 2	rone 💙 none 🔽			
Server 3	rone 🛛 V none V			
WPA2 Parameters				
WPA Compatibility Mode	Encble			
Allow WPA2 TKIF Clients	Enable			

- 17. [Apply] をクリックします。
- 18. [Security] メニューをクリックし、RADIUS サーバを追加します。
- 19. [New] をクリックします。
- 20. RADIUS サーバの IP アドレス(172.16.100.25)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。
- 21. 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。
- 22. [Apply] をクリックします。

Address 🔄 https://172.16.101.252/screens/frameset.html

CISCO SYSTEMS				
adha adha	MONITOR WLANS (	CONTROLLER	WIRELESS	SECURITY
Security	RADIUS Authentication	on Servers >!	New	
AAA General	Server Index (Priorit	ty) 1	1	
RADIUS Authentication RADIUS Accounting Local Net Users	Server IPAddress	172.1	16.100.25	
MAC Filtering Disabled Clients	Keys Format	ASC	II <b>v</b>	
AP Policies	Shared Secret	••••	••	
Access Control Lists Web Auth Certificate	Confirm Shared Secret	••••	••	
Wireless Protection Policies	Key Wrap			
Rogue Policies Standard Signatures	Port Number	1812		
Custom Signatures Client Exclusion Policies AP Authentication	Server Status	Enab	led 💙	
	Support for RFC 357	6 Enab	led ⊻	
	Retransmit Timeout	2	seconds	
	Network User	<b>I</b> E	inable	
	Management	E 6	nable	



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

## <u>EAP-TLS 認証</u>

EAP-TLS 認証を利用するには、コンピュータ証明書とユーザ証明書を無線クライアント上に配置 し、無線アクセス用のリモート アクセス ポリシーに EAP タイプとして EAP-TLS を追加して、 無線ネットワーク接続を再設定する必要があります。

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 DC\_CA 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のリリースでWeb Serverテンプレートを変更した ため、キーがエクスポートできなくなり、オプションが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>

- 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 と入力すると、Certificate Templates スナッ プインが開きます。

Certificate Templates	Teoplate Display Name	Minimum Supported CAs	Version	Autoenrolinent
	GgBast: EFS	Windows 2000	3.1	Not allowed
	CA Exchange	Windows Server 2003, En	106 0	Vot allowed
	CEP Encryption	Windows 2000	4.1	Vot allowed
	Code Signing	Winduws 2000	3.1	Not allowed
	Computer	Windows 2000	5.1	Not allowed
	Cross Certification Authority	Windows Server 2003, En	105 0	Not allowed
	DEMOACS	Windows Server 2000, Dn	100.2	Not sllowed
	Directory Email Replication	Windows Server 2003, Fn	1:50	Allowed
	Dorran Controler	Windows 2000	4.1	Not allowed
	Dorrain Controlor Authonaication	Windows Server 2003, En	1:00	Allowed
	EFS Recovery Agent	Windows 2000	6.1	Not allowed
	Enrolline it Agent	Winduws 2000	4.1	Not allowed
	Enrollment Agent (Computer)	Windows 2000	5.1	Vot allowed
	Exchange Enrolment Agent (Offline request)	Windows 2000	4.1	Vot allowed
	Exchange Signature Only	Windows 2000	6.1	Not allowed
	Exchange law	Windows 2000	7.1	Not allowed
	Dill-Sec	Windows 2000	8,1	Not allowed
	IPSec (Offine request)	Windows 2000	7.1	Not allowed
	Key Recovery Agent	Windows Server 2003, En	105 0	Allowed
	RAS and IAS Server	Windows Server 2003, En	101 0	Allowed
	Roo: Certification Authority	Windows 2000	5.1	Not allowed
	Router (Offline request)	Wheews 2000	4.1	Not allowed
	Construction Construction	Wincows 2000	6.1	Not allowed
	Smartcard User	Wincows 2000	11.1	Not allowed
	Subordinate Certification Authority	Wincows 2000	5.1	Not allowed
	Trust List Signing	Wincows 2000	3.1	Not allowed
	Gilluser .	Wincows 2000	3.1	Not allowed
	User Signature Only	Wincows 2000	4.1	Not allowed
	Wigh Server	Wincows 2000	4.1	Not allowed
	Dupicate Templace	Wincows Server 2003, En	1.0.3	Alowed
	Wi al tasks b late	Wincows Server 2003, En	101.0	Alowed
		Wincows Server 2003, En	101:0	Alowed
	Properties			1213203

## 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。
| operties of New Te  | mplate                                     |                        | ?                        |
|---|--|------------------------|--------------------------|
| Issuance Requiremen<br>General  | ts   Superseded Templa<br>Request Handling | tes Extension<br>Subje | ns   Security<br>ct Name |
| Template display nar  | ne:  |                        |                          |
| Copy of Web Server  |  |                        |                          |
| Minimum Supported I   | CAs: Windows Server 200                    | )3, Enterprise E       | dition                   |
| After you apply chan<br>name.   | ges to this tab, you can no                | longer change          | the template             |
| Template name:  |  |                        |                          |
| Copy of Web Server  |  |                        |                          |
| Yalidity period:<br>2 years<br>2 years<br>2 Do not autom<br>Directory | Enewal pe                                  | eriod:<br>eeks 💽       | sts in Active            |
|   |  | Consel                 |                          |

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

Issuance Requirement	ts   Superseded Templates   Extensions   S	Security
General	Request Handling Subject Nar	ne
T <u>e</u> mplate display nam	ie:	
ACS		
Minimum Supported F	°A∞ Windows Server 2003, Enterprise Edition	
Miniman Supported C	As. Windows Server 2000, Enkelphse Edikion	
After you apply chang name.	ges to this tab, you can no longer change the ter	mplate
Template name:		
Template name.		
ACS		
ACS		
ACS		
ACS ⊻alidity period:	<u>R</u> enewal period:	
ACS ⊻alidity period: 2 years	<u>R</u> enewal period: 6 weeks	
ACS ⊻alidity period: 2 years	■ Benewal period: 6 weeks ■	
ACS ⊻alidity period: 2 years	<u>R</u> enewal period: ▼ 6 weeks ▼	
ACS Validity period: 2 years	Eenewal period: 6 weeks   in Active Directory	
ACS Validity period: 2 years Publish certificate Do not automa	Eenewal period: 6 weeks • in Active Directory atically reenroll if a duplicate certificate exists in A	Active
ACS Validity period: 2 years _ Publish certificate Do not automa Directory	Enewal period: 6 weeks • in Active Directory atically reenroll if a duplicate certificate exists in A	Active
ACS Validity period: 2 years _ Publish certificate Do not automa Directory	Enewal period: 6 weeks • in Active Directory atically reenroll if a duplicate certificate exists in A	Active

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

ssuance Requirer General	Request Handling	Subject Name
<u>P</u> urpose:	Signature and encryption	T
1	Archive subject's encryption pr	rivate key
1	Include symmetric algorithms a	llowed by the subject
ſ		ficates (do not archive)
Minimum keu size	1024	
Allow private I	rail to be evported	
Allow private I	key to be exported	
Do the following v associated with th	key to be exported when the subject is enrolled and w his certificate is used:	hen the private key
<ul> <li>Allow private I</li> <li>Do the following v associated with the</li> <li>Enroll subject</li> </ul>	key to be exported when the subject is enrolled and w his certificate is used: without requiring any user input	hen the private key
<ul> <li>Allow private I</li> <li>Do the following v associated with the</li> <li>Enroll subject</li> <li>Prompt the us</li> </ul>	key to be exported when the subject is enrolled and w his certificate is used: without requiring any user input er during enrollment	hen the private key
<ul> <li>Allow private I</li> <li>Do the following vasociated with the solution</li> <li>Enroll subject</li> <li>Prompt the us private key is</li> </ul>	key to be exported when the subject is enrolled and w his certificate is used: without requiring any user input er during enrollment er during enrollment and require us used	hen the private key ser input when the
<ul> <li>Allow private I</li> <li>Do the following vassociated with the</li> <li>Enroll subject</li> <li>Prompt the us</li> <li>Prompt the us</li> <li>private key is</li> </ul>	key to be exported when the subject is enrolled and w his certificate is used: without requiring any user input er during enrollment er during enrollment and require used used	hen the private key ser input when the
<ul> <li>Allow private I</li> <li>Do the following vassociated with the</li> <li>Enroll subject</li> <li>Prompt the us</li> <li>Prompt the us</li> <li>private key is</li> <li>To choose which (CSPs) should be</li> </ul>	key to be exported when the subject is enrolled and w his certificate is used: without requiring any user input er during enrollment er during enrollment and require used used cryptographic service providers used, click CSPs.	hen the private key ser input when the <u>C</u> SPs
<ul> <li>Allow private I</li> <li>Do the following vassociated with the</li> <li>Enroll subject</li> <li>Prompt the us</li> <li>Prompt the us</li> <li>private key is</li> <li>To choose which (CSPs) should be</li> </ul>	key to be exported when the subject is enrolled and w his certificate is used: without requiring any user input er during enrollment er during enrollment and require used used cryptographic service providers used, click CSPs.	hen the private key ser input when the <u>C</u> SPs

5. [Requests must use one the following CSPs]を選択し、[Microsoft Base Cryptographic Provider v1.0]をオンにします。オンになっている他のCSPのチェックマークを外して、 [OK]をクリックします。

S Properties		?
Issuance Requirements   General	Superseded Templates Request Handling	Extensions   Security   Subject Name
SP Selection		? 🗴
Choose which cryptograp requests: C <u>R</u> equests can use ar	phic service providers (C ny CSP available on the :	SPs) can be used in subject's computer
Requests must use a	one of the following CSPs	g
<u>C</u> SPs:		
<ul> <li>Infineon SICRYPT Base Crypto</li> <li>Microsoft Base DSS a</li> <li>Microsoft DH SChann</li> <li>Microsoft Enhanced 0</li> <li>Microsoft Enhanced 0</li> <li>Microsoft Enhanced 0</li> <li>Microsoft Enhanced 1</li> <li>Microsoft Enhanced 1</li> </ul>	ase Smart Card CSP ographic Provider v1.0 and Diffie Hellman Crypto hel Cryptographic Provide Cryptographic Provider v DSS and Diffie Hellman 0 RSA and AES Cryptograp	ographic Provider er 1.0 Cryptographic Prov phic Provider
	OK	Cancel
	ОК	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。

General	Bequest Handling	Subject Name
<ul> <li>Supply in the re Select this option not have acce Autoenrollment</li> <li>Build from this A</li> </ul>	equest on to allow a variety of subject n ss to the domain of which the su is not allowed if you choose this Active Directory information	ame formats or if you do bject is a member. : option.
Select this option simplify certificate Subject name for	n to enforce consistency among e administration. Irmat:	subject names and to
None		<b>T</b>
∏ Include e-ma	ail name in subject name	
Include this infor	mation in alternate subject name al name (UPN)	ə:
i ⊃ei⊼ice biin	ahai wawa (oluw)	

7. 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。重要:このActive Directory情報 のみから構築する場合は、[User principal name (UPN)]にチェックマークを付け、Active Directory Users and ComputersスナップインのWirelessUserアカウントに電子メール名が入 力されていないため、[Include email name and E-mail name]のののチェックをを外にします 。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。

General Request H	andling St	ubject Name
Issuance Requirements 📔 Supersede	ed Templates   Exten	sions Security
<u>G</u> roup or user names:		
🖸 Administrator (WIRELESSDEM	0 \Administrator)	
🕵 Authenticated Users		
🕵 Domain Admins (WIRELESSDE	MONDomain Admins)	
🕼 Enterprise Admins (WIRELESS)	DEMO\Enterprise Adm	ins)
9		
	Add	Remove
		<u></u>
Permissions for Domain Admins	Allow	 Deny
Permissions for Domain Admins	Allow	Deny
<u>Permissions for Domain Admins</u> Full Control Read	Allow	Deny
Permissions for Domain Admins Full Control Read Write	Allow	
Permissions for Domain Admins Full Control Read Write Enroll	Allow	
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll		
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll	Allow V V V	
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll	Allow	
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll For special permissions or for advance click Advanced.	Allow	Deny

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。

General	Request Handling	Subject Name
Issuance Requireme	nts Superseded Templates	Extensions Security
Require the followin	g for enrollment:	
CA certificate m	anager approval	
This number of	authorized signatures: 0	
If you require m	, ore than one signature, autoer	nrollment is not allowed.
Policy type regi	ired in signature:	
		<b>.</b> .
Application polic	92.	
l		<u> </u>
Issuance policie	(S)	-
		Bemove
		4
Require the followin	g for reenfoliment:	
C Valid existing of	rtificate	
and a second		

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。

#### 新しい ACS Web サーバ証明書テンプレートの有効化

次のステップを実行します。

1. [Certification Authority] スナップインを開きます。「<u>Create the Certificate Template for the</u> <u>ACS Web Server</u>」セクションのステップ1 ~ 3に従って、[**Certificate Authority**]オプション を選択し、[**Local Computer**]を選択し、[**Finish**]をクリックします。

Certification Authority		<u>×</u>
Select the computer you wa This snap-in will always ma I Local computer: (the Another computer:	Int this snap-in to manage. anage: computer this console is running on)	Bjowse
Allow the selected co only applies if you sa	omputer to be changed when launching from ve the console.	the command line. This

2. コンソール ツリーで、wirelessdemoca を展開し、Certificate Templates を右クリックしま

Console Root\Certification Authority	y (Local)\wirelessdemoca\Certificate Temp	lates
Console Root Certification Authority (Local) Revolved Certificates Revolved Certificates Pending Requests Faied Requests Vew Vew Window from H Vew Taskpad View. Refresh Export List Telp	Name Wireless Liser Certificare Template Diractory Email Replication Diractory Email Replication Domain Controller Authentication Basic EFS Domain Controller Web Server Certificate Templace to Issue Subordinate Certification Authority ere Administrator	Intended Purpose Client A ithentication, Serure Email, Ebriz Directory Service Email Replication Client Authentication, Server Authentication Client Authentication, Server Authentication Server Authentication Client Authentication, Server Authentication Client Authentication, Server Authentication Encrypting File System, Secure Email, Clien <all> Nicrosoft Trust List Signing, Encrypting File</all>

- 3. New > Certificate Template to Issue の順に選択します。
- 4. ACS Certificate Template をクリックします。

#### Enable Certificate Templates

Select one or more Certificate Templates to enable on this Certification Authority

Name	Intended Purpose
ACS	Server Authentication
Authenticated Session	Client Authentication
🙀 CA Exchange	Private Key Archival
CEP Encryption	Certificate Request Agent
😹 Code Signing	Code Signing
Cross Certification Authority	<ad .<="" td=""></ad>
DEMOACS	Server Authentication
😹 Enrolment Agent	Certificate Request Agent
🐺 Enrolment Agent (Computer)	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Certificate Request Agent
Exchange Signature Only	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、 wirelessdemo.local domain を右クリックして Properties をクリックします。

? X



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。

	diffopercies			
General Manage	ed By Group Po	blicy		
To improve Grou Management Co	ip Policy manage nsole (GPMC). ent Group Policy	ment upgrade to Object Links for	o the Group Pr wirelessdemo	olicy
Group Policy O	bject Links		No Override	Disabled
S Default Dor	nain Policy			
Group Policy Obj This list obtained <u>N</u> ew	iects higher in the I from: cisco_w20 	e list have the hij 103.wirelessdem <u>E</u> dit	ghest priority. o.local	<u>Ц</u> р
Group Policy Obj This list obtained <u>N</u> ew <u>Options</u>	iects higher in the Ifrom: cisco_w20 A <u>d</u> d Dele <u>t</u> e	e list have the hij 103.wirelessdem <u>E</u> dit <u>P</u> roperties	ghest priority. o.local	<u>U</u> p Do <u>w</u> n

8. コンソールツリーで、[コンピュータの構成] > [Windowsの設定] > [セキュリティの設定] > [公開キーポリシー]を展開し、[自動証明書要求の設定]を選択します。

🚡 Group Policy Object Editor			
<u>File Action View H</u> elp			
4 -> 🖻 🖪 🛃 😫			
🛐 Default Domain Policy [cisco_w2003,wirel	essdemo.local]Po	licγ	Automatic Certificate Request 💋
🖻 🌆 Computer Configuration		2	There are
🕀 🦲 Software Settings			increater
🖻 🦲 Windows Settings			
Scripts (Startup/Shutdown)			
Security Settings			
E G System Services			
E Braistry			
File System			
🗄 🐺 Wireless Network (IEEE 8	02.11) Policies		
🖻 🧰 Public Key Policies			
Encrypting File System	n		
Automatic Certifical	n i e i i e Meiai		Automatic Certificate Request
🛄 Trusted Root Certif	14644	Т	Matomatic Certificate Request
Enterprise Trust	⊻iew		
Software Restriction Po -	Defrech		
IP Security Policies on A	Export List		
Administrative Templates	Export list	-	
Engla Oser Conniguration	Help		
Windows Settings			
Administrative Templates			
			l.

- 9. [Automatic Certificate Request Settings]を右クリックし、[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。

A certificate template is a set of prede computers. Select a template from the	efined properties for certificates issued to e following list.
C <u>e</u> rtificate templates:	
Name	Intended Purposes
Computer Demain Controller	Client Authentication, Server Authenticatio
Enrollment Agent (Computer)	Certificate Reguest Agent
IPSec	IP security IKE intermediate
•	•

12. Automatic Certificate Request Setup Wizard ページが終了したら、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	
Eile Action View Help	
S Default Domain Policy [cisco_w2003.wirelessdemo.local] Policy	Automatic Certificate Request
😑 🌄 Computer Configuration	Computer
🕀 🧰 Software Settings	
🖻 💼 Windows Settings	
🖻 📑 Security Settings	
🖻 🛃 Account Policies	
😟 🛃 Local Policies	
😟 🛃 Event Log	
🕀 🤷 Restricted Groups	
🕀 🤷 System Services	
🕀 🤷 Registry	
🕀 🤷 File System	
😐 🍸 Wireless Network (IEEE 802.11) Policies	
😑 🧰 Public Key Policies	
🚞 Encrypting File System	
Trusted Root Certification Authorities	
Enterprise Trust	

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。

🚡 Group Policy Object Editor	
Eile Action View Help	
Default Domain Policy [cisco_w2003.wirelessdemo.local] Policy          Omputer Configuration         Omputer Configuration      <	Object Type Enterprise Trust Autoenrollment Settings

- 14. 詳細ペインで [Auto-enrollment Settings] をダブルクリックします。
- 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
Do not enroll certificates automatically
Enroll certificates automatically
Renew expired certificates, update pending certificates, and remove revoked certificates
Update certificates that use certificate templates
OK Cancel Apply

16. [OK] をクリックします。

## <u>ACS 4.0 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

重要:ACS サーバが WLAN の EAP-TLS クライアントの認証を実行するには、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している必要があります。

**重要**:証明書の設定作業中は、IIS Manager が起動していないことを確認してください。IIS Manager が起動していると、キャッシュ情報に関する問題が発生することがあります。

- 1. Enterprise 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. ローカル ACS マシンで、ブラウザから http://<ルート CA の IP アドレス>/certsrv で Microsoft 認証局サーバを指定します。この例では、IP アドレスは 172.16.100.26 です。
- 3. Administrator でログインします。

Comparison of the second state of the s	Morash Scribbata Barrash Atana Batana Babarar	
No. ************************************	De De De See Faces De De	
Kongenee (2,22,4,2,6,22,22,24,24,24,24,24,24,24,24,24,24,24,	QBL *O = (* 2) C ≥ Sext *Setus *O C = Q C	
We come Use the Web Historie grant and the tory universe to the property of certain of a control of the second s	6 00 x0 (2) 0000 (1.1020.10) (1.102	<u>a</u> 🔁 💷
Welcome Jack to Xea bits to request a cett date to your web brower, estual dens, control xyran, Byreing a cett offs, you can very your weentight, web event web downling, portrespipe directificate you screet beform of a rest. (b) is an even of the to develop a cett add a cett add a site to Y), we cett add, cett add, cett add event of the to develop a cett add a cett add a site to Y). A cett add, cett add event add event add event add event add event add, cett add event	Alforosoft Denlinete Deroves relevader Loa	ttu
Lee the Wee Attended earlier and the torgan Hode brower, e-mail diem, or other brown. By rend earlier de outer type undernight beache you dominance with breache by a non-market brown and the Wee market earlier and the weekeel earlier and the we	Welcome	
xou zen a sou se finit Wee hiters deveload, a zentrade a litterty) wither rate, centrate eran, et rentrate reveration (*) Bit interview the table of a sector	use this Web Fitero request a certo site to your keep browser, e-mail client, or other program. By using a certo data (you can very your certify to be div over the Web is grifted encyptimes ages, and, depending, you regise of perificials you request perform other security takes.	egoù communicateredh
Former if on stor deau Confront Berken, see <u>Confront Berken Dearner taler</u> Select a teak: Addent if confinate Addent if confinate	You can a be use this Web nite to developed a contricate a life my ( 19) centricate, controlle exam, or centricate research on Let ( 3EL) on tested the status	tecupor pribreo a to a
Belost a tank:       Autom to contract         Movel in debase of a contract,	For more information about Conflicted Services uses <u>Conflicted Services Decementation</u>	
Autor Contract Section Contract,	Select a teak:	
Sector addate of a contract of and encoded         Request a Certificate] を選択して、[Next] をクリックします。         Microsoft Certificate Services - Microsoft Internet Explorer         Eile Edit View Favorites Tools Help	-tablet specificate	
Request a Certificate] を選択して、[Next] をクリックします。         Microsoft Certificate Services - Microsoft Internet Explorer         Elle Edit View Favorites Tools Help	V sve ill a daltas of a tea director all take tean exc	
Request a Certificate] を選択して、[Next] をクリックします。 Microsoft Certificate Services - Microsoft Internet Explorer Eile Edit Yiew Favorites Tools Help	Deen ead a StA controller, controller of an, ALC-C.	
Microsoft Certificate Services - Microsoft Internet Explorer         Eile       Edit       View       Favorites       Lools       Help	ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー	
Microsoft Certificate Services - Microsoft Internet Explorer File Edit View Favorites Tools Help	Request a Certificate ] 2 BYO C ([Next] 2 / 7 / 7 0 & 9	
<u>File Edit Yiew Favorites Tools H</u> elp	🚰 Microsoft Certificate Services - Microsoft Internet Explorer	
<u>File Edit View Favorites Tools H</u> elp		
Fig Fair Tour (Fightures Tools Tools	File Edit View Eavorites Tools Help	
	Fig. Far. Jow ( Troug Tools Tools	

Address 🥘 http://172.16.100.26/certsrv/certrgus.asp

Microsoft Certificate Services -- wirelessdemocal

#### **Request a Certificate**

Select the certificate type: User Certificate

Or, submit an advanced certificate request.

5. [Advanced Request] を選択して、[Next] をクリックします。

Submit a certificate request by can graphase 34 encoded CMC on FROS #1011s, or submit a renewal request by using a base 64 encoded PRC/S #2 rite. Request a certificate for a clinicit certification behalf of another user by using the smart card certificate onto ment cretion. Web You built fact at eactively spatial requests there a view and behalf or another user.

6. Create and submit a request to this CA を選択して、Next をクリックします。**重要:**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、前の手順で作成した ACS 証明書に基づいて、証明書の要求を生成する必要があるからです

licrosoft Caroli	cate Services — windessdem —a
1001050011 (S = 1400	
dvanced Ce	rtificate Request
ertificate Lemp	olate:
	Administrator
	Antrinistrator
ey Options:	
	LETS KELOVELY AVET. LITCE my key set
CSP <sup>1</sup>	Wireless User Can ficate Template Vibor v1.1 💌
Key Houng	
n.ej 05580.	Wer Sever
1407 S 20.	Max 15884
	🖲 Automatic key container name 👘 💭 User specified key confainer name
	💌 Mork keys as expendible
	🗖 Export keys to file
	🔲 Enable etrung private key protection
	D Store certificate in the Incal complimenced ficate store.
	Stores the certificate in the local computer store
	instand of is the veer's certificate stars. Dees het installate sed CA's configurate. You must be an
	administrator to generate or use a new in the local
	machine store.
deltrice al Contla	170°
unitariar opua	
escest Format.	© CMC ⊂ PKCS1J
lash Alcorithm:	3FA-1 💌
	Unly used to sign request.
	🗖 Save request to all te
Atticutes:	T I I I I I I I I I I I I I I I I I I I
	<u>x</u>
Friendly Mame:	
<ul> <li>Contraction (Contraction)</li> </ul>	

- 7. Certificate Templates で、前の手順で作成した ACS という名前の証明書テンプレートを選 択します。テンプレートを選択すると、オプションが変更されます。
- 8. Name に、ACS サーバの完全修飾ドメイン名を設定します。この場合、ACSサーバ名は cisco\_w2003.wirelessdemo.localです。[Store certificate in **the local computer certificate** store]がオンになっていることを確認し、[Submit]をクリックします。

Microsoft Certific	rate Services - Microsoft Internet Padacer	
File Edit New I	Feverites Tools Help	
🔾 Deck 🔹 🔘 🕤	🔹 🔹 🥠 🔎 Search 👷 Perontes 🕢 🔝 💀 🐷	
Address 🕘 http://17	72.16.L00.26(certsrv/certrqna.asp	
Certificate Toma	alatar	
certificate reing	hate:	
	ALS •	
Identifying Infor	mation For Offline Template:	
Name:	cisco_w2003.wirelessdemo.local	
E-Mail:		
Company:		
Department:		
City:		
State:		
Country/Region:		
Key Options:		
	Create new key set O Use existion key set	
CSP:	Microsoft Base Cryptographic Provider v1.0	
Key Usage:	@ Eschange	
Key Size:	1024 Min:1024 (common key stree: 1029.)	
	Automatic key container name     O User specified key container name	
	☑ Mark keys as exportable	
	Export keys to file	
	Store certificate in the local computer certificate store	
	Stores the certificate in the local computer store instead of in the user's certificate store. Does not	
	install the root CA's certificate. You must be an	
	administrator to generate or use a key in the local mechine store.	
Additional Uptic	ns.	
Hequest Format:	CONC OPRESIU	
Hash Algorithm:	SHA-1 Only used to sign request.	
	Save request to a file	
	×	
Attributes:	т Т	
Friendly Name:		
	Soldwit >	

9. ポップアップ ウィンドウに、スクリプト違反の可能性があることを示す警告が表示されま す [Ves] をクリックレます



10. [Install this certificate] をクリックします。

Eile	Edit	⊻iew	F <u>a</u> vorites	Tools	Help				
🔾 Ba	ick 👻	9 .	2 2 💰		Search	📌 Favorites	0	🔕 • 🕹	

Microsoft Certificate Services -- wirelessdemoca

## Certificate Issued

The certificate you requested was issued to you.



11. ポップアップ ウィンドウがもう一度表示され、スクリプト違反の可能性があることが警告 されます。[Yes] をクリックします。

	Potential S	cripting violation 🔀
	1	This Web site is adding one or more certificates to this computer. Allowing an unbrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
	1	Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
		<u>Υ</u> ps <u>No</u>
12.	Yes を	クリックすると、証明書がインストールされます。
	🎒 Micro	soft Certificate Services - Microsoft Internet Explorer
	Hic p	cit view Havonces Tools Help
	🕜 Back	🝷 🕘 🚽 🛐 🛃 🎤 pearch 👷 Havorites 🤬 🔛
	Address	🐮 http://172.16.10J.26/certsrv/pertrippi.asp
	Micro	soff Certificate Services wire esselementa
	Certi	ficate Installed
	Youri	new certificate has been successfully installed

 13. この時点で、証明書が Certificates フォルダにインストールされます。このフォルダにアク セスするには、[Start] > [Run]の順に選択し、mmcと入力してEnterキーを押し、[Personal] > [Certificates]を選択します。

🛗 Consule1			
Ele Action View Favorites Window Fel	p		
← → 🖻 🖬 🔏 🖎 🔐 🕞 🔮	9		
	a di mana di mana di mana		
A Lonsole Roor, Lerincares (Local Lompin	Pr) weeshaa (Lernin ares		
Console Rooc	ISSUED TO A	Issued by	EXJIFICIUM Date
Certificate Lenplates	EA 340	wirelessdemoca	3/8/2008
🗆 📴 Cortificatos (Local Computor)	cisco_w2003.wirelessdemo.local	wrelessdenoca	3/.6/2005
🗆 🦲 ?ersonal	🔤 qsco_w2003.wirelessdemo.local	wrelessdemoca	3/13/2008
Cortificatos			
🖃 🛄 Trusted Root Certification Authorities			
🖃 🦲 Enterprice Trust			
🖃 🧰 Intermediate Certification Authorities			
🖂 🥘 Trusted Publishers			
E D Jobrusted Certificates			
🕞 🦲 Third-Earty Boot Certification Authorit			
E . Trusted People			
HI- ACCILSOre			
El Certificate Enrollment Requests			
E			
🗄 📳 Certification Authority (Local)			

- 14. これで、ローカル コンピュータ(この例では、ACS または cisco\_w2003)に証明書がイン ストールされたので、続いて ACS 4.0 の証明書ファイル設定用の証明書ファイル (.cer)を生成する必要があります。
- 15. ACS サーバで(この例では cisco\_w2003)、ブラウザから http://172.16.100.26 /certsrv の Microsoft 認証局サーバを指定します。

<u>ACS 4.0 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. ACS サーバで(この例では cisco\_w2003)、ブラウザから http://172.16.100.26 /certsrv の Microsoft CA サーバを指定します。
- 2. Select a Task オプションから Download a CA certificate, certificate chain or CRL を選択します。
- 3. 無線エンコード方式として Base 64 を選択し、Download CA Certificate をクリックします。

🚰 Microsoft Fertificate Services - Microsoft Toternet Explorer	
Ele Edt view Favorites Ipols Help	
🔇 Back 🝷 🕙 👻 🛐 🐔 🔎 Search 👷 Favortes 🧔 🕼 🗞 😓 🚍	
Abdross 🔄 -ttp://172.10.100.26/certs/v/certoarclasp	

Microsoff Ceptificate Genuces -- wrelesedemonal

#### Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from the certification authority install this CA certificate chain.

To down ded a CA cort ficate, certificate chain, or CRL isolact the certificate and encoding method.

CA certificate:

C unent	[wire esistemoda]
	i i i in

Lacoding method:

⊂ D\_R ©Eese 64

<u>Down dad CA certificate</u> <u>Down dad CA certificate chain</u> Down dad latest base CRL <u>Down dad latest delta CRL</u>

4. File Download Security Warning ウィンドウが表示されます。[Save] をクリックします。

and a	Name:	certnew.ce <b>r</b>		
	Туре:	Security Certificate	e, 1.68 KB	
	From:	172.16.100.26		
		<u>O</u> pen	<u>S</u> ave	Cancel

5. ACS.cer など任意の名前でファイルを保存します。この名前は、ACS 4.0 の ACS Certificate Authority のセットアップで使用しますので、覚えておいてください。

Save As						? X
Save in:	🗇 Local Disk (C	)	•	0 🕫	📁 💷 •	
My Recent Documents Desktop My Documents My Computer	CNS62 Documents and II386 Program Files FFTP WINDOWS Wireless Wireless Wireless Wireless Compub CS.cer Certnew.cer	f Settings rt.cer				
My Network	File <u>n</u> ame:	ACS.cer			-	<u>S</u> ave
	Save as type:	Security Certificat	e		•	Cancel

- 6. インストール時に作成されたデスクトップのショートカットを使用して、ACS Admin を開 きます。
- 7. System Configuration をクリックします。

🖉 Cis	scoSed	cure A(	S - Micros	oft Inte	rnet Ex	plorer		
Eile	<u>E</u> dit	⊻iew	F <u>a</u> vorites	Tools	Help			·
🕝 В.	ack 🝷	Ð •	🗵 🗈 🤇	<u>م  </u>	5earch	☆ Favorites	•	🗟 🍕 📢
Addre	ess 🥫	http://	127.0.0.1:3	809/				



8. [ACS Certificate Setup] をクリックします。

# System Configuration



9. [Install ACS Certificate]をクリックします。

## System Configuration

Edit	
Install ACS Certificate	
Install new certificate	?
C Read certificate from file	
Certificate file	
• Use certificate from storage	
Certificate CN	
Private key file Private key password	

10. Use certificate from storage を選択し、完全修飾ドメイン名の cisco\_w2003.wirelessdemo.local(名前に ACS を使用している場合は ACS.wirelessdemo.local)を入力します。

## System Configuration

Edit
Install ACS Certificate
Install new certificate
O Read certificate from file
Certificate file
Ose certificate from storage
Certificate CN cisco_w2003.wirelessde
Private key file
Private key password

11. [Submit] をクリックします。

## System Configuration

_	_

## Install ACS Certificate

	Installed Certificate Information	
Issued to:	cisco_w2003.wirelessdemo.local	
Issued by:	wirelessdemoca	
Valid from:	March 17 2006 at 08:33:25	
Valid to:	March 16 2008 at 08:33:25	
Yalidity:	ок	

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

12. System Configuration をクリックします。

13. Service Control をクリックし、Restart をクリックします。

Select

CiscoSecure ACS on cisco\_w2003

## **Is Currently Running**

?

Services Log File Configuration
Level of detail
O None
OiFull
Generate New File
Every day
C Every week
O Every month
When size is greater than 2048 KB
Manage Directory
C Keep only the last 7 files
Delete files older than 7 days
💡 Back to Help

- 14. System Configuration をクリックします。
- 15. [Global Authentication Setup]をクリックします。
- 16. Allow EAP-TLS とその下にあるすべてのボックスにチェックマークを付けます。

## System Configuration

### **Global Authentication Setup**

EAP Configuratio	n 🦻
PEAP	
□ Allow EAP-MSCHAPV2	
□ Allow EAP-GTC	
Allow Posture Validation	
Cisco client initial message:	
PEAP session timeout (minutes):	120
Enable Fast Reconnect:	V
EAP-FAST	
EAP-FAST Configuration	
EAP-TLS	
Allow EAP-TLS	
Select one or more of the following options:	
🗹 Certificate SAN comparison	
🗹 Certificate CN comparison	
🗹 Certificate Binary comparison	
EAP-TLS session timeout (minutes):	120

- 17. [Submit + Restart] をクリックします。
- 18. System Configuration をクリックします。
- 19. ACS Certification Authority Setup をクリックします。
- 20. ACS Certification Authority Setup ウィンドウで、前の手順で作成した \*.cer ファイルの名前 と場所を入力します。この例では、作成した \*.cer ファイルは ACS.cer で、ルート ディレ クトリの c:\ に保存されています。
- 21. CA certificate file フィールドに c:\acs.cer と入力し、Submit をクリックします。

## System Configuration

ACS Certification A	Authority Setup		
CA Operatio	ons	?	]
Add new CA certificate to local certificat	te storage		
C to contificanto filo			
	::\acs.cer		
vstem Configuration	::\acs.cer		
ACS Certification Authority Setup	::\acs.cer		
ACS Certification Authority Setup	C:\\BCS.CET	the global :	system certifica
ACS Certification Authority Setup	C:\acs.cer New CA certificate is successully added into storage. CA certificate common name	the global s	system certifica

22. ACS サービスを再起動します。

PEAP support only.

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

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。

- イーサネット ケーブルを使用して CLIENT をスイッチに接続し、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 、wirelessdemo.local ドメインの CLIENT という名前のメンバ コンピュータとして設定しま す。
- Windows XP Professional SP2をインストールします。EAP-TLSおよびPEAPをサポートするには、このインストールが必要です。注意: Windows XP Professional SP2では、Windowsファイアウォールが自動的にオンになります。ファイアウォールをオフにしないでください。

<u> ワイヤレス ネットワーク接続の設定</u>

次のステップを実行します。

 ログオフし、wirelessdemo.local ドメインの WirelessUser アカウントを使用してログインします。注:コマンド・プロンプトでgpupdateと入力し、コンピュータとユーザー構成のグル ープポリシー設定を更新し、ワイヤレスクライアントコンピュータのコンピュータとユーザ ー証明書を直ちに取得します。または、一度ログオフしてから再度ログインしてください。 この操作は gpupdate と同じ効果があります。また、ドメインへのログオンには有線接続を 使用する必要があります。注:証明書がクライアントに自動的にインストールされていることを確認するには、証明書MMCを開き、WirelessUser証明書が[Personal Certificates]フォル ダで使用できることを確認します。

🚡 Console 1			
Le Action Yew Levortes Window Lep	ũ.		
← → 1 10 10 10 10 10 10 10 10 10 10 10 10 1			
🚡 Consule Root/Certificates - Corrent Us	er Personal/Certificates		
📴 Consule Root	Issued To	Essued By	Expiration Date In
<ul> <li>Certificates - Current User</li> <li>Fersonal</li> <li>Turster Rock Certification Authorities</li> <li>Figure Trust</li> <l< td=""><td>Whe essuser</td><td>,//relesstemoca</td><td>3/22/2005 CI</td></l<></ul>	Whe essuser	,//relesstemoca	3/22/2005 CI

- 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。

ichie ai	Wireless Networks Advanced
🖌 Use	Windows to configure my wireless network settings
Availa	able networks:
Toco	onnect :o, disconnect from, or find out more information
abou	Wileless retworks in range, click the button below.
	VIEW WILCESS INCOMINS
belov	Move up
	Move <u>dowr</u>
Learn	Add Remove Properties about <u>setting up wireless network</u>
	Add <u>R</u> emove Properties

- 4. [Add] をクリックします。
- 5. Association タブに移動し、Network name (SSID) フィールドに Employee と入力します。
- 6. Data Encryption に WEP が設定され、The key is provided for me automatically にチェック マークが入っていることを確認します。

<mark>ireless</mark> net	work prope	rties 🛛 🕐
Association ]	Authentication	Connection
Network name (SSID): - Wireless network key		Enployee
This betwo	ntk requires a k	ey for the following:
Network Authentication:		Open 💌
Data encr	yption:	WEP 🗸
Network k	ey:	
Contirm ne	twork key:	
Key index	(edvariced).	
🔽 The ke	y is provided fo	or me auromatically
This is a a access p	computei-to-co oints are not us	mputer (ad hoc) network; wireless sed
		OK Carcel

- 7. Authentication タブに移動します。
- 8. EAP タイプが Smart Card or other Certificate を使用する設定になっていることを確認しま す。そうなっていない場合は、ドロップダウン メニューでこれを選択します。
- 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 オプションを選択します。

Wireless netwo	ork proper	ties		? 🗙		
Association Au	thenlication	Connection				
Select this option wireless Ethern	on to provide el netwcrks E 802.1x au:h	authenticated entication for	d retwork access fo this retwork	ĸ		
EA <sup>o</sup> type: Sr	AP type: Smart Card or other Certhicate					
Aulhenticat	e as compulei e as guest wh	r when compl	Prope uter information s a	ities wailable		
			ок с	ancel		

10. [Properties] をクリックします。

11. 次のウィンドウに示す各ボックスにチェックマークが付いていることを確認します。

Vhen connecting	
 Jse my smart card	
Jse a certificate on this computer	
Jse simple certificate selection (Rec	ommended)
Validate server certificate	
Connect to these servers.	
Frusted Root Certification Authorities:	
ABA.ECOM Root CA	^
ACS333	
ACS40	
Autor dad Certificadora de la Asociació	on Nacional cel Notaria
Autor dad Lierhitzadora del Lioegio Na DelVeren 52 he DCT	cional de Correduria Pu
Balazoon E Tu et Brimeru 74	
C:W/HKT SecureNet CA Clave A	
	View Certficate
	on.
Llos a different upor name for the service li	

- 12. OK を 3 回クリックします。
- 13. システムトレイの無線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。
- 14. Employee の無線ネットワークをクリックし、Connect をクリックします。











- 15. 認証が成功したら、Network Connections を使用して、無線アダプタの TCP/IP 設定を確認 します。無線アダプタには、172.16.100.100 〜 172.16.100.254 の範囲内のアドレスが、 DHCP スコープ、または無線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。
- 16. 機能をテストするため、ブラウザを開いて、http://wirelessdemoca(または、エンタープラ イズ CA サーバの IP アドレス)を表示します。

### 関連情報

- 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 コンフィギュレーション ガイド</u>
- ・ ワイヤレス LAN コントローラと Lightweight アクセスポイントの基本設定例
- ・
   <u>無線 LAN コントローラでの VLAN の設定例</u>
- ・ <u>ワイヤレス LAN コントローラを使用した AP グループ VLAN の設定例</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>