PEAP in Unified Wireless Networks con Microsoft Internet Authentication Service (IAS)

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Convenzioni Panoramica di PEAP Configurazione Esempio di rete Configurazioni Configurazione di Microsoft Windows 2003 Server Configurazione di Microsoft Windows 2003 Server Installare e configurare i servizi DHCP in Microsoft Windows 2003 Server Installare e configurare il server Microsoft Windows 2003 come server CA (Certification Authority) Connetti client al dominio Installare il servizio di autenticazione Internet nel server Microsoft Windows 2003 e richiedere un certificato Configurare il servizio di autenticazione Internet per l'autenticazione PEAP-MS-CHAP v2 Aggiungi utenti ad Active Directory Consenti accesso wireless agli utenti Configurazione del controller LAN wireless e dei Lightweight Access Point Configurare il WLC per l'autenticazione RADIUS tramite il server MS IAS RADIUS Configurazione di una WLAN per i client Configurazione dei client wireless Configurazione dei client wireless per l'autenticazione PEAP-MS CHAPv2 Verifica e risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene fornito un esempio di configurazione per configurare l'autenticazione PEAP (Protected Extensible Authentication Protocol) con MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) versione 2 in una rete wireless unificata Cisco con Microsoft Internet Authentication Service (IAS) come server RADIUS.

Prerequisiti

Requisiti

Si presume che il lettore abbia una conoscenza dell'installazione di base di Windows 2003 e dell'installazione del controller Cisco, in quanto in questo documento vengono illustrate solo le configurazioni specifiche per facilitare i test.

Nota: questo documento ha lo scopo di fornire ai lettori un esempio della configurazione richiesta sul server MS per l'autenticazione PEAP - MS CHAP. La configurazione del server Microsoft illustrata in questa sezione è stata testata in laboratorio e ha rilevato che funziona come previsto. In caso di problemi durante la configurazione del server Microsoft, contattare Microsoft per assistenza. Cisco TAC non supporta la configurazione del server Microsoft Windows.

Per informazioni sull'installazione iniziale e sulla configurazione dei Cisco serie 4400 Controller, fare riferimento alla <u>Guida introduttiva: Cisco serie 4400 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.

Componenti usati

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

- Cisco serie 4400 Controller con firmware versione 4.0
- Cisco 1131 Lightweight Access Point Protocol (LWAPP) AP
- Windows 2003 Enterprise Server (SP1) con i servizi Internet Authentication Service (IAS), Certificate Authority (CA), DHCP e Domain Name System (DNS) installati
- Windows XP Professional con SP 2 (e Service Pack aggiornati) e Cisco Aironet 802.11a/b/g Wireless Network Interface Card (NIC)
- Aironet Desktop Utility versione 4.0
- Cisco 3560 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</u> <u>dei documenti.</u>

Panoramica di PEAP

PEAP utilizza Transport Level Security (TLS) per creare un canale crittografato tra un client PEAP di autenticazione, ad esempio un laptop Wireless, e un autenticatore PEAP, ad esempio Microsoft

Internet Authentication Service (IAS) o qualsiasi server RADIUS. PEAP non specifica un metodo di autenticazione, ma fornisce una protezione aggiuntiva per altri protocolli di autenticazione EAP, ad esempio EAP-MSCHAPv2, che possono funzionare tramite il canale crittografato TLS fornito da PEAP. Il processo di autenticazione PEAP è costituito da due fasi principali:

PEAP fase uno: canale crittografato TLS

Il client wireless viene associato all'access point. Un'associazione basata su IEEE 802.11 fornisce un'autenticazione a sistema aperto o a chiave condivisa prima che venga creata un'associazione sicura tra il client e il punto di accesso (LAP). Una volta stabilita l'associazione basata su IEEE 802.11 tra il client e il punto di accesso, la sessione TLS viene negoziata con l'access point. Al termine dell'autenticazione tra il client wireless e il server IAS, la sessione TLS viene negoziata tra di essi. La chiave derivata in questa negoziazione viene utilizzata per crittografare tutte le comunicazioni successive.

PEAP fase due: comunicazione autenticata da EAP

La comunicazione EAP, che include la negoziazione EAP, avviene all'interno del canale TLS creato da PEAP nella prima fase del processo di autenticazione PEAP. Il server IAS autentica il client wireless con EAP-MS-CHAP v2. Il LAP e il controller inoltrano messaggi solo tra il client wireless e il server RADIUS. Il WLC e il LAP non possono decrittografare questi messaggi perché non è l'endpoint TLS.

Dopo che si è verificata la prima fase PEAP e il canale TLS è stato creato tra il server IAS e il client wireless 802.1X, per un tentativo di autenticazione riuscito in cui l'utente ha fornito credenziali basate su password valide con PEAP-MS-CHAP v2, la sequenza di messaggi RADIUS è la seguente:

- 1. Il server IAS invia un messaggio di richiesta di identità al client: EAP-Request/Identity.
- 2. Il client risponde con un messaggio di risposta di identità: Risposta EAP/Identità.
- 3. Il server IAS invia un messaggio di richiesta MS-CHAP v2: EAP-Request/EAP-Type=EAP MS-CHAP-V2 (verifica).
- 4. Il client risponde con una richiesta MS-CHAP v2 e una risposta: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response).
- 5. Il server IAS restituisce un pacchetto MS-CHAP v2 con esito positivo quando il server ha autenticato correttamente il client: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (esito positivo).
- 6. Il client risponde con un pacchetto MS-CHAP v2 che ha avuto esito positivo quando ha autenticato correttamente il server: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (operazione riuscita).
- 7. Il server IAS invia un messaggio EAP-TLV che indica la riuscita dell'autenticazione.
- 8. Il client risponde con un messaggio di stato EAP-TLV riuscito.
- 9. Il server completa l'autenticazione e invia un messaggio di operazione riuscita EAP utilizzando testo normale. Se le VLAN vengono distribuite per l'isolamento del client, gli attributi VLAN sono inclusi in questo messaggio.

Configurazione

In questo documento viene illustrato un esempio di configurazione di PEAP MS-CHAP v2.

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:



Wireless Client C1 Wireless Client C2

In questa configurazione, un server Microsoft Windows 2003 svolge i seguenti ruoli:

- Controller di dominio per il dominio Wireless.com
- Server DHCP/DNS
- Server CA (Certification Authority)
- Active Directory per gestire il database utenti
- Servizio di autenticazione Internet (IAS) per autenticare gli utenti wireless

Il server si connette alla rete cablata tramite uno switch di layer 2, come mostrato.

Il controller WLC (Wireless LAN Controller) e il LAP registrato si connettono anche alla rete tramite lo switch di layer 2.

I client wireless C1 e C2 utilizzeranno l'autenticazione Wi-Fi Protected Access 2 (WPA2) - PEAP MSCHAP v2 per connettersi alla rete wireless.

L'obiettivo è configurare il server Microsoft 2003, il controller LAN wireless e il punto di accesso Light Weight per autenticare i client wireless con l'autenticazione PEAP MSCHAP v2.

La sezione successiva spiega come configurare i dispositivi per questa installazione.

Configurazioni

In questa sezione viene esaminata la configurazione necessaria per configurare l'autenticazione PEAP MS-CHAP v2 nella WLAN:

- Configurazione di Microsoft Windows 2003 Server
- Configurare il controller WLC (Wireless LAN Controller) e i punti di accesso Light Weight
- Configurazione dei client wireless

Iniziare con la configurazione del server Microsoft Windows 2003.

Configurazione di Microsoft Windows 2003 Server

Configurazione di Microsoft Windows 2003 Server

Come indicato nella sezione Installazione di rete, utilizzare il server Microsoft Windows 2003 nella rete per eseguire queste funzioni.

- Controller di dominio per il dominio Wireless
- Server DHCP/DNS
- Server CA (Certification Authority)
- Servizio di autenticazione Internet (IAS, Internet Authentication Service) per autenticare gli utenti wireless
- Active Directory per gestire il database utenti

Configurare il server Microsoft Windows 2003 per questi servizi. Iniziare con la configurazione del server Microsoft Windows 2003 come controller di dominio.

Configurare il server Microsoft Windows 2003 come controller di dominio

Per configurare il server Microsoft Windows 2003 come controller di dominio, attenersi alla seguente procedura:

 Fare clic sul pulsante Start, scegliere Esegui, digitare dcpromo.exe e quindi fare clic su OK per avviare l'Installazione guidata di Active Directory.



2. Fare clic su **Avanti** per eseguire l'Installazione guidata Active Directory.

ctive	e Directory Installation Wizard
Or	perating System Compatibility Improved security settings in Windows Server 2003 affect older versions of Windows.
	Domain controllers running Windows Server 2003 implement security settings that require clients and other servers to communicate with those domain controllers in a more secure way.
	Some older versions of Windows, including Windows 95 and Windows NT 4.0 SP3 or earlier, do not meet these requirements. Similarly, some non-Windows systems, including Apple Mac OS X and SAMBA clients, might not meet these requirements.
	For more information, see <u>Compatibility Help</u> .
	< <u>B</u> ack <u>Next></u> Cancel

3. Per creare un nuovo dominio, scegliere l'opzione **Controller di dominio** per un nuovo dominio.

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

4. Fare clic su **Avanti** per creare una nuova foresta di alberi di dominio.

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

 Se DNS non è installato nel sistema, la procedura guidata fornisce le opzioni per configurare DNS. Scegliere No, Installa e configura DNS nel computer. Fare clic su Next (Avanti).

tive Directory Installation Wizard	J
Install or Configure DNS You can configure or install Domain Naming Service (DNS) on this comput	er.
Domain Naming Service (DNS) is not configured on this computer. Is DNS running on this network?	already
Yes, I will configure the DNS client	
No, just install and configure DNS on this computer	
< Back Next >	Cancel

 Digitare il nome DNS completo per il nuovo dominio. In questo esempio viene utilizzato Wireless.com e fare clic su Avanti.

e Directory Installation Wizard			
lew Domain Name Specify a name for the new domain.			So and a second
Type the full DNS name for the new do (for example: headquarters.example.mi	main crosoft.com).		
<u>Full DNS name for new domain:</u>			
Wireless.com			
· •			
	Z Back	Next] [Canad

 Immettere il nome NETBIOS del dominio e fare clic su Avanti. In questo esempio viene utilizzato WIRELESS.

ctive Directory Installation W	izard
NetBIOS Domain Name Specify a NetBIOS name for	r the new domain.
This is the name that users o domain. Click Next to accep	of earlier versions of Windows will use to identify the new at the name shown, or type a new name.
Domain NetBIOS name:	WIRELESS
	< <u>B</u> ack <u>N</u> ext > Cancel

8. Scegliere i percorsi del database e del registro per il dominio. Fare clic su **Next** (Avanti).

ive Directory Installation Wizard		
Database and Log Folders Specify the folders to contain the Active Dir	rectory database and log fi	iles.
For best performance and recoverability, sto hard disks.	ore the database and the k	og on separate
Where do you want to store the Active Dire	ctory database?	
<u>D</u> atabase folder:		
C:\WINDOWS\NTDS		Browse
Where do you want to store the Active Dire	ctory log?	
C:\WINDOWS\NTDS		Br <u>o</u> wse
	< Back Nex	t> Cancel

9. Scegliere un percorso per la cartella Sysvol. Fare clic su **Next** (Avanti).

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 fill of the SYSVOL folder are replicated to all domain controllers in the do	les. The contents omain.
The SYSVOL folder must be located on an NTFS volume.	
Enter a location for the SYSVOL folder.	
Eolder location:	
C:\WINDOWS\SYSVOL	B <u>r</u> owse
< <u>B</u> ack <u>N</u> e	xt > Cancel

10. Scegliere le autorizzazioni predefinite per gli utenti e i gruppi. Fare clic su **Next** (Avanti).

ctive Dir	ectory Installation Wizard
Permi : Se	ssions elect default permissions for user and group objects.
So	ome server programs, such as Windows NT Remote Access Service, read information pred on domain controllers.
۲	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.
C	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

11. Impostare la password dell'amministratore e fare clic su **Avanti**.

Active Directory Installation Wizard
Directory Services Restore Mode Administrator Password This password is used when you start the computer in Directory Services Restore Mode.
Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.
The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.
Restore Mode Password:
Confirm password:
For more information about Directory Services Restore Mode, see <u>Active Directory Help</u> .
< <u>B</u> ack <u>N</u> ext > Cancel

12. Fare clic su **Avanti** per accettare le opzioni di dominio impostate in precedenza.

You chose to: Configure this server as the first domain controller in a new forest of domain trees. The new domain name is Wireless.com. This is also the name of the new forest. The NetBIOS name of the domain is WIRELESS Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The password of the new domain administrator will be the same as the password of the administrator of this computer.	ummary Review and confirm the options you s	alactad	
You chose to: Configure this server as the first domain controller in a new forest of domain trees. The new domain name is Wireless.com. This is also the name of the new forest. The NetBIOS name of the domain is WIRELESS Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The password of the new domain administrator will be the same as the password of the administrator of this computer.	neview and commit the options you s		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Configure this server as the first domain controller in a new forest of domain trees. The new domain name is Wireless.com. This is also the name of the new forest. The NetBIOS name of the domain is WIRELESS Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The password of the new domain administrator will be the same as the password of the administrator of this computer. To change an option, click Back. To begin the operation, click Next	You chose to:		
 The new domain name is Wireless.com. This is also the name of the new forest. The NetBIOS name of the domain is WIRELESS Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The password of the new domain administrator will be the same as the password of the administrator of this computer. 	Configure this server as the first domai	n controller in a new forest of o	domain trees.
The NetBIOS name of the domain is WIRELESS Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The password of the new domain administrator will be the same as the password of the administrator of this computer. To change an option, click Back. To begin the operation, click Next	The new domain name is Wireless.com	m. 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 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 V	VIRELESS	
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 /OL	
To change an option, click Back. To begin the operation, click Next	The password of the new domain adm the administrator of this computer.	iinistrator will be the same as th	ne password of
To change an option, click Back. To begin the operation, click Next			_
r o originge arreption, ellek black. Te begin the operation, ellek ritext	To change an option, click Back. To t	begin the operation, click Next	
		/ Back Na	ut Cancel

13. Fare clic su **Fine** per chiudere l'Installazione guidata Active Directory.



14. Riavviare il server per rendere effettive le

Windows must be restarted before the changes made by the Active Directory Installation wizard take effect.	Activ	ve Directory Installation W	/izard	
	Wi Dir	ndows must be restarted before ectory Installation wizard take e	the changes made by the Active Iffect.	
Li Kostart Now il Don't Restart Now I		Postat Nou	Don't Restart Now	

In questo passaggio è stato configurato il server Microsoft Windows 2003 come controller di dominio e creato un nuovo dominio **Wireless.com**. Configurare quindi i servizi DHCP nel server.

Installare e configurare i servizi DHCP in Microsoft Windows 2003 Server

Il servizio DHCP sul server Microsoft 2003 viene utilizzato per fornire indirizzi IP ai client wireless. Per installare e configurare i servizi DHCP in questo server, attenersi alla seguente procedura:

- 1. Scegliere Installazione applicazioni nel Pannello di controllo.
- 2. Fare clic su Aggiungi/Rimuovi componenti di Windows.
- 3. Scegliere Servizi di rete e fare clic su Dettagli.
- 4. Selezionare DHCP (Dynamic Host Configuration Protocol) e fare clic su

Networking Services	
To add or remove a component, click the c of the component will be installed. To see w	heck box. A shaded box means that only par what's included in a component, click Details.
Sub <u>c</u> omponents of Networking Services:	
🗹 📇 Domain Name System (DNS)	1.7 MB 🔄
🔽 县 Dynamic Host Configuration Protoc	ol (DHCP) 0.0 MB
🗌 🔲 🌉 Internet Authentication Service	0.0 MB
🗌 🗔 🚚 Remote Access Quarantine Service	e 0.1 MB
🔲 🔜 RPC over HTTP Proxy	0.0 MB
🗌 🗐 Simple TCP/IP Services	0.0 MB
🔲 🗆 🚚 Windows Internet Name Service (W	VINS) 0.9 MB 📘
Description: Sets up a DHCP server that addresses to client computer	automatically assigns temporary IP rs on the same network.
Total disk space required: 3.4 ME	3 Details
Space available on disk: 7224.5 ME	B Contraction
	OK Cancel

5. Fare clic su **Avanti** per installare il servizio DHCP.

Ĩ
nat only nt, click
) MB 🔼
3 МВ 📃
ив
) МВ
MB
protocols.
alls

6. Fare clic su **Fine** per completare l'installazione.



- 7. Per configurare i servizi DHCP, fare clic su Start > Programmi > Strumenti di amministrazione e fare clic sullo snap-in DHCP.
- 8. Selezionare il server DHCP tsweb-lapt.wireless.com (nell'esempio).
- 9. Fare clic su **Azione**, quindi su **Autorizza** per autorizzare il servizio DHCP.



- Nell'albero della console fare clic con il pulsante destro del mouse su tsweblapt.wireless.com, quindi scegliere Nuovo ambito per definire un intervallo di indirizzi IP per i client wireless.
- 11. Nella pagina Creazione guidata ambito della Creazione guidata ambito fare clic su Avanti.



12. Nella pagina Nome ambito digitare il nome dell'ambito DHCP. In questo esempio, utilizzare

DHCP-Clients come nome dell'ambito. Fare clic su **Next** (Avanti).

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

 Nella pagina Intervallo di indirizzi IP immettere gli indirizzi IP iniziale e finale dell'ambito e fare clic su Avanti.

New Scope Wizard	
IP Address Range You define the scope address range by ide addresses.	entifying a set of consecutive IP
Enter the range of addresses that the scop	e distributes.
Start IP address: 10 . 77 . 244 . 2	:18
End IP address: 10 . 77 . 244 . 2	:19
A subnet mask defines how many bits of ar IDs and how many bits to use for the host I length or as an IP address.	TP address to use for the network/subnet D. You can specify the subnet mask by
Length: 8	
S <u>u</u> bnet mask: 255 . 0 . 0 .	0
	< <u>B</u> ack <u>N</u> ext > Cancel

14. Nella pagina Aggiungi esclusioni specificare l'indirizzo IP che si desidera riservare/escludere dall'ambito DHCP. Fare clic su **Next** (Avanti).

Type the IP address r address, type an addr	ange that you want to exclu ress in Start IP address only	ude. If you want to exclude a single
Start IP address:	End IP address:	
.		Add
Excluded address ran	ige:	
		Remo⊻e
J		

15. Indicare la durata del lease nella pagina Durata lease e fare clic su Avanti.

New Scope Wizard	
Lease Duration The lease duration specifies how long a client can use an IP address from this scope.	J.
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate. Set the duration for scope leases when distributed by this server.	
Limited to:	
Days: Hours: Minutes:	
< <u>B</u> ack <u>N</u> ext > Cance	3 3

 Nella pagina Configura opzioni DHCP, scegliere Sì, configura ora l'opzione DHCP, quindi fare clic su Avanti.

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? • Mes, I want to configure these options now! • Ng, I will configure these options later
 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. Ng, I will configure these options later
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
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
 Yes, I want to configure these options now No, I will configure these options later
No, I will configure these options later
< <u>B</u> ack <u>N</u> ext > Cancel

17. Se è presente un router gateway predefinito, indicare l'indirizzo IP del router gateway nella pagina Router (gateway predefinito) e fare clic su **Avanti**.

I <u>P</u> address:		
- 	Add	
10.77.244.220	<u>R</u> emove	
	Цр	
	Down	

18. Nella pagina Nome dominio e server DNS digitare il nome del dominio configurato in precedenza. Nell'esempio, utilizzare **Wireless.com**. Immettere l'indirizzo IP del server. Fare clic su

Add.

Domain Name and DNS Servers The Domain Name System (DNS) maps clients on your network.	and translates domain name:	s used by
You can specify the parent domain you want	the client computers on you	r network to use for
Parent do <u>m</u> ain: Wireless.com		
To configure scope clients to use DNS serve servers.	rs on your network, enter the	e IP addresses for thos
To configure scope clients to use DNS serve servers. <u>S</u> erver name:	rs on your network, enter the I <u>P</u> address:	e IP addresses for thos
To configure scope clients to use DNS serve servers. <u>S</u> erver name:	IP address:	e IP addresses for thos
To configure scope clients to use DNS serve servers. <u>S</u> erver name: R <u>e</u> solve	IP address:	e IP addresses for thos Add <u>Add</u>
To configure scope clients to use DNS serve servers. <u>S</u> erver name: R <u>e</u> solve	IP address:	e IP addresses for thos Add Bemove
To configure scope clients to use DNS serve servers. Server name: Resolve	IP address:	e IP addresses for thos Add Add Bemove Up Down

- 19. Fare clic su Next (Avanti).
- 20. Nella pagina Server WINS fare clic su Avanti.
- 21. Nella pagina Attiva ambito scegliere **Sì, attiva l'ambito adesso**, quindi fare clic su **Avanti**.

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

22. Al termine della Creazione guidata ambito, fare clic su **Fine**.



23. Nella finestra Snap-in DHCP verificare che l'ambito DHCP creato sia

ie Artien Ven Lafe) → Ro R × 17 C R R R R R R (040P 	toord: Septeministers cars [18,77,2462] Senterics of OHCP Server Senterics of OHCP Server	33/6		<u>.</u>
→ ★ ★ ★ ★ ★ ★ ★ ↓	Example dept existence come [10,77,204,27 Suntexts of DHCP Server Stoppe [172, 56,04] DHCP-Clerke	23		
2 (04:0) - [2] [State State in the second (10:0101444) (10) (8] [3] Scope [172, 16, 0.0] (04:07-Clerks - [3] Server Options	toweb-logitorieless cars [18,77,244,27 Sintests of CHCP Serve Scape [172,16,0.0] CHCP-Clerks	0] 396		
(a) Contraction (a) Charles (a	Cantents of DHCP Server	2.8.15		
	The second character and the second s	** Active **	Deception DHCP Server for Wireless Clients	
				[

Ora che il server DHCP/DNS è abilitato sul server, configurarlo come server Enterprise Certificate Authority (CA).

Installare e configurare il server Microsoft Windows 2003 come server CA

(Certification Authority)

PEAP con EAP-MS-CHAPv2 convalida il server RADIUS in base al certificato presente sul server. Il certificato server deve inoltre essere rilasciato da un'Autorità di certificazione (CA) pubblica considerata attendibile dal computer client, ovvero il certificato CA pubblico esiste già nella cartella Autorità di certificazione radice attendibile nell'archivio certificati del computer client. In questo esempio, configurare il server Microsoft Windows 2003 come autorità di certificazione (CA) che rilascia il certificato al servizio di autenticazione Internet (IAS).

Per installare e configurare i servizi certificati nel server, eseguire la procedura seguente:

- 1. Fare clic su Installazione applicazioni nel Pannello di controllo.
- 2. Fare clic su Aggiungi/Rimuovi componenti di Windows.
- 3. Fare clic su Servizi
 - certificati.

indows Components	8
You can add or remove components of Windows.	
To add or remove a component, click the checkbox. A sha part of the component will be installed. To see what's includ Details.	ded box means that only led in a component, click
Components:	
🛛 🗹 📻 Accessories and Utilities	4.9 MB 📥
🛛 🗹 🇃 Application Server	34.4 MB 💻
🗹 📴 Certificate Services	1.8 MB
🔲 🗔 📇 E-mail Services	1.1 MB
	7.9 MB 💻
Description: Installs a certification authority (CA) to issue ce public key security programs. Total disk space required: 13.8 MB	ertificates for use with
Space available on disk: 7310.6 MB	Details

4. Fare clic su Sì per visualizzare il messaggio di avviso Dopo l'installazione di Servizi certificati, non è possibile rinominare il computer né aggiungerlo o rimuoverlo da un dominio. Continuare?

Microsof	t Certificate Services	1
♪	After installing Certificate Services, the machine name and domain membership may not be changed due to the binding of the machine name to CA information stored in the Active Directory. Changing the machine name or domain membership would invalidate the certificates issued from the CA. Please ensure the proper machine name and domain membership are configured before installing Certificate Services. Do you want to continue?	
	<u>Yes</u> <u>No</u>	Contraction of the local division of the loc

5. In Tipo Autorità di certificazione scegliere **CA radice dell'organizzazione** e fare clic su **Avanti**.

CA Type Select the type of CA y	you want to set up.	Ē
Foterorise root CA		
C Enterprise subordina	ate CA	
C Stand-alone root CA	Δ.	
 Stand-alone subordi 	linate CA	
The most trusted CA i	in an enterprise. Should be installed before any other CA.	
Use custom settings	s to generate the key pair and CA certificate	
☐ <u>U</u> se custom settings	s to generate the key pair and CA certificate	

 Immettere un nome per identificare la CA. In questo esempio viene utilizzato Wireless-CA. Fare clic su Next (Avanti).

Common name for this C	Ά·			
 Wireless-CA				
, <u>D</u> istinguished name suff	x.			
DC=Wireless,DC=com				
Preview of distinguished	name:			
Preview of distinguished CN=Wireless-CA,DC=W	rame: /ireless,DC=com			
Preview of distinguished CN=Wireless-CA,DC=W	I name: /ireless,DC=com			
Preview of distinguished	I name: /ireless,DC=com	Expiration d	ate:	

 Viene creata una directory "Registro certificati" per l'archiviazione del database dei certificati. Fare clic su Next (Avanti).

uration
Br <u>o</u> wse
Browse
and the second
Browse
Browse
cel Help

8. Se IIS è attivato, è necessario arrestarlo prima di procedere. Fare clic su **OK** per visualizzare il messaggio di avviso che indica che IIS deve essere arrestato. Si riavvia automaticamente dopo l'installazione di



9. Fare clic su **Fine** per completare l'installazione dei servizi CA.



Il passaggio successivo consiste nell'installare e configurare il servizio di autenticazione Internet nel server Microsoft Windows 2003.

Connetti client al dominio

Il passaggio successivo consiste nel connettere i client alla rete cablata e scaricare le informazioni specifiche del dominio dal nuovo dominio. In altre parole, connettere i client al dominio. A tale scopo, effettuare le seguenti operazioni:

- 1. Collegare i client alla rete cablata con un cavo Ethernet straight-through.
- 2. Avviare il client ed eseguire il login con il nome utente e la password del client.
- 3. Fare clic su **Start**; fare clic su **Esegui**; digitare **cmd**; e fare clic su **OK**.
- 4. Al prompt dei comandi, digitare **ipconfig** e fare clic su **Enter** per verificare che DHCP funzioni correttamente e che il client abbia ricevuto un indirizzo IP dal server DHCP.
- 5. Per aggiungere il client al dominio, fare clic con il pulsante destro del mouse su **Risorse del computer**, quindi selezionare **Proprietà**.
- 6. Fare clic sulla scheda Nome computer.
- 7. Fare clic su Cambia.
- 8. Fare clic su Dominio; digitare wireless.com; e fare clic su
| Comp | uter Name Char | iges | | 1 |
|----------------|-------------------------------------------|-------------------------------|-------------------------|-----------------------|
| You c
compi | an change the name
uter. Changes may a | e and the me
iffect access | mbership (
to networ | of this
k resource |
| Comp | uter name: | | | |
| Client | 1 | | | |
| Men | nber of
Domain: | | (| More |
| | Wireless | | | |
| 0 | Workgroup: | | | |
| | WURKGROUP | | | |
| | | 0 | к 🚺 | Cance |
| | | | | |

9. Digitare **Username Administrator** e la password specifica del dominio a cui il client si unisce. Si tratta dell'account amministratore in Active Directory sul

Computer Nam	e Changes	?
Enter the name ar	od password of an account w	ith permission
to join the domain	h passivora or an account w	on permission
<u>U</u> ser name:	🖸 administrator	*
Password:		



- 10. Fare clic su OK.
- 11. Fare clic su Sì per riavviare il computer.
- 12. Una volta riavviato il computer, effettuare l'accesso con queste informazioni: Username = Administrator; Password = <domain password>; Domain = Wireless.
- 13. Fare clic con il pulsante destro del mouse su **Risorse del computer**, quindi scegliere **Proprietà**.
- 14. Fare clic sulla scheda **Nome computer** per verificare che ci si trovi nel dominio Wireless.com.

ystem Proper	ties			?
System Re:	store	Automa	tic Updates	Remote
General	Com	puter Name	Hardware	Advanced
Wind on th	dows use: ie networl	s the following inf k.	ormation to identify	your computer
Computer <u>d</u> esc	ription:			
		For example: "H Computer".	Kitchen Computer'' (or ''Mary's
Full computer n	ame:	Client1.Wireles	s.com	
Domain:		Wireless.com		
To use the Net domain and cre ID.	work Ider ate a loc	ntification Wizard al user account, i	to join a [click Network [Network ID
To rename this	compute	r or join a domain	, click Change. 🛛 🛛	Change
🔥 Changes	will take (effect after you re	start this computer.	
		OK	Cancel	Apply

15. Il passaggio successivo consiste nel verificare che il client abbia ricevuto il certificato CA (trust) dal server.

- 16. Fare clic su **Start**; fare clic su **Esegui**; digitare **mmc** e fare clic su **OK**.
- 17. Fare clic su File, quindi su Aggiungi/Rimuovi snap-

Use this page to add	d or remove a standalone Snap-in fr	om the console.
Snap-ins added to:	🔄 Console Root	
Description		
Description		
- Description		

- 18. Fare clic su Add.
- 19. Scegliere Certificato, quindi fare clic su

	A CONTRACTOR OF	-	
S 1 3 1 1 1	alono	Snan	100
			-

 NET Framework 1.1 Configuration ActiveX Control Certificates Component Services Computer Management Device Manager 	Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation
ActiveX Control	Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation
Certificates Component Services Computer Management Quevice Manager	Microsoft Corporation Microsoft Corporation Microsoft Corporation
Component Services Computer Management Lovice Manager	Microsoft Corporation Microsoft Corporation
Scomputer Management Boundary Device Manager	Microsoft Corporation
📃 💻 Device Manager	
	Microsoft Corporation
🛛 😻 Disk Defragmenter	Microsoft Corp, Executi
😸 Disk Management	Microsoft and VERITAS
🚺 Event Viewer	Microsoft Corporation
🔜 Folder	Microsoft Corporation
 Description The Certificates snap-in allows you to brocertificate stores for yourself, a service, or 	Microsoft Corporation owse the contents of the or a computer.

20. Scegliere Account computer, quindi fare clic su Avanti.

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

21. Fare clic su **Fine** per accettare il computer locale predefinito.

elect the computer you wa	ant this snap-in to manage.	
This snap-in will always m	anage:	
 Local computer: (the 	computer this console is running on)	
Another computer:		Browse
only applies if you sa	ve the console.	g nom the command line. This

22. Fare clic su **Close** (Chiudi), quindi su **OK**.

23. Espandere Certificati (computer locale), Autorità di certificazione radice attendibili e fare clic su Certificati. Trovare Wireless

nell'elenco.						
To Console1 - [Console Root/Certific	ates (Local Computer)\Trusted R	oot Certification Authorities/Cer	tificates]	A REAL PROPERTY AND A DESCRIPTION OF A D		5 🔀
🚡 File Action View Favorites Win	dow Help					_ dose
← → 🖻 🗷 🖄 🗶 🗗 🛱	3 😰					
Console Root	Issued To - /	Issued By	Espiration Date	Intended Purposes	Friendly Name	Stati 🔨
Console Root Console Console Root Console Console	Issued To // SERVICIOS DE CERTIFICACION SIA Secure Cient CA SIA Secure Cient CA SIA Secure Server CA Setsskey Root CA Setsskey Root CA Setsskey Root CA To TrustCenter Class 1 CA To TrustCenter Class 2 CA To TrustCenter Class 2 CA To TrustCenter Class 3 CA To TrustCenter Class 3 CA To TrustCenter Tine Stamping CA To TrustCenter Tine Stamping CA To TrustCenter Tine Stamping CA Thawke Personal Premium CA Thawke Timestamping CA Thawke Timestamping CA UTN-USERFirst-Nerdware UTN-USERFirst-Nerdware UTN-USERFirst-Nerdware To UTN-USERFirst-Nerdware To UTN-USERFirst-Object Set YeriSign Commercial Software Publ The YeriSign Trust Network Set YeriSign Trust Network	Essend by SERVICIOS DE CERTIFICACION - A SIA Secure Cierk CA Svisskey Root CA Svisskey Root CA Svisskey Root CA Svisskey Root CA TC TrustCenter Class 1 CA TC TrustCenter Class 2 CA TC TrustCenter Class 3 CA TC TrustCenter Class 3 CA TC TrustCenter Class 4 CA Thavite Personal Breenal CA Thavite Personal Prenium CA UTN - DATACorp SGC UTN-USERPirst-Network Applications UTN-USERPirst-Network Applications UTN-USERPirst-Network Applications VerSign Trust Network VerSign Trust Network	Expiration Date 3/10/2009 7/9/2019 1/1/2016 5/1/2011 1/1/2011 1/1/2011 1/1/2011 1/1/2011 1/1/2011 1/1/2011 1/1/2011 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021 1/1/2021	Intended Purposes Secure Ensil, Server Secure Ensil, Server Time Stamping Clerk Authentication Clerk Authentication Clerk Authentication Clerk Authentication Server Authentication Server Authentication Secure Ensil Server Authentication Secure Ensil Server Authentication Secure Ensil Server Authentication Secure Ensil, Code S Secure Ensil, Chert Secure Ensil, Chert	Friendy Name SERVICIOS DE CERT Societa Interbancari Societa Interbancari Societa Interbancari Seisskey Root CA chane> TC TrustCenter Clas TC TrustCenter Clas Theves Personal Bre Thavte Personal Bre Thavte Personal Pre Thavte Personal Pre Thavte Personal Pre Thavte Personal Pre Thavte Personal Pre Thavte Personal Pre UTN - USERPist-Net UTN - USERPist-Net UTN - USERPist-Net UTN - USERPist-Net UTN - USERPist-Net UTN - USERPist-Net VerlSign Connercial VerlSign Class 2 Prim VerlSign Class 3 Prim VerlSign Class 3 Prim VerlSign Class 1 Prim VerlSign Class 1 Prim VerlSign Class 1 Prim	Stati A
	WeriSign Trust Network	VeriSign Trust Network Wireless-CA	5/19/2018 L2/17/2010	Secure Email, Client	VeriSign Class 1 Prim 	
<u><</u>	Corrt EZ by DST	Xcert EZ by DST	7/11/2009	Secure Enal, Server	Xcert EZ by DST	> *
Trusted Root Certification Authorities store co	ntains 109 certificates.		Suddalanda Su	the state of the s	se in the first of the first	
🐉 Start 👔 🊡 Consolet - [Conso	4e		New Other Street	8 -3		2:42 PM

24. Ripetere questa procedura per aggiungere altri client al dominio.

Installare il servizio di autenticazione Internet nel server Microsoft Windows 2003 e richiedere un certificato

In questa configurazione, il servizio di autenticazione Internet (IAS, Internet Authentication Service) viene utilizzato come server RADIUS per autenticare i client wireless con l'autenticazione PEAP.

Completare la procedura seguente per installare e configurare IAS sul server.

- 1. Scegliere Installazione applicazioni nel Pannello di controllo.
- 2. Fare clic su Aggiungi/Rimuovi componenti di Windows.
- 3. Scegliere Servizi di rete, quindi fare clic su Dettagli.
- 4. Scegliere Servizio di autenticazione Internet; fare clic su OK; e fare clic su

Networking Services	×
To add or remove a component, click the check box. A shaded box me of the component will be installed. To see what's included in a compon	eans that only part ent, click Details.
Sub <u>c</u> omponents of Networking Services:	
🗹 畏 Domain Name System (DNS)	1.7 MB 🔺
🗹 🚑 Dynamic Host Configuration Protocol (DHCP)	0.0 MB
🗹 🖳 Internet Authentication Service	0.0 MB
🔲 🚚 Remote Access Quarantine Service	0.1 MB
RPC over HTTP Proxy	0.0 MB
Simple TCP/IP Services	0.0 MB 🥣
🔲 🚚 Windows Internet Name Service (WINS)	0.9 MB 🗾
Description: Enables authentication, authorization and accounting of users. IAS supports the RADIUS protocol.	dial-up and VPN
Total disk space required: 3.4 MB	Details
Space available on disk: 7208.2 MB	200000
OK	Cancel

5. Fare clic su **Fine** per completare l'installazione di IAS.

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

- 6. Il passaggio successivo consiste nell'installare il certificato del computer per il servizio di autenticazione Internet (IAS).
- 7. Fare clic su Start; fare clic su Esegui; digitare mmc; e fare clic su



- 8. Scegliere Console dal menu file, quindi Aggiungi/Rimuovi snap-in.
- 9. Fare clic su Aggiungi per aggiungere uno snap-

ld/Remove Snap-i	in			?
Standalone Extensi	ons			
Use this page to ad	d or remove a sta	and-alone snap	-in from the	console.
Snap-ins added to:	Console Ro	ot		
Description				
	4			
Add	Remove	A <u>b</u> out		

10. Scegliere Certificati dall'elenco degli snap-in e fare clic su

Snap-in	Vendor
📲 🍇 .NET Framework 1.1 Configuration	Microsoft Corporation
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Compu	Microsoft Corporation
🕺 🛍 ActiveX Control	Microsoft Corporation
🛛 🍕 ADSI Edit	Microsoft Corporation
🛛 🜆 Authorization Manager	Microsoft Corporation
Certificate Templates	Microsoft Corporation
Certificates	Microsoft Corporation
Example 2 Certification Authority	Microsoft Corporation
Description The Certificates snap-in allows you to bro certificate stores for yourself, a service,	owse the contents of the or a computer.

11. Scegliere Account computer e fare clic su Avanti.

Certificates snap-in		×
This open is will show a service partities too for		
This shapin will always manage certificates for.		
C <u>M</u> y user account		
C Service account		
Computer account		
	< <u>₿</u> ack <u>N</u> ext>	Cancel
1		

12. Scegliere **Computer locale**, quindi fare clic su

iter:			
			Blowse
	ted computer to be a ou save the console	ted computer to be changed when la ou save the console.	ted computer to be changed when launching from th ou save the console.

13. Fare clic su **Close** (Chiudi), quindi su **OK**.

14. Espandere **Certificati (computer locale)**; fare clic con il pulsante destro del mouse su **Cartella personale**; scegliere **Tutte le attività** e quindi **Richiedi nuovo**

Tormole 1 - [Convole Root]		্রারা স
🐒 Elle Action Yen Fangrites Window Help		<u>_16 ×1</u>
Canada Roat Conflictes David Computer) Conflictes David Computer) Conflictes David Computer) Conflictes Conflictes Computer) Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflictes Conflic	Certificates (Lacol Camputer)	
Start 6 Network Connections	A dramant - IDH2129400 Distance duther to alive	
Transfer and the second	A CHORE I CHORE &	A COMPANY AND A COMPANY

15. Fare clic su Avanti nella Richiesta guidata certificato



16. Scegliere il modello di certificato Controller di dominio (se si richiede un certificato computer

in un server diverso dal controller di dominio, scegliere un modello di certificato **computer**) e fare clic su

Avanti.

Certificate Request Wizard	×
Certificate Types A certificate type contains preset properties for certificates.	
Select a certificate type for your request. You can access only certificate types that you have permissions for and that are available from a trusted CA.	
Directory Email Replication Domain Controller Domain Controller Authentication	
To select a cryptographic service provider and a CA, select Advanced.	
< <u>B</u> ack <u>N</u> ext > Car	icel

17. Digitare un nome e una descrizione per il certificato.

rtificate Friendly Name and De	escription		
You can provide a name and o certificate.	description that help you o	quickly identify a spec	tific
Type a mendiy name and des	cription for the new certif	icate.	
Eriendly name:			
PEAP-Wireless			
· · · · ·			
IAS Server Certificate - 802.	1× Authentication		

18. Fare clic su **Fine** per completare la procedura guidata per la richiesta di certificazione.



Configurare il servizio di autenticazione Internet per l'autenticazione PEAP-MS-CHAP v2

Dopo aver installato e richiesto un certificato per IAS, configurare IAS per l'autenticazione.

Attenersi alla seguente procedura:

- 1. Fare clic su **Start > Programmi > Strumenti di amministrazione**, quindi fare clic su Snap-in **Servizio di autenticazione Internet**.
- Fare clic con il pulsante destro del mouse su Servizio di autenticazione Internet (IAS) e quindi scegliere Registra servizio in Active Directory.

🞾 Internet Authentication Ser	wine and the second	
Elle girtion Yeve Help		
* > [] 2 2 0	• •	
Internet Authentication Service Brain RADIUS Clerits	Sat Service	ree to Internet Authentication Service
Remote Access Cogging Remote Access Policies Remote Access Policies Remote Access Policies	Register Server in Addive Directory	theritication Service (LKS) to autheriticate, authorize, and account for dai-up, VMA, wireless and Ditement connections to your network. You can also configure LKS to forward equants to any access server that is compatible with Remote Authentication Dial in User Service (RADUS).
	Pyperties	5 to read the remote access properties of user accounts in Active Directory, on the Action menu, click Register Server in Active Directory.
	H-b	atian about setting up 145, deployment scenarios, and troubleshooting, see Help.
Register Server in Active Deectory		A dependent (1982) 15400.
	and the set of the set	A

3. Verrà visualizzata la finestra di dialogo **Registra servizio di autenticazione Internet in Active Directory**. Fare clic su **OK**. In questo modo IAS è in grado di autenticare gli utenti in Active Directory.

Register Internet Authentication Server in Active Directory:	×
To enable IAS to authenticate users in the Active Directory, the computers running IAS must be au	thorized to read users' dial-in properties from the domain.
Do you wish to authorize this computer to read users' dial-in properties from the Wireless, com dom	nain?
OK Cancel	

4. Fate clic su OK nella finestra di dialogo

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

- 5. Aggiungere il controller LAN wireless come client AAA sul server MS IAS.
- 6. Fare clic con il pulsante destro del mouse su **Client RADIUS**, quindi scegliere **Nuovo client RADIUS**.

🖓 Internet Authentication Service				
Elle &ction Yerri Help				
+ → <u>1</u> [] [] [] [] [] [] []				
Image: Part of the second s	Maree Connections to Morosoft Routing and Reente	Order 1 2		
New Clent			ſ	
🐮 Start 💋 😢 Network Connections	PDHCP Anonget	[DHS]75WED P Internet Authenticati		🛯 🕄 🛢 🗟 🎒 🔩 🏹 7.13PM

7. Digitare il nome del client (in questo caso WLC) e immettere l'indirizzo IP del WLC. Fare clic su **Next**

(Avanti).

RADIUS Client		
Type a friendly name and	either an IP Address or DNS	name for the client.
Eriendly name:	WLC	
Client address (IP or DNS	3):	
10.77.244.210		⊻erify
	< <u>B</u> ac	k <u>N</u> ext> Cancel

8. Nella pagina successiva, in Client-Vendor, scegliere **RADIUS Standard**, immettere il segreto condiviso e fare clic su **Fine**.

9. Notare che il WLC viene aggiunto come client AAA sullo IAS.

A Internet Authentication Service			100000 - CT - C - C		
File Action View Hello					Cos
Internet detheritication Service Local	Directo Name /	- Zéhana	Destand	Cheret Vanada	
Connection Request Processing	₩ wLC	10.77.244.210	RADUS	Rabitis Sandard	
nadis leurscool	Libera	[***		1. And and a second sec	

- 10. Creare un criterio di accesso remoto per i client.
- 11. A tale scopo, fare clic con il pulsante destro del mouse su **Criteri di accesso remoto** e scegliere **Nuovi criteri di accesso**

	remoto.				
	🐓 Internet Authenti	cation Service			
	Elle girtion Yern	HMP			
Image: Automatical and a construction Image: Automatical and Automatical A	◆ → 🗈 🗉 (B 🛛 🕄 🖬			
🐉 Bant 🖉 🚫 Network Consections 🔯 Disco	Ball UE UE UE UE UE UE UE UE	La Bai Los Los Logang Logang Meri Remote Access Boley Servi • Servi • Servi • Servi • Servi • Expert Los · Ethol	More Connections to Microsoft Routing and Remote	Order 1 2	
	🐮 Start 🛛 🔏	Network Connections	Die Aternet	- [DN2]15/4D Poternet Authorite att.	

 Digitare un nome per il criterio di accesso remoto. Nell'esempio, utilizzare il nome PEAP. Quindi fare clic su Avanti.

ew Remote Acce	ss Policy Wizard
Policy Configu The wizard o	ration Method an create a typical policy, or you can create a custom policy.
How do you v	vant to set up this policy?
	e wizard to set up a typical policy for a common scenario
O Set up	a custom policy
Policy name:	PEAP-Wireless
	Example: Authenticate all VPN connections.
	< <u>B</u> ack <u>N</u> ext> Cancel

13. Scegliere gli attributi dei criteri in base alle proprie esigenze. In questo esempio, scegliere **Wireless**.

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

14. Nella pagina successiva scegliere **Utente** per applicare il criterio di accesso remoto all'elenco di utenti.

w Remote Access Policy Wizard	j
User or Group Access You can grant access to individual users, or you can grant access to sele groups.	ected
Grant access based on the following: User User access permissions are specified in the user account	
 <u>Group</u> Individual user permissions override group permissions. Group name: 	Add
	<u>R</u> emove
< <u>B</u> ack <u>N</u> ext>	Cancel

15. In Metodi di autenticazione scegliere PEAP (Protected EAP), quindi fare clic su Configura.

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

16. Nella pagina **Proprietà PEAP**, scegliere il certificato appropriato dal menu a discesa Certificato emesso e fare clic su

rotected EAP Prop	erties			1
This server identifies Select the certificate	itself to ca that you v	allers before the conr want it to use as proc	nection is comp of of identity.	leted.
Certificate issued		web-lapt.Wireless.co	m	
Friendly name:	PE/	AP-Wireless		
Issuer:	Wir	reless-CA		
Expiration date:	12/	/16/2008 5:53:02 PM	I	
🔲 Enable Fast Reco	nnect			
E <u>a</u> p Types				
Secured password (B	EAP-MSCH	AP v2)		Move Up
				Move Dow
Add	<u>E</u> dit	Remove	ОК	Cancel

17. Verificare i dettagli dei criteri di accesso remoto e fare clic su **Fine**.

New Remote Access Policy Wizard



X

18. I criteri di accesso remoto sono stati aggiunti all'elenco.



19. Fare clic con il pulsante destro del mouse sul criterio e quindi scegliere **Proprietà**. Scegliere "Concedi autorizzazione di accesso remoto" in "Se una richiesta di connessione soddisfa le condizioni

PEAP Properties				? ×
Settings				
Specify the con	ditions that connect	ion requests	must match.	
Policy condition	r.			
NAS-Port-Type	matches "Wireless	- Other OR \	Wireless - IEEE	802.11"
•				b
A <u>d</u> d	<u>E</u> dit	<u>R</u> emove		
If connection re	quests match the co	onditions spe	cified in this po on	olicy, the
	e mili be applied (o i	ine connect	011.	
Edit Profile				
Unless individua policy controls a	l access permission ccess to the netwo	s are specifi k.	ed in the user (profile, this
If a connection	equest matches the	specified o	onditions:	
C Deny remote	access permission	/ specified C	onations.	
Grant remote	access permission			
	(ок I	Cancel	Apply

Aggiungi utenti ad Active Directory

In questa configurazione, il database degli utenti viene gestito in Active Directory.

Per aggiungere utenti al database di Active Directory, attenersi alla seguente procedura:

 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**

<u>F</u> irst name:	Client 1		Initials:	
Last name:				
Full name:	Client 1			
User logon name	e			
Client1	-	@Wireless	com	•
User logon name	e (pre- <u>W</u> indows)	2000):		

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

D	L	
Password:	•••••	
<u>C</u> onfirm password:	•••••	
User <u>m</u> ust change p	assword at next logon	
User cannot change	password	
Pass <u>w</u> ord never exp	ires	
Account is disabled		

Avanti.

4. Nella finestra di dialogo Nuovo oggetto - Utente fare clic su

w Object ·	- User					
9	Create in:	Wireless.)	com/Users			
When you	ı click Finish,	, the followi	ng object will	be created:		
Full name	: Client 1					
User logo	n name: Clie	nt1@Wirele	ess.com			
1						
			< <u>B</u> ack	. Finish	Ca	nc

5. Ripetere i passaggi da 2 a 4 per creare altri account utente.

Consenti accesso wireless agli utenti

Attenersi alla seguente procedura:

- Nell'albero della console Utenti e computer di Active Directory fare clic sulla cartella Utenti, fare clic con il pulsante destro del mouse su WirelessUser, scegliere Proprietà e quindi passare alla scheda Connessione remota.
- 2. Scegliere Consenti accesso, quindi fare clic su

Remote control Termina General Address Account F Member Of Dial-in	al Services Profile COM+ Profile Telephones Organizat Environment Sessions
ا Remote Access Permission (Dial-in c	r VPN)
Allow access	
© Deny access	
C Control access through Remote /	Access <u>Policy</u>
Verify Caller-ID:	
- Callback Options)
No <u>C</u> allback	
© Set by Caller (Routing and Remo	te Access Service only)
C Always Callback to:	
C Assign a Static IP Address	
Apply Static <u>B</u> outes	,
Define routes to enable for this Dial	-in Static Roytes
connection.	

Configurazione del controller LAN wireless e dei Lightweight Access Point

Configurare ora le periferiche wireless per questa installazione. tra cui la configurazione dei Wireless LAN Controller, dei Lightweight Access Point e dei client wireless.

Configurare il WLC per l'autenticazione RADIUS tramite il server MS IAS RADIUS

Configurare innanzitutto il WLC in modo che utilizzi MS IAS come server di autenticazione. Per inoltrare le credenziali dell'utente a un server RADIUS esterno, è necessario configurare il WLC. Il server RADIUS esterno convalida quindi le credenziali dell'utente e fornisce l'accesso ai client wireless. A tale scopo, aggiungere il server MS IAS come server RADIUS nella pagina **Sicurezza > Autenticazione RADIUS**.

Attenersi alla seguente procedura:

 Scegliere Sicurezza e Autenticazione RADIUS dall'interfaccia utente del controller per visualizzare la pagina Server di autenticazione RADIUS. Per definire un server RADIUS, fare clic su New (Nuovo)

	A 2 + A 3.3.						a - ह ×
CISCO SPOTENS	<u></u>				Save Co	infiguration Ping	Logout Refresh
A.	MONITOR WLANS CONT	ROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	****
Security	RADIUS Authentication S	ervers > New				< Back	Apply
AAA General	Server Index (Priority)	1 ~					
RADIUS Authentication RADIUS Accounting	Server IPAddress	10.77.244.198					
MAC Filtering Disabled Clients	Shared Secret Format	ASCII 💌					
User Login Policies AP Policies	Shared Secret	•••••]	
Access Control Lists	Confirm Shared					1	
IPSec Certificates	Secret					1	
ID Certificate	Key Wrap						
Web Auth Certificate		_					
Wireless Protection Policies	Port Number	1812					
Trusted AP Policies Rogue Policies	Server Status	Enabled 💌					
Custom Signatures Client Exclusion Policies	Support for RFC 3576	Enabled 💌					
AP Authentication	Retransmit Timeout	2 seconds					
	Network User	Enable					
	Management	Enable					
	IPSec	🖸 Enable					

 Definire i parametri del server RADIUS nella pagina Server di autenticazione RADIUS > Nuovo. Questi parametri includono l'indirizzo IP, il segreto condiviso, il numero di porta e lo stato del server RADIUS. Le caselle di controllo Utente di rete e Gestione consentono di determinare se l'autenticazione basata su RADIUS è valida per gli utenti di rete e di gestione. In questo esempio viene utilizzato MS IAS come server RADIUS con indirizzo IP 10.77.244.198.

3 · 0 · 🗈 🖻	6 P + 0	🔊 - 🛃 📼	-33					N - 8 >
Cisco Sestems	MONITOR WLAN		WIRELESS	ECURITY	MANAGEMENT C	Save Configurat	ion Ping Logi	ut Refrest
Security	RADIUS Authenti	ication Servers					Apply Net	F
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies	Call Station ID T Credentials Cacl Use AES Key Wra	ype IP Address	V					
AP Poices	Network Manage User	ment Server Index	Server Address	Port	IPSec	Admin Statu	6	
IPSec Certificates CA Certificate ID Certificate Web Auth Certificate Wireless Protection Policies Trusted AP Policies Regue Policies Standard Signatures Custom Signatures Client Exclusion Policies AP Authentication] 1	10.77.244.198	1812	Disabled	Enabled	Edit Remov	E Pina

- 3. Fare clic su **Apply** (Applica).
- 4. Il server MS IAS è stato aggiunto al WLC come server Radius e può essere utilizzato per autenticare i client wireless.

Configurazione di una WLAN per i client

Configurare il SSID (WLAN) a cui si connettono i client wireless. In questo esempio, creare il SSID e denominarlo **PEAP**.

Definire l'autenticazione di layer 2 come WPA2 in modo che i client eseguano l'autenticazione basata su EAP (PEAP-MSCHAPv2 in questo caso) e utilizzino AES come meccanismo di crittografia. Mantenere tutti gli altri valori ai valori predefiniti.

Nota: questo documento associa la WLAN alle interfacce di gestione. Se la rete contiene più VLAN, è possibile creare una VLAN separata e associarla all'SSID. Per informazioni su come configurare le VLAN sui WLC, fare riferimento all'<u>esempio di configurazione delle VLAN sui controller LAN wireless</u>.

Per configurare una WLAN sul WLC, attenersi alla seguente procedura:

- 1. Fare clic su **WLAN** dall'interfaccia utente del controller per visualizzare la pagina WLAN. In questa pagina vengono elencate le WLAN esistenti sul controller.
- Per creare una nuova WLAN, selezionare New (Nuovo). Immettere l'ID WLAN e l'SSID WLAN per la WLAN, quindi fare clic su Applica.

3 · 0 · 🗈 🖻	6 P 🛧 🛛 🝰	- 🕹 🖂 🐴				🦓 - 8 ×
Cisco Sestens				Save C	onfiguration Ping	Logout Refresh
Andrea	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEME	NT COMMANDS	HELP	
WLANS	WLANs > New				< Back	Apply
WLANS WLANS	WLAN ID	1 🛩	1			
AP Groups VLAN	WLAN SSID	PEAP				

 Dopo aver creato una nuova WLAN, viene visualizzata la pagina WLAN > Modifica per la nuova WLAN. In questa pagina è possibile definire vari parametri specifici per la WLAN, tra cui Criteri generali, Server RADIUS, Criteri di sicurezza e Parametri 802.1x.

002.17.						
Cinco Svarums				Save Co	nfiguration Ping	Logout Refre
dry dry	MONITOR WLANS C	ONTROLLER WIRELESS	SECURITY MANAG	EMENT COMMANDS	HELP	
WLANs	WLANs > Edit				< Back	Apply
WLANS	WLAN ID	1				
AP Groups VLAN	Profile Name	PEAP				
	WLAN SSID	PEAP				
	General Policies			Security Polici	es	
	Radio Policy	All		1Pv6 Enable		
	Admin Status	C Enabled				
	Session Timeout (secs)	0		Layer 2 Securit	WPA1+WP	A2 💌
	Quality of Service (QoS)	Silver (best effort)			MAC File	sning
	WMM Policy	Disabled 💌		Laver 3 Securit	None	
	7920 Phone Support	Client CAC Limit CAP	CAC Limit		Web Poli	CY *
	Broadcast SSID	Enabled				
	Aironet IE	Enabled				
	Allow AAA Override	Enabled		* Web Policy ca IPsec.	annot be used in cor	nbination with
	Client Exclusion	Enabled ** 60		** When client	autorios is apable.	d a time of
	DHCP Server	Timeout V	alue (secs)	value of zero m administrative	neans infinity(will re override to reset ex	quire cluded clients)
	DHCP Addr. Assignment	Required		CKIP is not	t supported by 10xx	: APS
	Interface Name	management 💌				
	MFP Version Required	1				
	MFP Signature Generation	Global MFP Disabled)				
	H-REAP Local Switching					
	* H-REAP Local Switchin authentications.	g not supported with IPSEC,	CRANITE and FORTRES	s		

- 4. Per abilitare la WLAN, controllare **lo stato dell'amministratore** in Criteri generali. Se si desidera che l'access point trasmetta l'SSID nei frame del beacon, selezionare **Broadcast SSID**.
- 5. In Protezione di livello 2, scegliere WPA1+WPA2. Ciò abilita WPA sulla WLAN. Scorrere la pagina verso il basso e scegliere il criterio WPA. In questo esempio viene utilizzata la crittografia WPA2 e AES. Scegliere il server RADIUS appropriato dal menu a discesa in Server RADIUS. Nell'esempio, utilizzare 10.77.244.198 (indirizzo IP del server MS IAS). Gli altri parametri possono essere modificati in base ai requisiti della rete MILAN.

Cinco Statum				Save C	onfiguration Ping Logout Refresh
dr. dr.	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS	HELP
WLANs	WPA1+WPA2 Parameters		_		2
WLANS WLANS	WPA1 Policy WPA2 Policy	R			
AP Groups VLAN	WPA2 Encryption	AES TKIP			
	Auth Key Mgmt	802.1× ¥			

6. Fare clic su Apply

WLANS	WLANS						1
WLANS WLANS AP Groups VLAN	Profile Name	WLAN ID	WLAN SSID	Admin Status	Security Policies		
	PEAP	1	PEAP	Enabled	[WPA2][Auth(802.1x)]	Edit	Ren
	* WLAN IDs 9-16 will not be	e pushed to 1130,1	1200 and 1240 AP models.				

Configurazione dei client wireless

Configurazione dei client wireless per l'autenticazione PEAP-MS CHAPv2

In questo esempio vengono fornite informazioni su come configurare il client wireless con Cisco Aironet Desktop Utility. Prima di configurare l'adattatore client, verificare che sia utilizzata la versione più recente del firmware e dell'utility. La versione più recente del firmware e delle utility è disponibile nella pagina dei download wireless all'indirizzo Cisco.com.

Per configurare la scheda client wireless Cisco Aironet 802.11 a/b/g con l'ADU, attenersi alla seguente procedura:

- 1. Aprire Aironet Desktop Utility.
- 2. Fare clic su Gestione profili, quindi su Nuovo per definire un profilo.
- Nella scheda Generale, immettere il nome del profilo e il SSID. Nell'esempio, utilizzare il SSID configurato sul WLC (PEAP).

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

4. Selezionare la scheda Protezione, scegliere **WPA/WPA2/CCKM**, in WPA/WPA2/CCKM EAP digitare choose **PEAP [EAP-MSCHAPv2]**, quindi fare clic su **Configura**.

Prof	ile Management		? 🗙
Ger	neral Security Advanced		
	Set Security Options		
	⊙ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type: FEAP (EAP-MSCHAP V2)	
	O WPA/WPA2 Passphrase		
	O 802.1x	802.1x EAP Type: EAP FAST	
	O Pre-Shared Key (Static WEP)		
	O None		
	Configure	Allow Association to Mixed Cells Profile Locked	
		Limit Time for Finding Domain Controller To: 0 Sec	
	Group Policy Delay:	60 📚 sec	
		ОК С	ancel

5. Scegliere **Convalida certificato server**, quindi **Wireless-CA** dal menu a discesa Autorità di certificazione fonti

Use Machine Information fr	or Domain Logon
Validate Server Identity	
Trusted Root Certification Auth	norities
Wireless-CA	
When connecting, use:	
Certificate	
 User Name and Password 	d
Select a Certificate	
	10
Use Windows User Name	; and Password (EAR-MSCHAR V2) Authentication
User Name	Administrator
Password	
Password	

6. Fare clic su OK e attivare il profilo.Nota: quando si utilizza PEAP-MSCHAPv2 (Protected EAP-Microsoft Challenge Handshake Authentication Protocol versione 2) con Microsoft XP SP2 e la scheda wireless è gestita da Microsoft Wireless Zero Configuration (WZC), è necessario applicare l'hotfix KB885453 di Microsoft. In questo modo si evitano diversi problemi di autenticazione relativi alla funzionalità di ripristino rapido di PEAP.

Verifica e risoluzione dei problemi

Per verificare se la configurazione funziona come previsto, attivare il profilo PEAP-MSCHAPv2 sul client wireless Client1.

😨 Cisco Aironet Desktop Utility	y - Current Profile: PEAP-MS	ichapv2 🛛 🛛 🔀
Action Options Help		
Current Status Profile Management	Diagnostics	
CISCO SYSTEMS		
Profile Name:	PEAP-MSCHAPv2	
Link Status:	Authenticated	Network Type: Infrastructure
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 64
Server Based Authentication:	PEAP (EAP-MSCHAP V2)	Data Encryption: AES
IP Address:	10.77.244.218	
Signal Strength:		
		Advanced

Una volta attivato il profilo PEAP-MSCHAPv2 sull'ADU, il client esegue l'autenticazione 802.11 open e quindi l'autenticazione PEAP-MSCHAPv2. Di seguito è riportato un esempio di autenticazione PEAP-MSCHAPv2 riuscita.

Utilizzare i comandi di debug per comprendere la sequenza di eventi che si verificano.

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Questi comandi di debug sul controller LAN wireless sono utili.

- debug dot1x events enable: per configurare il debug degli eventi 802.1x
- debug aaa events enable: per configurare il debug degli eventi AAA
- debug mac addr <indirizzo mac> Per configurare il debug MAC, usare il comando debug mac
- debug dhcp message enable: per configurare il debug dei messaggi di errore DHCP

Di seguito vengono riportati gli output di esempio dei comandi **debug dot1x events enable** e **debug client <indirizzo mac>**.

debug dot1x events enable:

Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 2) Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity Response (count=2) from mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 6, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 7) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 7, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 8) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 8, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 9) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 12) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 12, EAP Type 25) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Accept for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP-Success to

mobile 00:40:96:ac:e6:57 (EAP Id 13) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending default RC4 key to mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received Auth Success while in Authenticating state for mobile 00:40:96:ac:e6:57

debug mac addr <Indirizzo MAC>:

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

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

```
on AP 00:0b:85:51:5a:e0, slot 0, interface = 2
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
Card = 0 (slot 0), InHandle = 0x0000000,
OutHandle = 0x00000000, npuCryptoFlag = 0x0000
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Successfully plumbed mobile rule (ACL ID 255)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Reached RETURN: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend
Auth Success state (id=12) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received Auth Success
while in Authenticating state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x -
moving mobile 00:40:96:ac:e6:57 into Authenticated state
```

Nota: se si utilizza il supplicant Microsoft per autenticarsi con un Cisco Secure ACS per l'autenticazione PEAP, il client potrebbe non eseguire l'autenticazione correttamente. A volte la connessione iniziale può essere autenticata correttamente, ma i successivi tentativi di autenticazione con connessione rapida non riescono a connettersi. Si tratta di un problema noto. I dettagli di questo problema e la soluzione corrispondente sono disponibili <u>qui</u>.

Informazioni correlate

- PEAP in Unified Wireless Networks con ACS 4.0 e Windows 2003
- Esempio di configurazione dell'autenticazione EAP con i controller WLAN (WLC)
- Aggiornamento del software Wireless LAN Controller (WLC) alle versioni 3.2, 4.0 e 4.1
- Guide alla configurazione di Cisco Wireless LAN Controller serie 4400
- 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).