PEAP in UWN con ACS 5.1 e Windows 2003 Server

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Convenzioni Configurazione Esempio di rete Installazione di Windows Enterprise 2003 con IIS, Certification Authority, DNS, DHCP (CA) CA (democa) Cisco 1121 Secure ACS 5.1 Installazione con l'accessorio serie CSACS-1121 Installare il server ACS Configurazione controller Cisco WLC5508 Creare la configurazione necessaria per WPAv2/WPA Autenticazione PEAP Installare lo snap-in Modelli di certificato Creare il modello di certificato per il server Web ACS Abilita il nuovo modello di certificato server Web ACS Configurazione certificato ACS 5.1 Configura certificato esportabile per ACS Installare il certificato nel software ACS 5.1 Configura archivio identità ACS per Active Directory Aggiunta di un controller ad ACS come client AAA Configurazione dei criteri di accesso ACS per reti wireless Crea regola di servizio e criterio di accesso ACS Configurazione CLIENT per PEAP con Windows Zero Touch Eseguire un'installazione e una configurazione di base Installare la scheda di rete wireless Configurazione della connessione di rete wireless Risoluzione dei problemi di autenticazione wireless con ACS Autenticazione PEAP non riuscita con server ACS Informazioni correlate

Introduzione

In questo documento viene descritto come configurare l'accesso wireless sicuro utilizzando i

controller LAN wireless, il software Microsoft Windows 2003 e Cisco Secure Access Control Server (ACS) 5.1 tramite il protocollo PEAP (Protected Extensible Authentication Protocol) con Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) versione 2.

Nota: per informazioni sulla distribuzione di connessioni wireless sicure, fare riferimento al <u>sito</u> <u>Web Microsoft Wi-Fi</u> e al <u>Cisco SAFE Wireless Blueprint</u>.

Prerequisiti

Requisiti

Si presume che il programma di installazione abbia una conoscenza sufficiente dell'installazione di base di Windows 2003 e del controller LAN wireless Cisco, in quanto nel presente documento vengono illustrate solo le configurazioni specifiche per semplificare i test.

Per informazioni sull'installazione iniziale e sulla configurazione dei Cisco serie 5508 Controller, fare riferimento alla <u>Guida all'installazione dei Cisco Wireless Controller serie 5500</u>. Per informazioni sull'installazione iniziale e sulla configurazione dei Cisco serie 2100 Controller, fare riferimento alla <u>Guida introduttiva: Cisco serie 2100 Wireless LAN Controller</u>.

Le guide all'installazione e alla configurazione di Microsoft Windows 2003 sono disponibili all'indirizzo <u>Installazione di Windows Server 2003 R2</u>.

Prima di iniziare, installare il sistema operativo Microsoft Windows Server 2003 con SP1 in ognuno dei server del laboratorio di prova e aggiornare tutti i Service Pack. Installare i controller e i Lightweight Access Point (LAP) e verificare che siano configurati gli ultimi aggiornamenti software.

Windows Server 2003 con SP1, Enterprise Edition viene utilizzato per consentire la configurazione della registrazione automatica dei certificati utente e workstation per l'autenticazione PEAP. La registrazione automatica e il rinnovo automatico dei certificati semplificano la distribuzione dei certificati e migliorano la protezione tramite la scadenza e il rinnovo automatici dei certificati.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Controller Cisco serie 2106 o 5508 con 7.0.98.0
- Cisco 1142 Lightweight Access Point Protocol (LWAPP) AP
- Windows 2003 Enterprise con Internet Information Server (IIS), CA (Certification Authority), DHCP e DNS (Domain Name System) installati
- Cisco 1121 Secure Access Control System Appliance (ACS) 5.1
- Windows XP Professional con SP (e service pack aggiornati) e scheda di interfaccia di rete wireless (NIC) (con supporto CCX v3) o di terze parti.
- Cisco 3750 Switch

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.</u>

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:

Topologia Cisco Secure Wireless Lab



Lo scopo principale di questo documento è quello di fornire la procedura dettagliata per implementare PEAP in Unified Wireless Networks con ACS 5.1 e Windows 2003 Enterprise Server. L'enfasi principale è sulla registrazione automatica del client in modo che il client esegua la registrazione automatica e riceva il certificato dal server.

Nota: per aggiungere WPA (Wi-Fi Protected Access)/WPA2 con TKIP (Temporal Key Integrity Protocol)/AES (Advanced Encryption Standard) a Windows XP Professional con SP, consultare l'aggiornamento WPA2/Wireless Provisioning Services Information Element (WPS IE) per Windows XP con Service Pack 2.

Installazione di Windows Enterprise 2003 con IIS, Certification Authority, DNS, DHCP (CA)

CA (democa)

CA è un computer che esegue Windows Server 2003 con SP2, Enterprise Edition ed esegue i seguenti ruoli:

- Un controller di dominio per il dominio demo.local che esegue IIS
- Un server DNS per il dominio DNS demo.local
- Un server DHCP
- CA radice dell'organizzazione per il dominio demo.local

Per configurare la CA per questi servizi, eseguire la procedura seguente:

- 1. Eseguire un'installazione e una configurazione di base.
- 2. Configurare il computer come controller di dominio.
- 3. Aumentare il livello di funzionalità del dominio.
- 4. Installare e configurare DHCP.
- 5. Installare i servizi certificati.
- 6. Verificare le autorizzazioni di amministratore per i certificati.
- 7. Aggiungere computer al dominio.
- 8. Consenti accesso wireless ai computer.
- 9. Aggiungere utenti al dominio.
- 10. Consenti accesso wireless agli utenti.
- 11. Aggiungere gruppi al dominio.
- 12. Aggiungere utenti al gruppo di utenti wireless.
- 13. Aggiungere computer client al gruppo wirelessusers.

Eseguire l'installazione e la configurazione di base

Attenersi alla procedura seguente:

- 1. Installare Windows Server 2003 con SP2, Enterprise Edition come server autonomo.
- 2. Configurare il protocollo TCP/IP con l'indirizzo IP *10.0.10.10* e la subnet mask *255.255.255.0*.

Configurare il computer come controller di dominio

- 1. Per avviare l'Installazione guidata di Active Directory, scegliere **Start > Esegui**, **digitare dcpromo.exe** e fare clic su **OK**.
- 2. Nella pagina Installazione guidata Active Directory fare clic su Avanti.
- 3. Nella pagina Compatibilità sistema operativo fare clic su Avanti.
- 4. Nella pagina Tipo di controller di dominio selezionare **Controller di dominio per un nuovo dominio** e fare clic su **Avanti**.
- 5. Nella pagina Crea nuovo dominio selezionare Dominio in una nuova foresta e fare clic su

Avanti.

- 6. Nella pagina Installa o configura DNS selezionare **No, installa e configura DNS nel computer** e fare clic su **Avanti**.
- 7. Nella pagina Nuovo nome di dominio digitare demo.local e fare clic su Avanti.
- 8. Nella pagina Nome di dominio NetBIOS, immettere il nome di dominio NetBIOS come **demo** e fare clic su **Avanti**.
- 9. Nella pagina Percorsi del database e delle cartelle di log accettare le directory predefinite del database e delle cartelle di log e fare clic su

Active Directory Installation Wizard	×
Database and Log Folders 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?	
Database folder:	
C:\WINDOWS\NTDS	Bjowse
Where do you want to store the Active Directory log?	
Log folder:	
C:\WINDOWS\NTDS	Browse
< <u>B</u> ack <u>N</u> ext>	Cancel

Avanti. 10. Nella pagina Volume di sistema condiviso verificare che il percorso predefinito della cartella sia corretto e fare clic su

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:
C:\WINDOWS\SYSVOL Bjowse
< <u>B</u> ack <u>N</u> ext> Cancel

Avanti.

11. Nella pagina Autorizzazioni verificare che l'opzione Autorizzazioni compatibili solo con i sistemi operativi Windows 2000 o Windows Server 2003 sia selezionata e fare clic su

Some server programs, such as Windows NT Remote Access Service, read info stored on domain controllers. © Permissions compatible with pre-Windows 2000 server operating systems	mation
$\odot~\underline{P}\text{ermissions}$ compatible with pre-Windows 2000 server operating systems	mauori
Select this option if you run server programs on pre-Windows 2000 server op systems or on Windows 2000 or Windows Server 2003 operating systems the members of pre-Windows 2000 domains.	erating at are
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 Windo Server 2003 operating systems that are members of Active Directory domains authenticated users can read information on this domain.	ows s. Only

12. Nella pagina Password di amministrazione modalità ripristino servizi directory lasciare vuote le caselle della password e fare clic su **Avanti**.

13. Rivedere le informazioni nella pagina Riepilogo e fare clic su

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 SYSVDL folder: C:\WINDOWS\SYSVDL 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.	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 Nest.	mmary Review and confirm the options you se	ected.
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 SYSVDL folder: C:\WINDOWS\SYSVDL 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.	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 Nest.	You chose to:	
The NetBIOS name of the domain is EXAMPLE Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVDL 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.	The NetBIOS name of the domain is EXAMPLE Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVDL folder: C:\WINDOWS\SYSVDL 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.	The new domain name is example.com	. This is also the name of the new forest.
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.	Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVDL folder: C:\WINDOWS\SYSVDL 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.	The NetBIOS name of the domain is E	KAMPLE
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.	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.	Database folder: C:\WINDOWS\NTD: Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSV	S DL
The password of the new domain administrator will be the same as the password of the administrator of this computer.	The password of the new domain administrator will be the same as the password of the administrator of this computer.	The DNS service will be installed and o will be configured to use this DNS serv	configured on this computer. This computer er as its preferred DNS server.
	To change an option, click Back. To begin the operation, click Next.	The password of the new domain admitted the administrator of this computer.	inistrator will be the same as the password of
To change an option, click Back. To begin the operation, click Next.		To change an option, click Back. To b	egin the operation, click Next.

Avanti.

- 14. Al termine dell'installazione di Active Directory, fare clic su Fine.
- 15. Quando viene richiesto di riavviare il computer, fare clic su Riavvia ora.

Aumentare il livello di funzionalità del dominio

- Aprire lo snap-in Domini e trust di Active Directory dalla cartella Strumenti di amministrazione (Start > Programmi > Strumenti di amministrazione > Domini e trust di Active Directory) e quindi fare clic con il pulsante destro del mouse sul computer del dominio CA.demo.local.
- Fare clic su Aumenta livello di funzionalità dominio e quindi selezionare Windows Server 2003 nella pagina Aumenta livello di funzionalità dominio.



3. Fare clic su Aumenta, quindi su OK e infine di nuovo su OK.

Installare e configurare DHCP

- 1. Installare DHCP (Dynamic Host Configuration Protocol) come componente Servizio di rete utilizzando Installazione applicazioni nel Pannello di controllo.
- 2. Aprire lo snap-in DHCP dalla cartella Strumenti di amministrazione (Start > Programmi > Strumenti di amministrazione > **DHCP**), quindi evidenziare il server DHCP, **CA.demo.local**.
- 3. Per autorizzare il servizio DHCP, fare clic su Azione e quindi su Autorizza.
- 4. Nell'albero della console fare clic con il pulsante destro del mouse su **CA.demo.local**, quindi scegliere **Nuovo ambito**.
- 5. Nella pagina iniziale della Creazione guidata ambito fare clic su Avanti.
- 6. Nella pagina Nome ambito digitare **CorpNet** nel campo Nome.

New Scope Wizard		
Scope Name You have to p providing a de	provide an identifying scope name. You also have the option of escription.	(j)
Type a name how the scop	and description for this scope. This information helps you quickly id e is to be used on your network.	entify
Name:	CorpNet	
Description:		
	< <u>B</u> ack <u>N</u> ext>	Cancel

 Fare clic su Avanti e specificare i seguenti parametri:Indirizzo IP iniziale - 10.0.20.1Indirizzo IP finale - 10.0.20.200Lunghezza - 24Subnet mask -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. Fare clic su **Next** (Avanti) e immettere *10.0.20.1* per l'indirizzo IP iniziale e *10.0.20.100* per l'indirizzo IP finale da escludere. Quindi fare clic su **Avanti**. Gli indirizzi IP compresi nell'intervallo da 10.0.20.1 a 10.0.20.100 vengono riservati. Questi indirizzi IP di riserva non sono assegnati dal server DHCP.

w Scope Wizard
Add Exclusions Exclusions are addresses or a range of addresses that are not distributed by the server.
Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.
Start IP address: End IP address: 10.0.20.1 10.0.20.100
Excluded address range:
Remo <u>v</u> e
< <u>B</u> ack <u>N</u> ext > Cancel

- 9. Nella pagina Durata lease fare clic su Avanti.
- 10. Nella pagina Configura opzioni DHCP, selezionare **Sì, configurare le opzioni** e fare clic su **Avanti**.

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 addresses of routers (default gateways), DNS s scope.	DHCP options such as the IP ervers, and WINS settings for that
The settings you select here are for this scope a Server Options folder for this server.	and override settings configured in the
Do you want to configure the DHCP options for	this scope now?
Yes, I want to configure these options now	
O No, I will configure these options later	
	< <u>B</u> ack <u>N</u> ext > Cancel

11. Nella pagina Router (gateway predefinito) aggiungere l'indirizzo del router predefinito *10.0.20.1* e fare clic su **Avanti**.

New Scope Wizard	
Router (Default Gateway) You can specify the routers, or default gateways, to be distributed by this scope.	Ð
To add an IP address for a router used by clients, enter the address below.	
IP address: 10 . 0 . 20 . 1 Add Image: Image state stat	
D <u>o</u> wn	
< <u>B</u> ack <u>N</u> ext > Cancel	

12. Nella pagina Nome dominio e server DNS digitare *demo.local* nel campo Dominio padre, digitare *10.0.10.10* nel campo Indirizzo IP e quindi fare clic su **Aggiungi** e fare clic su **Avanti**.

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

- 13. Nella pagina Server WINS fare clic su Avanti.
- 14. Nella pagina Attiva ambito scegliere **Sì, attiva l'ambito adesso** e fare clic su **Avanti**.

New Scope Wizard		
Activate Scope Clients can obtain address leases only if a s	cope is activated.	S S
Do you want to activate this scope now?		
Yes, I want to activate this scope now		
O No, I will activate this scope later		
		1
	< <u>B</u> ack <u>N</u> ext> C	ancel
	< <u>B</u> ack <u>N</u> ext > C	ancel

15. Al termine, fare clic su Fine.

Installa Servizi certificati

Attenersi alla procedura seguente:

Nota: prima di installare Servizi certificati è necessario installare IIS e l'utente deve appartenere all'unità organizzativa Enterprise Admin.

- 1. Nel Pannello di controllo aprire **Installazione applicazioni** e quindi fare clic su **Installazione componenti di Windows**.
- 2. Nella pagina Aggiunta guidata componenti di Windows scegliere Servizi certificati e quindi fare clic su Avanti.
- 3. Nella pagina Tipo di CA scegliere CA radice dell'organizzazione (enterprise) e fare clic su Avanti.
- Nella pagina Informazioni di identificazione della CA digitare *democa* nella casella Nome comune per la CA. È inoltre possibile immettere gli altri dettagli facoltativi. Fare quindi clic su Avanti e accettare le impostazioni predefinite nella pagina Impostazioni database certificati.
- 5. Fare clic su Next (Avanti). Al termine dell'installazione, fare clic su Fine.
- 6. Fare clic su OK dopo aver letto il messaggio di avviso relativo all'installazione di IIS.

Verifica autorizzazioni amministratore per i certificati

- 1. Scegliere Start > Strumenti di amministrazione > Autorità di certificazione.
- 2. Fare clic con il pulsante destro del mouse su demo CA e quindi scegliere Proprietà.
- 3. Nella scheda Protezione fare clic su Amministratori nell'elenco Utenti e gruppi.
- 4. Nell'elenco Autorizzazioni per amministratori verificare che queste opzioni siano impostate su Consenti:Rilasciare e gestire certificatiGestisci CARichiedi certificatiSe una di queste opzioni è impostata su Nega o non è selezionata, impostare le autorizzazioni su

ca.demo.local Properties	? ×
General Policy Module Exit Mod Certificate Managers Restrictions Auditin	lule Extensions Storage ng Recovery Agents Security
Group or user names: Administrators (DEMO\Administrators Authenticated Users Domain Admins (DEMO\Domain Adm Enterprise Admins (DEMO\Enterprise) nins) e Admins)
Permissions for Administrators	A <u>d</u> d <u>R</u> emove Allow Deny
Read Issue and Manage Certificates Manage CA Request Certificates	
OK	Cancel Apply

Consenti.

5. Fare clic su **OK** per chiudere la finestra di dialogo Proprietà CA demo e quindi chiudere Autorità di certificazione.

Aggiungi computer al dominio

Attenersi alla procedura seguente:

Nota: se il computer è già stato aggiunto al dominio, passare a Aggiungi utenti al dominio.

- 1. Aprire lo snap-in Utenti e computer di Active Directory.
- 2. Nell'albero della console espandere demo.local.

- 3. Fare clic con il pulsante destro del mouse su Computer, scegliere Nuovo e quindi Computer.
- 4. Nella finestra di dialogo Nuovo oggetto Computer digitare il nome del computer nel campo Nome computer e fare clic su **Avanti**. In questo esempio viene utilizzato il nome del computer

	Create in: demo	o.local/Users	
Computer	n <u>a</u> me:		
Computer	name (pre-Window	s 2000):	
CLIENT	Q		
The follow User or gro	ving user or group c oup:	an join this computer t	to a domain.
Default: D	omain Admins		<u>C</u> hange
E Assign	this computer acco	ount as a pre-Window	s 2000 computer
☐ Assign	this computer acco	ount as a backup don	nain controller

- 5. Nella finestra di dialogo Gestito fare clic su Avanti.
- 6. Nella finestra di dialogo Nuovo oggetto Computer fare clic su Fine.
- 7. Ripetere i passaggi da 3 a 6 per creare altri account computer.

Consenti accesso wireless ai computer

- Nell'albero della console Utenti e computer di Active Directory fare clic sulla cartella Computer e fare clic con il pulsante destro del mouse sul computer per cui si desidera assegnare l'accesso wireless. In questo esempio viene illustrata la procedura con computer Client aggiunta al passaggio 7. Fare clic su Proprietà, quindi selezionare la scheda Connessione remota.
- 2. In Autorizzazione di accesso remoto, scegliere Consenti accesso, quindi fare clic su

li	ient Properties ?
	General Operating System Member Of Location Managed By Dial-in
	Remote Access Permission (Dial-in or VPN)
	• Allow access
	○ <u>D</u> eny access
	C Control access through Remote Access Policy
	Callback Options
	• No <u>C</u> allback
	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>

Aggiungi utenti al dominio

- 1. Nell'albero della console Utenti e computer di Active Directory fare clic con il pulsante destro del mouse su **Utenti**, scegliere **Nuovo** e quindi fare clic su **Utente**.
- 2. Nella finestra di dialogo Nuovo oggetto Utente digitare il nome dell'utente wireless. In questo esempio viene utilizzato il nome *wirelessuser* nel campo Nome e *wirelessuser* nel campo Nome di accesso utente. Fare clic su **Next**

New Object - User	
Create ir	n: demo.local/Users
<u>F</u> irst name:	wirelessuser <u>I</u> nitials:
Last name:	
Full n <u>a</u> me:	wirelessuser
<u>U</u> ser logon name:	
wirelessuser	@demo.local
User logon name (p	re- <u>W</u> indows 2000):
DEMO\	wirelessuser
	< Back Next > Cancel

3. Nella finestra di dialogo Nuovo oggetto - Utente digitare una password a scelta nei campi Password e Conferma password. Deselezionare la casella di controllo **Cambiamento obbligatorio password all'accesso successivo** e fare clic su

New Object - Us	er			
Cre	ate in: dem:	o.local/Users		
Password:		•••••		
<u>C</u> onfirm passw	ord:	•••••		
🔲 User <u>m</u> ust	change passw	vord at next logon		
U <u>s</u> er cann	ot change pas	sword		
Pass <u>w</u> ord	never expires			
Account is	disabled			
		< <u>B</u> ack	(<u>N</u> ext>	Cancel
·i				

- 4. Nella finestra di dialogo Nuovo oggetto Utente fare clic su Fine.
- 5. Ripetere i passaggi da 2 a 4 per creare altri account utente.

Consenti accesso wireless agli utenti

- 1. Nell'albero della console Utenti e computer di Active Directory fare clic sulla cartella **Utenti**, fare clic con il pulsante destro del mouse su **utente wireless**, scegliere **Proprietà** e quindi selezionare la scheda **Connessione remota**.
- 2. In Autorizzazione di accesso remoto, scegliere Consenti accesso, quindi fare clic su

Remote control Termin	al Services Profile	COM+
General Address Account	Profile Telephones	Organizatio
Member Of Dial-in	Environment	Sessions
- Remote Access Permission (Dial-in (or VPN)	
Allow access		
C Denv access		
C. Castral second through Remote	Assess Reliev	
C Control access through Hemote	Access Folicy	
Callback Options	,	
No Callback		
C Set by Caller (Routing and Rem	ote Access Service on	y)
C Always Callback to:		
•	1	
🗖 Assign a Static IP Address		
Apply Static Routes	,	
Define motes to enable (exitin Die	15	
connection.	Static Ro	ytes

Aggiungi gruppi al dominio

- 1. Nell'albero della console Utenti e computer di Active Directory fare clic con il pulsante destro del mouse su **Utenti**, scegliere **Nuovo** e quindi fare clic su **Raggruppa**.
- 2. Nella finestra di dialogo Nuovo oggetto Gruppo digitare il nome del gruppo nel campo Nome gruppo e fare clic su **OK**. Nel documento viene utilizzato il nome del gruppo *wireless*

Create in: demo	o.local/Users
Group name:	
wirelessusers	
Group name (pre- <u>W</u> indows 20	000):
wirelessusers	
	- Cruze hans
Group scope	Group type
Group scope	Group type Security
Group scope C Domain local Global	<u>Security</u> <u>Distribution</u>
Group scope Domain local Global Duniversal	<u>Security</u> <u>Distribution</u>
Group scope C Domain local Global C Universal	Group type
Group scope C Domain local Global C Universal	 Group type ⊆ecurity <u>D</u>istribution

Aggiungi utenti al gruppo di utenti wireless

- 1. Nel riquadro dei dettagli di Utenti e computer di Active Directory fare doppio clic sul gruppo *WirelessUsers*.
- 2. Passare alla scheda Membri e fare clic su Aggiungi.
- 3. Nella finestra di dialogo Seleziona utenti, contatti, computer o gruppi digitare il nome degli utenti che si desidera aggiungere al gruppo. In questo esempio viene illustrato come aggiungere l'utente *wireless* al gruppo. Fare clic su

Select this object type:	
Users or Other objects	Object Typ
From this location:	
demo.local	Locations
Enter the object names to select (<u>examples</u>): wirelessuser	heck Nar

4. Nella finestra di dialogo Trovati più nomi fare clic su **OK**. L'account utente wireless viene aggiunto al gruppo

Mambara Lu	relessusers Properties				
neral members Membe	er Of Managed	Ву			
1embers:					
Name Activ	ve Directory Fold	er			
🙍 Administrator 👘 demo	o.local/Users				
🖸 wirelessuser 👘 demo	o.local/Users				
Add	/B				
Add	/B				
Add	/B				

wirelessusers.

- 5. Per salvare le modifiche apportate al gruppo di utenti wireless, fare clic su OK.
- 6. Ripetere questa procedura per aggiungere altri utenti al gruppo.

Aggiungi computer client al gruppo wireless Users

Attenersi alla procedura seguente:

- 1. Ripetere i passaggi 1 e 2 nella sezione <u>Aggiunta di utenti al gruppo di utenti wireless</u> di questo documento.
- 2. Nella finestra di dialogo Seleziona utenti, contatti o computer digitare il nome del computer che si desidera aggiungere al gruppo. In questo esempio viene illustrato come aggiungere il computer denominato *client* al

elect 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):	
client	
Clicity	Check Names
icinca iq	Check Names
	 <u>C</u> heck Names

gruppo. 🛏

3. Fare clic su **Tipi di oggetto**, deselezionare la casella di controllo **Utenti** e quindi selezionare **Computer**.

Object Types		? ×
Select the types of objects you want to find.		
Object types:		
🗹 🎻 Other objects		
Contacts		
Users States		
	OK Can	cel

4. Fare clic su OK due volte. L'account del computer CLIENT viene aggiunto al gruppo

wirelessusers Proper	ties	? X
General Members	Member Of Managed By	
Members:		
Name Administrator Client Wirelessuser	Active Directory Folder demo.local/Users demo.local/Computers demo.local/Users	
Add	<u>B</u> emove	
	OK Cancel	Apply

wirelessusers.

5. Ripetere la procedura per aggiungere altri computer al gruppo.

Cisco 1121 Secure ACS 5.1

Installazione con l'accessorio serie CSACS-1121

L'accessorio CSACS-1121 è dotato del software ACS 5.1. In questa sezione viene fornita una panoramica del processo di installazione e delle attività da eseguire prima di installare ACS.

- 1. Collegare il CSACS-1121 alla rete e alla console dell'accessorio. Vedere <u>il Capitolo 4,</u> <u>"Collegamento dei cavi".</u>
- 2. Accendere il CSACS-1121. Vedere <u>il Capitolo 4, "Accensione dell'accessorio della serie</u> <u>CSACS-1121".</u>
- 3. Eseguire il comando **setup** al prompt della CLI per configurare le impostazioni iniziali per il server ACS. Vedere Esecuzione del programma di installazione.

Installare il server ACS

In questa sezione viene descritto il processo di installazione del server ACS sugli accessori della serie CSACS-1121.

- Eseguire il programma di installazione
- Verifica del processo di installazione
- Operazioni successive all'installazione

Per informazioni dettagliate sull'installazione di Cisco Secure ACS Server, consultare la guida

Configurazione controller Cisco WLC5508

Creare la configurazione necessaria per WPAv2/WPA

Attenersi alla procedura seguente:

Nota: si presume che il controller disponga della connettività di base alla rete e che la raggiungibilità IP dell'interfaccia di gestione abbia esito positivo.

1. Per accedere al controller, selezionare



https://10.0.1.10.

- 2. Fare clic su Login.
- 3. Accedere con l'utente admin predefinito e la password admin predefinita.
- 4. Creare una nuova interfaccia per il mapping della VLAN nel menu Controller.
- 5. Fare clic su Interfacce.
- 6. Fare clic su New.
- 7. Nel campo Nome interfaccia immettere *Dipendente*. Questo campo può contenere qualsiasi valore.
- 8. Nel campo VLAN ID, immettere *20*. (Questo campo può essere qualsiasi VLAN trasportata nella rete).
- 9. Fare clic su **Apply** (Applica).
- 10. Configurare le informazioni come mostrato in questa finestra Interfacce > Modifica:Indirizzo IP interfaccia 10.0.20.2Maschera di rete 255.255.255.0Gateway 10.0.10.1DHCP primario 10.0.10.10

10.0.10.10

սիսիս			S	a <u>v</u> e Configuration	Ping Logo	ut <u>R</u> efrei
	LANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Controller	Interfaces > Edit			< 8	ack A	pply
General Inventory Interfaces	General Informa	tion				
Multicast Network Routes	Interface Name MAC Address	em 00:	ployee 24:97:69:4d:e	0		
Internal DHCP Serve	Configuration					
P Mobility Managemer Ports	Guest Lan					
NTP CDP	Quarantine Quarantine Vian Io	1 1				
Advanced	Physical Informa	tion				
	Port Number		2			
	Active Port		0			
	Enable Dynamic A	P Management				
	Interface Addres	5				
	VLAN Identifier		20			
	IP Address		10.0.20.2			
	Netmask Gateway		255.255.255.	0		
	DHCP Informatio	n				
	Primary DHCP Ser	ver	10.0.10.10			
	Secondary DHCP 5	Server				
	Access Control L	ist				
	ACL Name		none 💌		_	
	Note: Changing the I temporarily disabled some clients.	nterface param and thus may r	eters causes t esult in loss of	he WLANs to be f connectivity for		

- 11. Fare clic su **Apply** (Applica).
- 12. Fare clic sulla scheda WLAN.
- 13. Scegliere Crea nuovo, quindi fare clic su Vai.
- 14. Immettere il nome di un profilo e nel campo SSID WLAN immettere *Employee*.

սիսիս					Sa <u>v</u> e Configuration	Ping I	Logout <u>R</u> efre
	WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMAN	IDS HELP
WLANs	WI	LANs > New			< B	ack	Apply
 WLANs WLANs Advanced 	1	Type Profile Name SSID ID		WLAN Employee Employee 1			

15. Selezionare l'ID della WLAN e fare clic su Apply (Applica).

- 16. Configurare le informazioni per questa WLAN quando viene visualizzata la finestra WLAN > Modifica.Nota: WPAv2 è il metodo di crittografia di livello 2 scelto per questa esercitazione. Per consentire l'associazione di WPA con i client TKIP-MIC a questo SSID, è inoltre possibile selezionare le caselle Modalità compatibilità WPA e Consenti client TKIP WPA2 o i client che non supportano il metodo di crittografia 802.11i AES.
- 17. Nella schermata WLAN > Modifica, fare clic sulla scheda Generale.
- 18. Verificare che la casella Stato sia selezionata per Abilitato e che sia selezionata l'interfaccia appropriata (dipendente). Verificare inoltre che la casella di controllo Abilitato per Broadcast SSID sia

20		nata
30	וסבוטו	ιαια.

վողե				S	a <u>v</u> e Configuration	Ping	Logout <u>R</u> efre
CISCO MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COM	MANDS HELP
WLANs	W	LANs > Edit			< B:	ack	Apply
WLANs	ſ	General Sec	curity QoS	Advanc	ed		
Advanced		Profile Name	Employee				
		Туре	WLAN				
		SSID	Employee				
		Status	Enabled				
		Security Policies	[WPA2][Auth(802.1X)]			
		() c	Modifications dor hanges.)	ne under secu	rity tab will appear	r after ag	pplying the
		Radio Policy	All	•			
		Interface	employee 💌	1			
		Broadcast SSID	Enabled				

- 19. Fare clic sulla scheda **Protezione**.
- 20. Nel sottomenu di layer 2, selezionare **WPA + WPA2** per Sicurezza di layer 2. Per la crittografia WPA2, selezionare **AES + TKIP** per consentire i client TKIP.
- 21. Scegliere 802.1x come metodo di

WLANs > E	dit		
General	Security	QoS	Advanced
Layer 2	Layer 3	AAA S	ervers
Layer 2 WPA+WPA	Layer 2 Security WPA+WPA2 MAC Filtering WPA+WPA2 Parameters		
WPA Po	licy		
WPA2 P	olicy	2	
WPA2 E	WPA2 Encryption AES TKI		ES 🔽 TKIP
Auth Ke	y Mgmt	802.	1X 💌

autenticazione.

- 22. Ignorare il sottomenu di layer 3 poiché non è necessario. Una volta configurato il server RADIUS, è possibile scegliere il server appropriato dal menu Autenticazione.
- 23. Le schede **QoS** e **Advanced** possono essere lasciate in posizione predefinita, a meno che non siano richieste configurazioni speciali.
- 24. Fare clic sul menu **Security** per aggiungere il server RADIUS.
- 25. Nel sottomenu RADIUS fare clic su Autenticazione. Fare quindi clic su Nuovo.
- 26. Aggiungere l'indirizzo IP del server RADIUS (10.0.10.20), che è il server ACS configurato in precedenza.
- 27. Verificare che la chiave condivisa corrisponda al client AAA configurato nel server ACS. Verificare che la casella **Utente di rete** sia selezionata e fare clic su **Applica**.

սիսիս		Saye 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
 AAA General General Authentication Accounting Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies 	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap R Port Number	
Local EAP	Server Status	Enabled 💌
Priority Order	Support for REC 3576	Enabled 💌
Certificate	Server Timeout	2 seconds
Access Control Lists	Network User	Enable
 Wireless Protection Policies 	Management	Enable
Web Auth	IPSec	Enable Enable
Advanced		

28. La configurazione di base è stata completata ed è possibile iniziare a eseguire il test di PEAP.

Autenticazione PEAP

PEAP con MS-CHAP versione 2 richiede certificati sui server ACS ma non sui client wireless. La registrazione automatica dei certificati dei computer per i server ACS può essere utilizzata per semplificare una distribuzione.

Per configurare il server CA in modo che fornisca la registrazione automatica per i certificati del computer e dell'utente, completare le procedure descritte in questa sezione.

Nota: Microsoft ha modificato il modello Server Web con la release di Windows 2003 Enterprise CA in modo che le chiavi non siano più esportabili e l'opzione non sia disponibile. Non sono disponibili altri modelli di certificato forniti con i servizi certificati per l'autenticazione server e consentono di contrassegnare le chiavi come esportabili disponibili nell'elenco a discesa, pertanto è necessario creare un nuovo modello che consenta di eseguire questa operazione.

Nota: Windows 2000 consente l'esportazione di chiavi e queste procedure non devono essere seguite se si utilizza Windows 2000.

Installare lo snap-in Modelli di certificato

- 1. Scegliere Start > Esegui, immettere mmc e fare clic su OK.
- 2. Scegliere Aggiungi/Rimuovi snap-in dal menu File e quindi fare clic su Aggiungi.
- 3. In Snap-in fare doppio clic su Modelli di certificato, fare clic su Chiudi e quindi su OK.

- 4. Nell'albero della console fare clic su **Modelli di certificato**. Tutti i modelli di certificato vengono visualizzati nel riquadro dei dettagli.
- 5. Per ignorare i passaggi da 2 a 4, immettere *certtmpl.msc* per aprire lo snap-in Modelli di certificato.

hyConsole - [Console Root\Ce	rtificate Templates]	
🚡 Elle Action View Favorites	<u>Window</u> <u>H</u> elp	_ & ×
Course Bast		In the second second
Console Root	Template Display Name	Minimum Supported CAs
Certificate Templates	Case Signature Only	Windows 2000
	Exchange User	Windows 2000
	Ligg 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
	30 Smartcard Liser	Windows 2000
	Subardinate Certification Authority	Windows 2000
	Trush Lish Size in a	Windows 2000
	Cage Trust List Signing	windows 2000
	ugg User	Windows 2000
	User Signature Only	Windows 2000
	Web Server	Windows 2000
	Workstation Authe	Windows Server 2003, En 👻
	All Tasks	
Using this template as a base, creates a	template that supports Properties	

Creare il modello di certificato per il server Web ACS

- 1. Nel riquadro dei dettagli dello snap-in Modelli di certificato fare clic sul modello Server Web.
- 2. Scegliere **Duplica modello** dal menu

operties of New Ter	nplate	?
Issuance Requirement General	s Superseded Template Request Handling	s Extensions Security Subject Name
Template display nam	e:	
Copy of Web Server		
Minimum Supported C	As: Windows Server 2003	, Enterprise Edition
After you apply chang name.	jes to this tab, you can no lo	nger change the template
Iemplate name:		
Copy of Web Server		
Validity period:	Renewal peri	od:
2 years	- 6 [wee	ks 💌
-	_ , ,	_
I Publish certificate	in Active Directory	
Directory	itically reenrol if a duplicate	certificate exists in Active
		and 1
	UK	Cancel Apply

Azione. 🖵

3. Nel campo Nome visualizzato modello, immettere

opercies of New 1	femplate	?
Issuance Requirem	ents Superseded Templates	Extensions Securi
General	Request Handling	Subject Name
Template display r	name:	
ACS		
Minimum Commenter	104 m 116 days Carry 2002 F	damin E film
Minimum Supporte	d LAs: Windows Server 2003, E	nterprise Edition
After you apply ch	anges to this tab, you can no long	er change the template
name.		
Iemplate name:		
ACS		
Lune .		
Validhu nariod	Peneural period	
Yainty beind.	<u>n</u> eriewai period.	
2 years	 6 weeks 	·
Publish certific	ate in Active Directory	
E Bublish certific	ate in Active Directory	dificate exists in Active
Publish certific Do not aut Directory	ate in Active Directory omatically reenroll if a duplicate ce	rtificate exists in Active
Publish certific Do not aut Directory	ate in Active Directory omatically reenroll if a duplicate ce	rtificate exists in Active
Do not aut Directory	ate in Active Directory omatically reenroll if a duplicate ce	rtificate exists in Active
Publish certific Do not aut Directory	ate in Active Directory omatically reenroll if a duplicate ce	rtificate exists in Active
Publish certific Do not aut Directory	omatically reenroll if a duplicate ce	rtificate exists in Active

ACS.

4. Andare alla scheda Gestione richieste e selezionare Consenti esportazione della chiave

privata. Verificare inoltre che Signature and Encryption sia selezionato dal menu a discesa

Properties of Ne	w Template ? 🗙
Issuance Requ General	irements Superseded Templates Extensions Security Request Handling Subject Name
<u>P</u> urpose:	Signature and encryption Archive subject's encryption private key Include symmetric algorithms allowed by the subject Delete revoked or expired certificates (do not archive)
Minimum key s	ize: 1024 te key to be exported g when the subject is enrolled and when the private key h this certificate is used:
 Enroll subj Prompt the private key 	ect without requiring any user input user during enrollment user during enrollment and require user input when the r is used
To choose wh (CSPs) should	ich cryptographic service providersSPs be used, click CSPs.
	OK Cancel Apply

Purpose (Scopo).

5. Scegliere Richieste deve utilizzare uno dei seguenti CSP e selezionare Microsoft Base Cryptographic Provider v1.0. Deselezionare tutti gli altri CSP selezionati e fare clic su

5P Selection		?
Choose which cryptograph requests:	hic service providers (CSF	s) can be used in
C Requests can use any	y CSP available on the sul	bject's computer
• Requests must use on	ne of the following CSPs:	
<u>C</u> SPs:		
Gemplus GemSAFE Ca	ard CSP v1.0	-
Infineon SICRYPT Bas	e Smart Card CSP	
Microsoft Base Cryptog	graphic Provider v1.0	Li D. il
Microsoft Base DSS an	nd Diffie-Hellman Cryptogr	aphic Provider
Microsoft DH SChanne	el Liyptographic Provider	
Microsoft Enhanced Li	ryptographic Provider v1.U	ata avaabia Brav
Microsoft Enhanced D	55 and Dime-Heilman Uly SA and AES Counterschi	o Provider
Microsoft BSA SChang	on and Acts Cryptographi and Cruptographic Provider	
	OK.	Cancel
	L	
	OK Ca	ncel Anniu
	01, 00	

6. Andare alla scheda Nome soggetto, scegliere Fornitura nella richiesta e fare clic su

opercies of new 1	emplace	
Issuance Requirem	ents Superseded Templates	Extensions Security
General	Request Handling	Subject Name
• Supply in the re	equest	
Select this opti	on to allow a variety of subject r	name formats or if you do
Autoenrollmen	ss to the domain of which the su is not allowed if you choose this	ibject is a member. s option.
C		
Build from this /	Active Directory information	
Select this optio	n to enforce consistency among e administration	subject names and to
Cubiect name fr	o dumi istration.	
Name I	ninar.	-
INone		
Include e-m	ail name in subject name	
Include this info	mation in alternate subject nam	e:
E-mail name		
DNS name		
Luser prinicip	al name (UPN)	
☐ Service prin	cipal name (SPN)	
	OK	Cancel Apply

- 7. Andare alla scheda Protezione, evidenziare il gruppo Domain Admins e assicurarsi che l'opzione Enroll sia selezionata in Allowed.Nota: se si sceglie di compilare da queste informazioni di Active Directory, controllare solo il nome dell'entità utente (UPN) e deselezionare l'opzione Includi nome di posta elettronica nel nome dell'oggetto e nel nome di posta elettronica. Non è stato immesso un nome di posta elettronica per l'account utente wireless nello snap-in Utenti e computer di Active Directory. Se queste due opzioni non vengono disattivate, la registrazione automatica tenterà di utilizzare la posta elettronica, generando un errore relativo.
- 8. Se necessario, sono disponibili misure di protezione aggiuntive per impedire che i certificati vengano automaticamente estratti. Tali informazioni sono disponibili nella scheda Requisiti di rilascio. Questo punto non viene ulteriormente discusso nel presente

Properties of New Template
General Request Handling Subject Name Issuance Requirements Superseded Templates Extensions Security
Require the following for enrollment:
This number of authorized signatures:
If you require more than one signature, autoenrollment is not allowed.
Policy type required in signature:
Application policy:
Issuance policies:
A <u>d</u> d <u>B</u> emove
Require the following for reenrollment: Same criteria as for enrollment Valid existing certificate
OK Cancel Apply

documento.

9. Fare clic su **OK** per salvare il modello e passare a rilasciare il modello dallo snap-in Autorità di certificazione.

Abilita il nuovo modello di certificato server Web ACS

- 1. Aprire lo snap-in Autorità di certificazione. Eseguire i passaggi da 1 a 3 della sezione <u>Creazione del modello di certificato per il server Web ACS</u>, scegliere l'opzione Autorità di certificazione, scegliere Computer locale e fare clic su Fine.
- 2. Nell'albero della console Autorità di certificazione espandere **ca.demo.local**, quindi fare clic con il pulsante destro del mouse su **Modelli di certificato**.
- 3. Andare a Nuovo > Modello di certificato da emettere.
| 2 🖪 | | |
|------------------|---|--|
| al) | Name | |
| | 🔯 Direc | tory Email Replication |
| s | Dom/ | ain Controller Authentication |
| | 🔯 EFS I | Recovery Agent |
| | 🔯 Basio | : EFS |
| | Dom | ain Controller |
| Manage | | Server |
| | | huter |
| <u>N</u> ew | > | Certificate Template to Issue |
| View | • | rdinate Certification Authority |
| <u>-</u> | | histrator |
| Re <u>f</u> resh | | |
| Export <u>L</u> | ist | |
| Help | | |
| | I)
S
Manage
New
⊻iew
Refresh
Export L
Help | I) Name
I) Name
I Direc
I Dom
I Dom
I Dom
I EFS
I Dom
I EFS
I Dom
I Dom
I EFS
I |

4. Fare clic sul modello di certificato

ACS.

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	<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. Fare clic su OK e aprire lo snap-in Utenti e computer di Active Directory.
- 6. Nell'albero della console fare doppio clic su **Utenti e computer di Active Directory**, fare clic con il pulsante destro del mouse su **demo.local** e quindi scegliere

🐗 Active Directo	ry Users and Computers	
🎸 Eile 🗛 Action	⊻iew <u>W</u> indow <u>H</u> elp	
⇐ ⇒ €<	🛍 🗳 🖻 🗟 😭 🖬	🖥 🖉 💩 💎 🍕 🕽
active Director	y Users and Computers [A demo	local 5 objects
Saved Que Saved Que	ries Name	
Canone	Delegate Control	
	Find	ers
	Connect to Domain	Controllers
	Connect to Domain Controller	SecurityPrincipals
	Raise Domain Functional Level	
	Operations Masters	
	New	•
	All Tas <u>k</u> s	•
	⊻iew	•
	New Window from Here	
	Refresh	
	Export List	
	P <u>r</u> operties	
	Help	

Proprietà.

7. Nella scheda Criteri di gruppo fare clic su **Criterio dominio predefinito** e quindi su **Modifica**. Verrà aperto lo snap-in Editor oggetti Criteri di

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 Policy or demo	,
Group Policy Object Links	No Override Di	isabled
Group Policy Objects higher in the list have the h This list obtained from: AD2003.demo.local	ighest priority.	
New Add Edit	ļ	Jp.
Options Delete Properties	Da	nwn
Block Policy inheritance		
Close	Cancel	Apply

gruppo.

 Nell'albero della console espandere Configurazione computer > Impostazioni di Windows > Impostazioni protezione > Criteri chiave pubblica, quindi scegliere Impostazioni richiesta automatica certificati.



- 9. Fare clic con il pulsante destro del mouse su **Impostazioni richiesta automatica certificati**, quindi scegliere **Nuovo > Richiesta automatica certificati**.
- 10. Nella pagina Installazione guidata richiesta automatica certificati fare clic su Avanti.
- 11. Nella pagina Modello di certificato fare clic su Computer e quindi su

rtificate Template The next time a computer logs on, a c provided.	certificate based on the template you select is
A certificate template is a set of prede computers. Select a template from the	fined properties for certificates issued to following list.
Certificate templates:	
Name	Intended Purposes
Computer	Client Authentication, Server Authentication
Domain Controller	Client Authentication, Server Authentication
Enrolment Agent (Computer)	Certificate Request Agent
•	>
	a Dark Cours
	< <u>Back N</u> ext> Cano

Avanti. 🖵

12. Al termine dell'installazione guidata richiesta automatica certificati, fare clic su **Fine**. Il tipo di certificato Computer verrà visualizzato nel riquadro dei dettagli dello snap-in Editor oggetti Criteri di

gruppo.

🚡 Group Policy Object Editor	
Eile Action View Help	
S Default Domain Policy [AD2003.demo.local] Policy	Automatic Certificate Request
E-B Computer Configuration	Computer
Software Settings	
- Windows Settings	
- Scripts (Startup/Shutdown)	
🖻 🔂 Security Settings	
Account Policies	
Local Policies	
Event Log	
Restricted Groups	
System Services	
🕢 🛄 Registry	
🕖 🔛 File System	
😑 🦳 Public Key Policies	
Encrypting File System	
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. Nell'albero della console espandere Configurazione utente > Impostazioni di Windows > Impostazioni protezione > Criteri chiave pubblica.
- 14. Nel riquadro dei dettagli fare doppio clic su **Impostazioni registrazione** automatica.



15. Scegliere Registra automaticamente i certificati e selezionare Rinnova i certificati scaduti, aggiorna i certificati in sospeso e rimuovi i certificati revocati e Aggiorna i certificati che utilizzano modelli di

	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 rem revoked certificates	iove
	Update certificates that use certificate templates	
certificato	OK Cancel Ap	ply

16. Fare clic su OK.

Configurazione certificato ACS 5.1

Configura certificato esportabile per ACS

Nota: per autenticare un client PEAP WLAN, il server ACS deve ottenere un certificato server dal server CA radice dell'organizzazione (enterprise).

Nota: verificare che Gestione IIS non sia aperto durante il processo di installazione del certificato perché causa problemi con le informazioni memorizzate nella cache.

1. Accedere al server ACS con diritti di amministratore di account.

Add.

2. Selezionare Amministrazione sistema > Configurazione > Certificati server locale. Fare clic su

► 🔗 My Workspace	System A	Administration > Confi	guration > Local Serv	ver Certificates > Loca	Certificates	
Interview Resources	Local	Certificates		Sho	wing 1-1 of 1 50 💌	per page Go
B Users and Identity Stores	Filter		Match if		Gol 🔻	
Policy Elements	-		materia.			
Access Policies		Friendly Name	 Issued To 	Issued By	Valid From	Valid To (Ex
 Monitoring and Reports 		<u>acs</u>	acs	acs	04:29 20.09.2010	04:29 20.09
🔹 💐 System Administration						
 Administrators Accounts Roles Settings Users Authentication Settings Operations Distributed System Management Software Repositories Centralized Software Updates Scheduled Backups Local Operations Configuration Softbace Options Software System Options Dictionaries Local Server Certificates Local Server Certificates Local Certificates Certificates Local Certificates Configuration Licensing Contificates Certificates Certificates	× Add	Edit Delete	[Export		Page 1	• of 1

3. Quando si sceglie un metodo per la creazione di un certificato server, scegliere **Genera richiesta di firma del certificato**. Fare clic su **Next** (Avanti).



 Immettere l'oggetto del certificato e la lunghezza della chiave, quindi fare clic su Fine:Oggetto certificato - CN=acs.demo.localLunghezza chiave -1024



5. ACS richiederà di generare una richiesta di firma del certificato. Fare clic su **OK**.



6. In Amministrazione sistema, passare a Configurazione > Certificati server locale > Richieste di firma in attesa.Nota: questo passaggio è dovuto al fatto che Windows 2003 non consente l'esportazione di chiavi ed è necessario generare una richiesta di certificato basata sul certificato ACS creato in precedenza.



7. Scegliere la voce **Richiesta di firma del certificato** e fare clic su **Esporta**.



8. Salvare il file .pem del certificato ACS sul

Save in: Desktop Computer My Recent Desktop My Documents My Network Places My Computer My Computer My Network Places	?×								Save As
My Recent Documents Desktop My Documents My Documents My Documents My Computer My Computer My Network Places		• 🖽 •	D DE E	G	•			Desktop	Save in:
My Network File name: ACS_ctal							nts er « Places	My Documer My Compute	My Recent Documents Desktop My Documents My Computer
	Save	-	3			_cal	ACS	File name:	My Network
Save as type: .pem Document Co	ancel	•	1			n Document	.pe	Save as type:	Places

Installare il certificato nel software ACS 5.1

Attenersi alla procedura seguente:

1. Aprire un browser e connettersi all'URL del server CA http://10.0.10.10/certsrv.



2. Verrà visualizzata la finestra Servizi certificati Microsoft. Scegliere Richiedi



certificato.

3. Fare clic per inviare una richiesta di certificato



avanzata.

4. Nella richiesta avanzata, fare clic su Invia una richiesta di certificato utilizzando una codifica

Microsoft Certificate Services - ca.demo.local	<u>lome</u>
Advanced Certificate Request	
The policy of the CA determines the types of certificates you can request. Click one of the following options to:	
Create and submit a request to this CA.	
Submit a certificate request by using a base-64-encoded CM PKCS #10 file, or submit a renewal request by using a base-6 encoded PKCS #7 file.	<u>C or</u> 34-
Request a certificate for a smart card on behalf of another use using the smart card certificate enrollment station. Note: You must have an enrollment agent certificate to submit a request of behalf of another user.	<u>er by</u> on

in base 64...

5. Nel campo Richiesta salvata, se la protezione del browser lo consente, individuare il file di richiesta del certificato ACS precedente e

Submit a Certi	ficate Request or Renewal Request	
To submit a sav #10 certificate r source (such as	ed request to the CA, paste a base-64-encoded CMC equest or PKCS #7 renewal request generated by an e a Web server) in the Saved Request box.	or PKCS external
Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):		
Certificate Templ	ate:	
	Administrator	
Additional Attribu	ites:	
Attributes:	× × ×	

inserirlo.

6. Le impostazioni di protezione del browser potrebbero non consentire l'accesso al file su disco. In tal caso, fare clic su **OK** per eseguire un'operazione Incolla manuale.

Windows	Internet Explorer
♪	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. Individuare il file ACS *.pem della precedente esportazione ACS. Aprire il file utilizzando un editor di testo, ad esempio Blocco

ACS_csr PEM File 1 KB Open Edit	
Open With 🔹 🕨	🔊 📕 Notepad
Send To 🔹	, 🏉 Internet Explorer
Cut Copy	Choose Program
Create Shortcut Delete Rename	
Properties	

note.

8. Evidenziare l'intero contenuto del file e fare clic su

🚺 A	CS_cs	r - Note	pad								
File	Edit	Format	View	Help							
	BE	GIN CE	RTT	Undo	-DEO	JES.	Γ	0	MII	∃vj⊂	CA
				Cut							
				Сору	19270						

Copia.

9. Tornare alla finestra Richiesta certificato Microsoft. Incollare il contenuto copiato nel campo

Microsoft Certifica	ate Servi	ces ca.d	emo.local
Submit a Certi	ficate F	Request o	or Rene
To submit a sav renewal request	ed requ t genera	uest to the ated by an	CA, pa: externa
Saved Request:	0		
Base-64-encoded certificate request		Undo	
(CMC or PKCS #10 or		Gut Copy	
PKC5 #7):	-	Paste Delete	
	Browse	Select All	517-
Certificate Templ	ate:		
	Adminis	trator	

10. Scegliere ACS come modello di certificato e fare clic su

Saved Request:	
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	YIZIAYb4QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUA DXoioRABct447w077+uAk8crn26oaEhcfG/ZR15X ONZQ5xnrK23yxEdQNvSFC30mzR2EbQq4s5MvFE2Z /MWqXej3NjpicpAgiV8CSwNd END CERTIFICATE REQUEST
Certificate Temp	Browse for a file to insert. late:
Additional Attribu	utes:
Attributes:	× v ×

11. Una volta rilasciato il certificato, scegliere Codifica Base 64 e fare clic su Scarica

Microsoft Certificate Services - ca.dem	no. local
Certificate Issued	
C DER encoded or C DER encoded or C DER encoded or C DER encoded or C Download certificate ch	ssued to you. Base 64 encoded ain
	File Download - Security Warning X Do you want to open or save this file? Name: certnew.cer Type: Security Certificate, 1.89KB From: ca Open Save Cancel Vibile files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

12. Per salvare il certificato sul desktop, fare clic su Save

Save As				<u> </u>
Save in	Desktop		. 0 0 12	 -
My Recent Documents Desktop My Documents My Computer	My Document My Computer My Network P	s laces		
My Network	File name:	ACS_cert		Save
riaces	Save as type:	Security Certificate	•	Cancel

(Salva).

13. Selezionare ACS > System Administration > Configuration > Local Server Certificates (ACS > Amministrazione sistema > Configurazione > Certificati server locale). Scegliere Associa certificato firmato CA, quindi fare clic su



14. Fare clic su Sfoglia e individuare il certificato



salvato.

Apri.

15. Scegliere il certificato ACS emesso dal server CA e fare clic su

Choose file							<u>?×</u>
Look in:	Desktop		•	+		-	
My Recent Documents Desktop My Documents My Computer	My Documents My Computer My Network Pl ACS_cert ACS_csr	aces					
My Network	File name:	ACS, cert			-	E	Open
Piaces	Files of type:	All Files (".")			•]	Cancel

16. Selezionare inoltre la casella Protocollo per EAP e fare clic su



Fine.

 Il certificato ACS rilasciato dalla CA verrà visualizzato nel certificato locale ACS.

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

Configura archivio identità ACS per Active Directory

Attenersi alla procedura seguente:

- 1. Connettersi ad ACS ed eseguire l'accesso con l'account Admin.
- 2. Passare a Utenti e archivi identità > Archivi identità esterni > Active



Directory.

3. Immettere il dominio Active Directory *demo.local*, immettere la password del server e fare clic su **Test connessione**. Per continuare, fare clic su

General	Directory Groups	Directory Attributes		
Connect	ion Details			
Active D	Directory Domain	demo.local		
addine.				
Please sp	pecify the credentia	Is used to join this machine	e to the Active Directory Domain:	
o Userna	ime:	administrator		
O Passw	ord		-	
reachable	l.	Test Connection		Do
Click on 'S	e. Save Changes' to c cessfully connected	Test Connection onnect to the Active Directo to the Domain, yr Window	ry Domain and save this configuration. 5 Internet Explorer	One
Click on % Click on % have succ to be avail	e. Save Changes' to c cessfully connected lable for use in poli	Test Connection onnect to the Active Directo to the Domain, yr Window icy rules.	ry Domain and save this configuration. s Internet Explorer	
Click on % Click on % have succ to be avail	a. Save Changes' to c cessfully connected lable for use in poli r Authentication St	Test Connection	ry Domain and save this configuration. s Internet Explorer Connection test to 'demo.local' succeede	Onc X
Click on S have succ to be avail End User	e. Save Changes' to c cessfully connected lable for use in pol r Authentication Se able password cha	Test Connection onnect to the Active Directo to the Domain, yr Window icy rules.	ry Domain and save this configuration. 5 Internet Explorer Connection test to 'demo.local' succeede	Onc ×
Click on % have succ to be avail End User F En: F En:	a. Save Changes' to c pessfully connected lable for use in poli r Authentication Se able password cha able machine authe	Test Connection	ry Domain and save this configuration. s Internet Explorer Connection test to 'demo.local' succeede OK	Onc X
Click on 'S have succ to be avail End User IF En: IF En: IF En:	e. Save Changes' to c cessfully connected lable for use in poli r Authentication Se able password cha able machine auth- able Machine Acces	Test Connection onnect to the Active Directo to the Domain, yr Window icy rules. ettings inge entication ss Restrictions	ry Domain and save this configuration. 5 Internet Explorer Connection test to 'demo.local' succeede OK	Onc X

4. Fare clic su Salva

OK.



modifiche.

informazioni sulla procedura di integrazione di ACS 5.x, vedere <u>Esempio di integrazione con</u> <u>Microsoft Active Directory in ACS 5.x e versioni successive</u>.

Aggiunta di un controller ad ACS come client AAA

Attenersi alla procedura seguente:

1. Connettersi ad ACS e selezionare Risorse di rete > Dispositivi di rete e client AAA. Fare clic

				ework Device	5.8
 Interview Resources 	Netw	ork Devic	es		
 Network Device Groups Network Devices and AAA Clients 	Filter			• M	atc
Default Network Device External RADIUS Servers	П	Name	•	IP / Mask	1
🚳 Users and Identity Stores		No data	to dis	splay	
Policy Elements					
🔓 Access Policies					
Monitoring and Reports					
3 System Administration					

su Crea.

2. Immettere quanto segue nei campi:Name - wlcIP - 10.0.1.10Casella di controllo RADIUS - SelezionataSegreto condiviso -

Network Device Gro	ups		
Location	All Locations		Select
Device Type	All Device Types		Select
IP Address Single IP Address IP: 10.0.1.10	(s)	Authentication Options TACACS+ Shared Secret Single Connect Device C Legacy TACACS+ Sing TACACS+ Draft Compl Support RADIUS RADIUS Shared Secret Cisco TrustSec Device ID for TrustS Device ID: Password: TrustSec Advanced Setti	le Connect S liant Single C lec identificat

3. Al termine, fare clic su Invia. Il controller verrà visualizzato come voce nell'elenco Periferiche di rete

ACS.

► 🚭 My Workspace	Network	Resources	i > Ne	twork Devices an	d AAA Clients		
Network Resources	Netw	ork Devic	es				Showing 1-1 of 1
 Network Device Groups Network Devices and AAA Clients 	Filter			Match	it:	٠	Go 💌
Default Network Device External RADIUS Servers		Name	•	IP / Mask	NDG:Location		NDG:Device Type
B Users and Identity Stores	L	wic		10.0.1.10/32	All Locations		All Device Types
Policy Elements							
Access Policies							
Monitoring and Reports							

Configurazione dei criteri di accesso ACS per reti wireless

Attenersi alla procedura seguente:

1. In ACS, selezionare Access Policies > Access Services (Policy di accesso > Servizi di



accesso).

2. Nella finestra Servizi di Access fare clic su

Access P	olicies > Acces	Contraction of the			
Acces	s Services			Showing 1-2 of 2	50 💌 p
Filter:		Match i	t 💌	Go 🔻	
	Name	-	Service Type	Included Policies	Descripti
	Default Devi	ce Admin	Device Administration	Identity Authorization	Default D
	Default Netv	vork Access	Network Access	Identity Authorization	Default

3. Creare un servizio di accesso e immettere un nome, ad esempio WirelessAD. Scegliere

Basato sul modello di servizio, quindi fare clic su

ccess Policies > Access Services > Create	
General Allowed Protocols	
Step 1 - General	
General	
Name: WirelessAD	
Description:	
Access Service Policy Structure	
Based on service template	Selec
C Based on existing service	Selec
C User Selected Service Type Netwo	ork Access

Seleziona.

4. Nella finestra di dialogo della pagina Web, scegliere Accesso di rete - Semplice. Fare clic su OK.

Acces	s Services			Showing 1-4
Filter:	Match if:	G0 🔻		
	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. Nella finestra di dialogo della pagina Web, scegliere **Accesso di rete - Semplice**. Fare clic su **OK**. Dopo aver selezionato il modello, fare clic su

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

6. In Protocolli consentiti selezionare le caselle Consenti MS-CHAPv2 e Consenti PEAP. Fare



clic su Finish (Fine).

7. Quando ACS chiede di attivare il nuovo servizio, fare clic su **Sì**.

D				Authorization
٠ ـ		WirelessAD	Network Access	Identity
n 💌				Authorization
				EX
Access Service?	e created	successfully. Would	d you like to modify the Service	e Selection policy to activate
		Ye	s No	

 Nel nuovo servizio di accesso appena creato/attivato, espandere e scegliere Identità. Per Origine identità, fare clic su Seleziona.



9. Scegliere AD1 per Active Directory configurato in ACS, quindi fare clic su

Filter: Match if: Name Description C AD1 C CN Username Predefined Certificate Authentication Profile C DenyAccess C Internal Hosts C Internal Users	Lisco	Secure ALS -	- We	ebpage Dialog
Name Description C AD1 C CN Username Predefined Certificate Authentication Profile C DenyAccess C Internal Hosts C Internal Users	Juenu	ly store		
Name Description C AD1 C CN Username Predefined Certificate Authentication Profile C DenyAccess Internal Hosts C Internal Users Internal Users	Filter:	I	•	Match if: Go V
C AD1 C CN Username Predefined Certificate Authentication Profile O DenyAccess O Internal Hosts O Internal Users		Name	*	Description
C CN Username Predefined Certificate Authentication Profile C DenyAccess Internal Hosts C Internal Users Internal Users	С	AD1		
C DenyAccess C Internal Hosts C Internal Users	C	CN Usernar	ne	Predefined Certificate Authentication Profile
C Internal Hosts C Internal Users	0	DenyAccess		
O Internal Users	0	Internal Hos	ts	
	0	Internal Use	rs	
C NAC Profiler Default Entry for NAC Profiler	0	NAC Profiler		Default Entry for NAC Profiler

10. Verificare che l'origine dell'identità sia AD1 e fare clic su **Salva**

	Access Policies > A	Access Services > WirelessAD > Identity	
	Single result	It selection 🗢 Rule based result sel	lection
	Identity Source:	AD1	Select
medifiele e		 Advanced Options 	
moailiche.			

Crea regola di servizio e criterio di accesso ACS

Attenersi alla procedura seguente:

1. Andare a Criteri di accesso > Regole selezione servizio.



2. Fare clic su **Crea** nella finestra Criteri di selezione servizi. Assegnare un nome alla nuova regola, ad esempio *WirelessRule*. Selezionare la casella **Protocollo** per trovare una corrispondenza con

Raggio.	
🖉 Cisco Secure ACS Webpage Dialog	
General Name: WirelessRule S	Status: Enabled 💽 In the lower right area of the policy rules scree
Conditions	are available here for use in policy rules.
Results	
	Cisco Secure ACS Webpage Di Enum Definition

Radius

Tacacs

C

0

1

- 3. Selezionate Raggio (Radius), quindi fate clic su OK.
- 4. In Risultati, scegliere **WirelessAD** per Service (creato nel passaggio precedente).

conditions and results are available here for use in policy rules.
Conditions
Protocol: match Radius Select
Results Service: WirelessAD

5. Una volta creata la nuova regola wireless, scegliere e **spostare** questa regola all'inizio, che sarà la prima regola per identificare l'autenticazione radius wireless mediante Active

Ser	vice Se	election P	olicy			
Filt	er: Sta	itus 🔄	Match if: Equa	als 💌		Clear
		Status	Name	Protocol	Conditions	
3		• •	WirelessRule	match Radius		
1		0	Rule-1	match Radius		
2			Rule-2	match Tacacs		
				\ \		
-	_					
		Default		If no rules defin	ed or no enab	led rule
С	reate	I- D	uplicate 👻 E	dit Delete	Move to	V

Configurazione CLIENT per PEAP con Windows Zero Touch

Nell'esempio, CLIENT è un computer che esegue Windows XP Professional con SP che funge da client wireless e ottiene l'accesso alle risorse della Intranet tramite il punto di accesso wireless. Completare le procedure descritte in questa sezione per configurare il client come client wireless.

Eseguire un'installazione e una configurazione di base

Attenersi alla procedura seguente:

- 1. Collegare il CLIENT al segmento della rete Intranet utilizzando un cavo Ethernet collegato all'hub.
- 2. In CLIENT, installare Windows XP Professional con SP2 come computer membro denominato CLIENT del dominio demo.local.

3. Installare Windows XP Professional con SP2. Per poter utilizzare il supporto PEAP, è necessario che sia installato.**Nota:** Windows Firewall viene attivato automaticamente in Windows XP Professional con SP2. Non disattivare il firewall.

Installare la scheda di rete wireless

Attenersi alla procedura seguente:

- 1. Arrestare il computer CLIENT.
- 2. Disconnettere il computer CLIENT dal segmento di rete Intranet.
- 3. Riavviare il computer CLIENT, quindi accedere utilizzando l'account di amministratore locale.
- 4. Installare la scheda di rete wireless. Nota: non installare il software di configurazione del produttore per la scheda di rete wireless. Installare i driver della scheda di rete wireless utilizzando l'Installazione guidata hardware. Inoltre, quando richiesto, fornire il CD fornito dal produttore o un disco con i driver aggiornati da utilizzare con Windows XP Professional con SP2.

Configurazione della connessione di rete wireless

Attenersi alla procedura seguente:

- 1. Disconnettersi e quindi accedere utilizzando l'account WirelessUser nel dominio demo.local.
- 2. Scegliere **Start > Pannello di controllo**, fare doppio clic su **Connessioni di rete**, quindi fare clic con il pulsante destro del mouse su **Connessione rete wireless**.
- 3. Fare clic su **Proprietà**, andare alla scheda **Reti wireless** e verificare che **Usa Windows per configurare le impostazioni della rete wireless** sia

General Wirele	ss Networks Advar	nced
🔽 Use Windo	ws to configure my w	ireless network settings
Available net	works:	
To connect t about wireles	o, disconnect from, o s networks in range,	r find out more information click the button below.
		View Wireless Networks
below:		Move up
below:		Move up Move down
Add	Remove	Move up Move down Properties
Add	Remove	Move up Move down Properties work Advanced
Add	Remove	Move up Move down Properties work

selezionato.

- 4. Fare clic su Add.
- 5. Nella scheda Associazione, immettere Dipendente nel campo Nome rete (SSID).
- 6. Scegliere WPA per Autenticazione di rete e verificare che la crittografia dei dati sia impostata

Wireless network properties	<u>?</u> ×
Association Authentication 0	Connection
Network name (SSID):	mployee
Wireless network key	
This network requires a key	for the following:
Network Authentication:	WPA 💌
Data encryption:	ТКІР
Network key:	
Confirm network key:	
Key index (advanced):	2
The key is provided for r	ne automatically
This is a computer-to-comp access points are not used	uter (ad hoc) network; wireless
	OK Cancel

su TKIP.

- 7. Fare clic sulla scheda Autenticazione.
- 8. Verificare che il tipo EAP sia configurato per l'utilizzo di **PEAP (Protected EAP)**. In caso contrario, sceglierlo dal menu a discesa.
- 9. Se si desidera che il computer venga autenticato prima dell'accesso (che consente l'applicazione di script di accesso o push di Criteri di gruppo), selezionare Autentica come computer quando sono disponibili informazioni sul



computer.

- 10. Fare clic su **Proprietà**.
- 11. Poiché PEAP prevede l'autenticazione del server da parte del client, verificare che il **certificato Convalida server** sia selezionato. Verificare inoltre che l'autorità di certificazione che ha rilasciato il certificato ACS sia selezionata nel menu Autorità di certificazione radice attendibili.
- 12. Scegliere **Password protetta (EAP-MSCHAP v2)** in Metodo di autenticazione in quanto viene utilizzata per l'autenticazione

Protected EAP Properties	1
When connecting:	
Validate server certificate	
Connect to these servers:	
Trusted Root Certification Authorities:	
C&W HKT SecureNet CA Root	
Certiposte Classe A Personne	
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	Concession of the local distance of the loca

interna.

correttamente

- 13. Verificare che la casella di controllo **Abilita riconnessione rapida** sia selezionata. Quindi, fare clic su **OK** tre volte.
- 14. Fare clic con il pulsante destro del mouse sull'icona della connessione di rete wireless in systray e quindi scegliere **Visualizza reti wireless disponibili**.
- 15. Fare clic sulla rete wireless Employee e quindi su **Connetti**. Il client wireless visualizzerà **Connesso** se la connessione viene stabilita

⁽⁽ † ⁾⁾ Wireless Network Connection		
Network Tasks	Choose a wireless network	
💋 Refresh network list	Click an item in the list below to connect to a wireless network in r information.	ange or to get more
Set up a wireless network for a home or small office	((Q)) Employee	Connected 👷
	Security-enabled wireless network (WPA2)	

- 16. Al termine dell'autenticazione, controllare la configurazione TCP/IP per la scheda di rete wireless utilizzando Connessioni di rete. Deve avere un intervallo di indirizzi compreso tra 10.0.20.100 e 10.0.20.200 dall'ambito DHCP o dall'ambito creato per i client wireless CorpNet.
- 17. Per verificare la funzionalità, aprire un browser e selezionare http://10.0.10.10 (o l'indirizzo IP del server CA).

Risoluzione dei problemi di autenticazione wireless con ACS

Attenersi alla procedura seguente:

1. Selezionare ACS > Monitoraggio e report, quindi fare clic su Avvia Visualizzatore



monitoraggio e report.

2. Viene visualizzata una finestra ACS separata. Fare clic su

🔻 🔝 Monitoring and Reports				
Dashboard .				
Alarms				
Inbox				
- Thresholds				
Schedules				
Reports				
- Favorites				
- Shared				
🗄 - Catalog				
Troubleshooting				
- Connectivity Tests				
ACS Support Bundle				
Expert Troubleshooter				
Monitoring Configuration				

Dashboard.

3. Nella sezione Report preferiti fare clic su Autenticazioni - RADIUS -

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

Oggi. ^L

4. In un registro tutte le autenticazioni RADIUS vengono visualizzate come Superate o Non riuscite. All'interno di una voce registrata, fare clic sull'**icona della lente di ingrandimento** nella colonna

Dettagli.

AAA Protocol > RADIUS Authentication									
Authentication Status : Date :	Pass or Fail September 22, 2010 (Last 30 Minutes Last Hour Last 12 Hours Today Yesterday Last 7 Days Last 30 Days)								
Generated on September 22, 2010 5:51:34 PM PDT									
2 Reload									
✓=Pass ×=Fail									
Logged At	RADIUS NAS Status Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method			
Sep 22,10 5:51:17.843 P	M 🖌	9	wirelessuser	00-21-5c-69-9a-39	WirelessAD	PEAP (EAP-MSCHAPv2)			

5. Nel campo Dettagli autenticazione RADIUS vengono fornite molte informazioni sui tentativi
| AAA Protocol > F | ADIUS Authentication Detail |
|---------------------------|----------------------------------|
| ACS session ID : a | cs/74551189/31 |
| Date : S | eptember 22, 2010 |
| Generated on Septe | mber 22, 2010 5:52:16 PM PDT |
| Authentication Sum | imary |
| 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: | <u>WirelessAD</u> |
| Identity Store: | AD1 |
| Authorization Profile | es: Permit Access |
| CTS Security Group |):
 |
| Authentication
Method: | PEAP(EAP-MSCHAPv2) |

registrati. L

 Il conteggio riscontri del servizio ACS può fornire una panoramica dei tentativi corrispondenti alle regole create in ACS. Selezionare ACS > Access Policies > Access Services, quindi fare clic su Service Selection Rules (Regole di selezione

Results Service	Hit Count
WirelessAD	33
Default Network Access	0

Autenticazione PEAP non riuscita con server ACS

Quando il client non esegue l'autenticazione PEAP con un server ACS, verificare se è possibile trovare il messaggio di errore NAS duplicated authentication try (Tentativo di autenticazione duplicata NAS) nell'opzione Failed TRIES (Tentativi non riusciti) del menu Report and Activity (Report e attività) di ACS.

Èpossibile che questo messaggio di errore venga visualizzato quando Microsoft Windows XP SP2 è installato nel computer client e Windows XP SP2 esegue l'autenticazione in un server di terze parti diverso da un server Microsoft IAS. In particolare, il server Cisco RADIUS (ACS) utilizza un metodo diverso per calcolare l'ID EAP-TLV (Extensible Authentication Protocol Type:Length:Value format) rispetto al metodo utilizzato da Windows XP. Microsoft ha identificato questo problema come difetto nel supplicant di XP SP2.

Per un aggiornamento rapido, contattare Microsoft e fare riferimento all'articolo <u>Autenticazione</u> <u>PEAP non riuscita quando ci si connette a un server RADIUS di terze parti</u>. Il problema di base è che sul lato client, con l'utilità Windows, l'opzione di riconnessione rapida è disabilitata per impostazione predefinita per PEAP. Tuttavia, questa opzione è attivata per impostazione predefinita sul lato server (ACS). Per risolvere il problema, deselezionare l'opzione Riconnessione rapida sul server ACS (in Opzioni globali di sistema). In alternativa, è possibile abilitare l'opzione di riconnessione rapida sul lato client per risolvere il problema.

Per abilitare la riconnessione rapida sul client che esegue Windows XP con l'utilità Windows, eseguire la procedura seguente:

- 1. Selezionare Start > Impostazioni > Pannello di controllo.
- 2. Fare doppio clic sull'icona Connessioni di rete.
- 3. Fare clic con il pulsante destro del mouse sull'icona **Connessione rete senza fili** e quindi scegliere **Proprietà**.
- 4. Fare clic sulla scheda Reti wireless.
- 5. Scegliere l'opzione **Usa Windows per configurare le impostazioni della rete wireless** per consentire a Windows di configurare la scheda client.
- 6. Se è già stato configurato un SSID, sceglierlo e fare clic su **Proprietà**. In caso contrario, fare clic su **New** (Nuovo) per aggiungere una nuova WLAN.
- 7. Immettere il SSID nella scheda Associazione. Verificare che Autenticazione di rete sia **Aperta** e che Crittografia dati sia impostata su **WEP**.
- 8. Fare clic su Autenticazione.
- 9. Selezionare l'opzione Abilita autenticazione IEEE 802.1x per questa rete.
- 10. Selezionate PEAP come tipo EAP, quindi fate clic su Proprietà (Properties).
- 11. Scegliere l'opzione Abilita riconnessione rapida nella parte inferiore della pagina.

Informazioni correlate

- PEAP in Unified Wireless Networks con ACS 4.0 e Windows 2003
- Esempio di configurazione di Cisco Wireless LAN Controller (WLC) e Cisco ACS 5.x (TACACS+) per l'autenticazione Web
- Guida all'installazione e all'aggiornamento di Cisco Secure Access Control System 5.1
- Documentazione e supporto tecnico Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).