Esempio di autenticazione EAP locale sul controller LAN wireless con EAP-FAST e configurazione del server LDAP

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Premesse Configurazione Esempio di rete Configurazioni Configurazione di EAP-FAST come metodo di autenticazione EAP locale sul WLC Genera un certificato dispositivo per il WLC Download del certificato del dispositivo sul WLC Installare il certificato radice di PKI nel WLC Genera un certificato dispositivo per il client Genera il certificato CA radice per il client Configurazione di EAP locale sul WLC Configura server LDAP Creazione di utenti nel controller di dominio Configurare l'utente per l'accesso LDAP Utilizzo di LDP per identificare gli attributi utente Configura client wireless Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

Questo documento spiega come configurare EAP (Extensible Authentication Protocol) -Autenticazione flessibile tramite FAST (Secure Tunneling) Autenticazione EAP locale su un controller WLC. In questo documento viene inoltre spiegato come configurare il server LDAP (Lightweight Directory Access Protocol) come database back-end per il protocollo EAP locale in modo da recuperare le credenziali dell'utente e autenticarlo.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Cisco serie 4400 WLC con firmware 4.2
- Cisco Aironet serie 1232AG Lightweight Access Point (LAP)
- Server Microsoft Windows 2003 configurato come controller di dominio, server LDAP e server Autorità di certificazione.
- Cisco Aironet 802.11 a/b/g Client Adapter con firmware versione 4.2
- Cisco Aironet Desktop Utility (ADU) con firmware versione 4.2

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>

Premesse

L'autenticazione EAP locale sui controller LAN wireless è stata introdotta con Wireless LAN Controller versione 4.1.171.0.

EAP locale è un metodo di autenticazione che consente agli utenti e ai client wireless di essere autenticati localmente sul controller. È progettato per l'utilizzo in uffici remoti che desiderano mantenere la connettività ai client wireless quando il sistema back-end viene interrotto o il server di autenticazione esterno si blocca. Quando si abilita il protocollo EAP locale, il controller funge da server di autenticazione e da database degli utenti locali, pertanto rimuove la dipendenza da un server di autenticazione esterno. EAP locale recupera le credenziali utente dal database degli utenti locale o dal database backend LDAP per autenticare gli utenti. Local EAP supporta l'autenticazione LEAP, EAP-FAST, EAP-TLS, P EAPv0/MSCHAPv2 e PEAPv1/GTC tra il controller e i client wireless.

EAP locale può utilizzare un server LDAP come database backend per recuperare le credenziali utente.

Un database backend LDAP consente al controller di eseguire una query su un server LDAP per ottenere le credenziali (nome utente e password) di un utente specifico. Queste credenziali vengono quindi utilizzate per autenticare l'utente.

II database backend LDAP supporta i seguenti metodi EAP locali:

• EAP-FAST/GTC

- EAP-TLS
- PEAPv1/GTC.

Sono supportati anche LEAP, EAP-FAST/MSCHAPv2 e PEAPv0/MSCHAPv2, **ma solo se il server LDAP è configurato per restituire una password non crittografata**. Microsoft Active Directory, ad esempio, non è supportato perché non restituisce una password non crittografata. Se non è possibile configurare il server LDAP in modo che restituisca una password non crittografata, i protocolli LEAP, EAP-FAST/MSCHAPv2 e PEAPv0/MSCHAPv2 non sono supportati.

Nota: se sul controller sono configurati server RADIUS, il controller tenta di autenticare prima i client wireless utilizzando i server RADIUS. Il tentativo di eseguire EAP locale viene eseguito solo se non vengono trovati server RADIUS, a causa del timeout dei server RADIUS o della mancata configurazione di server RADIUS. Se sono configurati quattro server RADIUS, il controller tenta di autenticare il client con il primo server RADIUS, quindi con il secondo server RADIUS e infine con l'EAP locale. Se il client tenta di eseguire nuovamente l'autenticazione manualmente, il controller tenta di eseguire il terzo server RADIUS, quindi il quarto server RADIUS e infine l'EAP locale.

In questo esempio viene utilizzato EAP-FAST come metodo EAP locale sul WLC, che a sua volta è configurato per eseguire una query sul database backend LDAP per ottenere le credenziali utente di un client wireless.

Configurazione

In questo documento viene usato EAP-FAST con certificati sia sul lato client che sul lato server. A tale scopo, il programma di installazione utilizza il server **Microsoft Certificate Authority (CA)** per generare i certificati client e server.

Le credenziali utente vengono archiviate nel server LDAP in modo che, dopo la convalida del certificato, il controller interroghi il server LDAP per recuperare le credenziali utente e autentichi il client wireless.

In questo documento si presume che queste configurazioni siano già presenti:

- Un LAP è registrato sul WLC. Per ulteriori informazioni sul processo di registrazione, fare riferimento a <u>Registrazione di un Lightweight AP (LAP) su un Wireless LAN Controller (WLC)</u>.
- Un server DHCP è configurato per assegnare un indirizzo IP ai client wireless.
- Il server Microsoft Windows 2003 è configurato sia come controller di dominio che come server CA. In questo esempio viene utilizzato wireless.com come dominio.Per ulteriori informazioni sulla configurazione di un server Windows 2003 come controller di dominio, fare riferimento a <u>Configurazione di Windows 2003 come controller di dominio</u>.Per configurare il server Windows 2003 come server CA dell'organizzazione, consultare il documento sull'installazione e configurazione di Microsoft Windows 2003 Server come server CA dell'organizzazione (Enterprise).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Per implementare questa configurazione, completare i seguenti passaggi:

- Configurazione di EAP-FAST come metodo di autenticazione EAP locale sul WLC
- <u>Configura server LDAP</u>
- <u>Configura client wireless</u>

Configurazione di EAP-FAST come metodo di autenticazione EAP locale sul WLC

Come accennato in precedenza, in questo documento viene utilizzato il metodo di autenticazione EAP-FAST con certificati sia sul lato client che sul lato server. Il primo passaggio consiste nel scaricare e installare i certificati seguenti nel server (in questo caso WLC) e nel client.

Il WLC e il client necessitano entrambi di questi certificati per essere scaricati dal server CA:

- Certificato dispositivo (uno per il WLC e uno per il client)
- Certificato radice dell'infrastruttura a chiave pubblica (PKI) per il WLC e certificato CA per il client

Genera un certificato dispositivo per il WLC

Eseguire questa procedura per generare un certificato del dispositivo per il WLC dal server CA. Questo certificato di dispositivo viene utilizzato dal WLC per l'autenticazione al client.

1. Visitare il sito Web all'indirizzo **http://<indirizzo IP del server CA>/certsrv** dal PC che dispone di una connessione di rete al server CA. Accedere come amministratore del server



2. Selezionare **Richiedi** certificato.

| Microsoft Certificate Services - Microsoft Internet Explorer | |
|---|--|
| Ple, Edt. Yen Pavortis' Took ' Help | 4 |
| d3mm @ http://10.77.244.190/certaru/ | 🛩 🄁 Go |
| Afficrosoft Certificate Services wireless | Home |
| Welcome | |
| Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, dentity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of perform other security tasks. | you can verify your entificate you request, |
| You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revoc few the status of a pending request. | ation list (CRL), or to |
| For more information about Certificate Services, see Certificate Services Documentation. | |
| Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL | |
| | |
| | |

3. Nella pagina Richiedi un certificato fare clic su Richiesta avanzata di

| certificati. | |
|--|----------|
| Microsoft Certificate Services - Microsoft Internet Explorer | |
| File Edit View Pavorities' Tools Help | A |
| Address all http://10.77.244.198/certsrv/certraus.asp | 😒 🔁 Go |
| | |
| Microsoft Certificate Services wireless | Home |
| Request a Certificate | |
| Select the certificate type: | |
| User Cartificate | |
| | |
| On submit an advanced certificate request. | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | <u>e</u> |
| http://10.77.244.198/certsrv/certrgad.asp | Internet |

 Nella pagina Richiesta avanzata di certificati fare clic su Crea e invia una richiesta a questa CA. Verrà visualizzato il modulo di richiesta avanzata dei certificati.

| Microsoft Certificate Services - Microsoft Internet Explorer | |
|--|--|
| e Edit View Pavorites Tools Help | |
| iress 🕘 Mtp://10.77.244.198/certsrv/certrgad.asp | Z ➡ |
| ficrosoft Certificate Services witeless | Home |
| dvanced Certificate Request | |
| e policy of the CA determines the types of certificates you can request. Click one of the f | lowing options to: |
| Create and submit a request to this CA. | |
| Submit a certificate request by using a base 64-encoded CMC or PKCS #10 file, or sul PKCS #7 file. | nit a renewal request by using a base-64-encoded |
| Request a certificate for a smart card on behalf of another user by using the smart card on Note: You must have an enrollment agent certificate to submit a request on behalf of another user. | rtificate enrolment station, |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | Internet |

- 5. Nel modulo di richiesta avanzata del certificato scegliere Server Web come modello di certificato. Specificare quindi un nome per il certificato del dispositivo. In questo esempio viene utilizzato il nome del certificato ciscowlc123. Compilare le altre informazioni di identificazione in base alle proprie esigenze.
- 6. Nella sezione Opzioni chiave selezionare l'opzione Contrassegna chiavi come esportabili. A volte questa opzione è disattivata e non può essere attivata o disattivata se si sceglie un modello di server Web. In questi casi, scegliere Indietro dal menu del browser per tornare indietro di una pagina e tornare nuovamente a questa pagina. Questa volta dovrebbe essere disponibile l'opzione Contrassegna le chiavi come esportabili.

| esponabili. | |
|---|----------|
| 🗃 Microsoft Certificate Services - Microsoft Internet Explorer | |
| Pile Edt View Pavoritek Tools Help | |
| Q bak · Q · e & Pranth of Parentes @ 2. 3 2 3 | |
| 2003ess () http://10.77.244.198/cartiarv/certrigna.asp | 💌 🔁 GO |
| | |
| Alcrosoft Centrate Benness Miletexs | Heme |
| Advanced Certificate Request | |
| | |
| Certificate Template: | |
| Web Server 💌 | |
| Identifying Information For Offline Template: | |
| Name: ciscowic123 | |
| 15-Mail | |
| Company risco | |
| Department | |
| | |
| City: | |
| State | |
| Countryviewgion: | |
| Key Options: | |
| Create new key set Ouse existing key set | |
| CSP: Microsoft RSA SChannel Cryptographic Provider 🛩 | |
| Key Usage: (*) Exchange | |
| Key Size: 1024 Max 1004 (common key sizer 512 1024 2006 4090 6192 10264.) | |
| Automatic key container name O User specified key container name | |
| Imark keys as exportable | |
| Export keys to file | |
| Enable strong private key protection | |
| Store certificate in the local computer certificate store | |
| Done | Internet |

7. Configurare tutti gli altri campi necessari e fare clic su **Invia**.

| Alicrosoft Certificate Services - Microsoft Internet Explorer | |
|---|----------|
| File Edit View Pavorites Tools Help | |
| 🔇 Back + 🕥 - 🖹 📓 🐔 🔑 Search 🦅 Pavortes 🤣 🔗 🌺 🖼 🦓 | |
| Zd(3Fess a) https://10.77.244.198/certary/certrgna.asp | 🛩 🔁 Go |
| Create new key set Use existing key set | 2 |
| CSP: Microsoft RSA SChannel Cryptographic Previder 🛩 | |
| Kay Usage: 🛞 Exchange | |
| Key Size: 1024 Min: 004 (common key size: 512 1024 2048 4045 5192 10204) | |
| Automatic key container name O User specified key container name | |
| 🗹 Mark keys as exportable | |
| Export keys to file | |
| Enable strong private key protection | |
| Store certificate in the local computer certificate store Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store. | |
| Additional Options: | |
| Request Format: O CMC @ PKCS10 | |
| Hash Algorithm: SHA-1 💌 | |
| Only used to sign request. | |
| Save request to a file | |
| Attributes: | |
| Friendly Name: | |
| Submit > | |
| | |
| | Internet |

8. Fare clic su **Sì** nella finestra successiva per consentire il processo di richiesta del certificato.

| Potentia | al Scripting Violation |
|----------|--|
| ♪ | This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now? |
| | Yes No |

 Viene visualizzata la finestra Certificato rilasciato che indica che il processo di richiesta del certificato è stato completato correttamente. Il passaggio successivo consiste nell'installare il certificato rilasciato nell'archivio certificati del PC. Fare clic su Installa il certificato.

| Alicrosoft Certificate Services - Microsoft Internet Explorer | |
|---|----------|
| Ple Edt View Pavortis' Tools Help | |
| Address (a) http://10.77.244.198/certsrvjcert/rish.asp | 💌 🛃 Go |
| Mirmonit Certificato Saninon wirelenn | Hame |
| | Listins |
| Certificate Issued | |
| The certificate you requested was issued to you. | |
| Install this certificate | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| () | Internet |

10. Il nuovo certificato è stato installato correttamente nel PC da cui la richiesta è stata generata nel server

| CA. | |
|--|----------------------------|
| Microsoft Certificate Services - Microsoft Internet Explorer | |
| File Edit View Pavorites Tools Help | |
| Address 🗃 http://10.77.244.198/bertsrv/oertrepn.asp | 💌 🎒 Go |
| Microsoft Certificate Services wineless | Home |
| Certificate Installed | |
| OF UNION WINDOW | |
| Your new certificate has been successfully installed. | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | 3 |
| Done | Internet |
| l nassangio successivo consiste nell'esportare il certificato dall'arc | hivio certificati al disco |

11. Il passaggio successivo consiste nell'esportare il certificato dall'archivio certificati al disco rigido come file. Questo file di certificato verrà utilizzato successivamente per scaricare il certificato nel WLC.Per esportare il certificato dall'archivio certificati, aprire il browser Internet Explorer, quindi fare clic su Strumenti > Opzioni Internet.

| Pde Ede View Pavortes Tools Help | 10 |
|---|----|
| The Ed: Were Percenter took took Address a about blank Percenter and the second | |
| | × |

12. Fare clic su **Contenuto > Certificati** per accedere all'archivio certificati in cui i certificati sono installati per impostazione

| predefinita. |
|---|
| Internet Options |
| General Security Privacy Content Connections Programs Advanced Content Advisor Settings help you control the Internet content that can be viewed on this computer. Enable Settings Certificates Use certificates to positively identify yourself, certification |
| Clear SSL State Certificates Publishers Personal information AutoComplete stores previous entries AutoComplete |
| And suggests matches for you. Microsoft Profile Assistant stores your personal information. My Profile |
| OK Cancel Apply |

 I certificati dei dispositivi vengono in genere installati nell'elenco dei certificati personali. In questo punto dovrebbe essere visualizzato il certificato appena installato. Selezionare il certificato e fare clic su Esporta.

| Certificate | s | | | | ? 🔀 |
|-------------|--------------|-------------------------------|---|-------------------|-----|
| Intended pu | rpose: | <all></all> | | | ~ |
| Personal | Other Peop | le Intermediate Certification | Authorities Trusted R | oot Certification | < > |
| | | | | | |
| Issued | То | Issued By | Expiratio Frier | ndly Name | |
| E cisco | wkc123 | wireless | 1/25/2010 <nor< td=""><td>ne></td><td></td></nor<> | ne> | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | - |
| Import | | ort Remove | | Advance | d |
| Certificate | intended p | irposes | | | |
| Server Au | theotication | | | | |
| Derver Au | Cherrocecion | | | Linux | |
| | | | | View | |
| | | | | | |
| | | | | Close | |
| | | | | | |

14. Fare clic su **Avanti** nelle seguenti finestre. Scegliere l'opzione **Sì, esporta la chiave privata** nella finestra **Esportazione guidata certificati**. Fare clic su **Next**

| (Avanti). | |
|--|--------------|
| Certificate Export Wizard | \mathbf{X} |
| Export Private Key You can choose to export the private key with the certificate. | |
| Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page. | |
| Do you want to export the private key with the certificate? | |
| Yes, export the private key | |
| No, do not export the private key | |
| | |
| | |
| | |
| | |
| | |
| | |
| < Back Next > Cance | |

15. Scegliere il formato del file di esportazione come **.PFX** e scegliere l'opzione **Abilita protezione avanzata**. Fare clic su **Next** (Avanti).

| DER encoded binary X.509 (.CER) Base-64 encoded X.509 (.CER) |
|---|
| DER encoded binary X.509 (.CER) Base-64 encoded X.509 (.CER) |
| |
| Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) |
| Include all certificates in the certification path if possible |
| Personal Information Exchange - PKCS #12 (.PFX) |
| Include all certificates in the certification path if possible |
| Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above) |
| Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above) |

16. Nella finestra Password, immettere una password. In questo esempio viene utilizzato **cisco** come

| password. | | | |
|----------------|--|----------------------------------|-------|
| Certificat | te Export Wizard | | × |
| Passwe To r | ord maintain security, you must protect the | private key by using a password. | |
| Тур | be and confirm a password. Password: | | |
| | ***** | | |
| | Confirm password: | | |
| | ***** | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | < <u>B</u> ack <u>N</u> ext ≻ C | ancel |

17. Salvare il file del certificato (file PFX) sul disco rigido. Fare clic su **Avanti** e completare l'esportazione.



Download del certificato del dispositivo sul WLC

Ora che il certificato del dispositivo WLC è disponibile come file con estensione PFX, il passaggio successivo consiste nel scaricare il file sul controller. I WLC Cisco accettano certificati solo in formato .PEM. Pertanto, è innanzitutto necessario convertire il file in formato PFX o PKCS12 in un file PEM utilizzando il programma openSSL.

Convertire il certificato in formato PFX in formato PEM utilizzando il programma openSSL

Èpossibile copiare il certificato in qualsiasi PC in cui è installato openSSL per convertirlo in formato PEM. Immettere i seguenti comandi nel file Openssl.exe nella cartella bin del programma openSSL:

Nota: è possibile scaricare openSSL dal sito Web OpenSSL .

!--- This is the same password that is mentioned in step 16 of the previous section. MAC
verified Ok Enter PEM Pass phrase : cisco
!--- Specify any passphrase here. This example uses the PEM passphrase as cisco. Verifying - PEM
pass phrase : cisco

Il file del certificato viene convertito nel formato PEM. Il passaggio successivo consiste nel scaricare il certificato del dispositivo in formato PEM sul WLC.

Nota: prima di questo, avete bisogno di un software server TFTP sul vostro PC da cui il file PEM sta per essere scaricato. Il PC deve essere connesso al WLC. Per il server TFTP devono essere specificate la directory corrente e la directory di base con la posizione in cui è memorizzato il file PEM.

Scaricare il certificato dispositivo in formato PEM convertito nel WLC

Questo esempio spiega il processo di download dalla CLI del WLC.

- 1. Accedere alla CLI del controller.
- 2. Immettere il comando transfer download datatype eapdevcert.
- 3. Immettere il comando **transfer download serverip** *10.77.244.196*.10.77.244.196 è l'indirizzo IP del server TFTP.
- 4. Immettere il comando **transfer download filename** *ciscowlc.pem*.ciscowlc123.pem è il nome del file utilizzato in questo esempio.
- 5. Immettere il comando **transfer download certpassword** per impostare la password per il certificato.
- 6. Immettere il comando transfer download start per visualizzare le impostazioni aggiornate.Quindi, rispondere y quando viene richiesto di confermare le impostazioni correnti e avviare il processo di download.Nell'esempio viene mostrato l'output del comando download:

(Cisco Controller) >transfer download start

| Mode TFTP | |
|--|--|
| Data Type Vendor Dev Cert | |
| TFTP Server IP 10.77.244.196 | |
| TFTP Packet Timeout 6 | |
| TFTP Max Retries 10 | |
| TFTP Path | |
| TFTP Filename ciscowlc.pem | |
| | |
| This may take some time. | |
| Are you sure you want to start? (y/N) y | |
| TFTP EAP CA cert transfer starting. | |
| Certificate installed. | |
| Reboot the switch to use the new certificate. | |
| Enter the reset system command to reboot the controller. | |

The controller is now loaded with the device certificate.

7. Immettere il comando **reset system** per riavviare il controller. Il controller è ora caricato con il certificato del dispositivo.

Installare il certificato radice di PKI nel WLC

Ora che il certificato del dispositivo è installato nel WLC, il passaggio successivo consiste nell'installare il certificato radice della PKI nel WLC dal server CA. Attenersi alla procedura seguente:

1. Visitare il sito Web all'indirizzo **http://<indirizzo IP del server CA>/certsrv** dal PC che dispone di una connessione di rete al server CA. Eseguire il login come amministratore del server CA

| 0/ \. | | | |
|--|---|--------|--------|
| about:blank - Microsoft Internet Explorer | | | X |
| File Edt Ver Filvortes Toole Help | | | |
| Address Mtps://10.77.244.198/certsrv | | | 🛩 💽 Go |
| Copening page http://10.77.244.198/certory | Connect to 10, 77, 244, 198 Connecting to 10, 77, 244, 198 User name: administrator Password: Remember my passwor OK | Carcel | |
| | | | |

2. Fare clic su Scarica un certificato CA, una catena di certificati o un

| RL. | | |
|---|---|--------------|
| Norosoft Certificate Services - Microsoft Internet Explorer | | |
| Edt Veen Favorites Tools 1940 | | |
| 000 00 Http://10.77.244.198/contsrv/ | | N (3) |
| Nerosoft Certificate Services Wireless | | Home |
| elcome | | |
| e this Web site to request a certificate for your Web browse entity to people you communicate with over the Web, sign an inform other security tasks. | er, e-mail client, or other program. By using a certificate, you can verify yo ind encrypt messages, and, depending upon the type of certificate you rec | ur quest, |
| u can also use this Web site to download a certificate authors with status of a pending request. | ority (CA) certificate, certificate chain, or certificate revocation list (CRL), | orto |
| r more information about Certificate Services, see Certifica | ate Services Documentation. | |
| elect a task: Request a certificate View the status of a pending certificate request | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

 Nella pagina risultante è possibile visualizzare i certificati CA correnti disponibili nel server CA nella casella Certificato CA. Scegliere DER come metodo di codifica e fare clic su Scarica certificato

CA.

| Microsoft Certificate Services - Microsoft Internet Explorer | |
|--|----------|
| Pée Edit Wew Pavortes' Tools Help | |
| Addrass 🕘 http://10.77.244.198/certsrv/certcarc.asp | ං 🛃 🐱 |
| Aliensedt Certificate Services - wireless | Home |
| Download a CA Certificate, Certificate Chain, or CRL | |
| To trust certificates issued from this certification authority, install this CA certificate chain. | |
| To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method. | |
| CA certificate: | |
| (Current (wireless) | |
| Encoding method: | |
| () DER | |
| O Base 64 | |
| Download CA certificate chain | |
| Download latest base CRL | |
| Download latest deta CRL | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | internet |

- 4. Salvare il certificato come file **.cer**. In questo esempio viene utilizzato **certnew.cer** come nome di file.
- 5. Il passaggio successivo consiste nel convertire il file con estensione cer in formato PEM e scaricarlo sul controller. Per eseguire questi passaggi, ripetere la stessa procedura descritta nella sezione Download del certificato del dispositivo sul WLC con le seguenti modifiche: I file "-in" e "-out" openSSL sono certnew.cer e certnew.pem.Inoltre, in questo processo non sono richieste passphrase PEM o password di importazione.Inoltre, il comando openSSL per convertire il file .cer nel file .pem è:x509 -in certnew.cer -inform DER -out certnew.pem outform PEMNel passaggio 2 della sezione Download del certificato sul WLC è:(Cisco Controller)>transfer download datatype eapcacertII file da scaricare sul WLC è certnew.pem.

come segue:

 Dall'interfaccia utente del WLC, fare clic su Security (Sicurezza). Nella pagina Protezione fare clic su Avanzate > Certificati IPSec nelle attività visualizzate a sinistra. Fare clic su Certificato CA per visualizzare il certificato CA installato. Di seguito è riportato l'esempio:



 Per verificare se il certificato del dispositivo è installato sul WLC, dall'interfaccia utente del WLC fare clic su Security. Nella pagina Protezione fare clic su Avanzate > Certificati IPSec nelle attività visualizzate a sinistra. Fare clic su ID certificato per visualizzare il certificato del dispositivo installato. Di seguito è riportato

| resempio. | | | | | | | | | | |
|--|--------------------|--------|------------|-----------------------------|---------------|-------------------|------------------|-------------|----------|----------------|
| 🗿 wic2006 - Microsoft Inte | rnet Explorer | | | | | | | | | |
| File Edit View Favorites | Tools Help | | | | | | | | | <u></u> |
| ahaha | | | | | | | Sage Co | nfiguration | Eing | Logout Befresh |
| CISCO | MONITOR | WLANS | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | | |
| Security | ID Certific | ate | | | $\overline{}$ | , | | | | New |
| AAA General RADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies E Local EAP Priority Order Access Control Lists Wireless Protection Policies Web Auth Advanced CIDS Sensors Shunned Clients | Name bsnSslEapD | evCert | ¥a Pro | lid Period m 2008 Jan 24 | ₩, 12:10:31 (| GMT Until 2010 Ja | n 23rd, 12:18:31 | | | |
| D Certificate | | | | | | | | | | |
| ê) | | | | | | | | | 🔒 🔵 Inke | met |
| | | | | | | | | | | |

Genera un certificato dispositivo per il client

Ora che il certificato del dispositivo e il certificato della CA sono installati sul WLC, il passaggio successivo consiste nel generare questi certificati per il client.

Per generare il certificato del dispositivo per il client, eseguire la procedura seguente. Questo certificato verrà utilizzato dal client per l'autenticazione al WLC. In questo documento vengono illustrati i passaggi necessari per la generazione di certificati per il client Windows XP Professional.

 Visitare il sito Web all'indirizzo http://<indirizzo IP del server CA>/certsrv dal client che richiede l'installazione del certificato. Eseguire l'accesso come nome di dominio omeutente al server CA. Il nome utente deve corrispondere al nome dell'utente che utilizza questo computer XP e l'utente deve essere già configurato come parte dello stesso dominio del server

| CA. | |
|---------------------|----------------------|
| Connect to 10.7 | 7.244.198 🔹 🔁 🔀 |
| | |
| Connecting to 10.73 | 7.244.198 |
| User name: | 🖸 wireless\user2 |
| Password: | |
| | Remember my password |
| | OK Cancel |

2. Selezionare Richiedi

Certificato. Microsoft Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - Wireless Memo Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

| Felect a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL | | | | | | |
|---|--|--|--|--|--|--|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

3. Nella pagina Richiedi un certificato fare clic su **Richiesta avanzata di** certificati.

| Microsoft Certificate Services - Microsoft Internet Explorer | X 6 刘 |
|--|----------|
| File Edit View Pavorities' Tools Help | A |
| Address 🕘 Mtp://10.77.244.198/certsrv/certraus.esp | 💌 🛃 Go |
| Alicrosoft Certificate Services wireless | Home |
| Request a Certificate | |
| Select the certificate type: | |
| User Certificate | |
| Or submit an advanced certificate request. | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| (c) http://10.77.244.198/ceetsrv/ceetrgad.asp | Internet |
| | |

4. Nella pagina Richiesta avanzata di certificati fare clic su **Crea e invia una richiesta a questa CA**. Verrà visualizzato il modulo di richiesta del certificato

| vanzato. | |
|---|-------------|
| Microsoft Certificate Services - Microsoft Internet Explorer | |
| Edit View Favorites Tools Help | 1 |
| 2003 🕘 Http://10.77.244.190/certsrv/certrqad.asp | 🗹 🔁 😡 |
| Hicrosoft Certificate Services - wireless | Home |
| dvanced Certificate Request | |
| he 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 CMC or PKCS #10 file, or submit a renewal request by using a base PKCS #7 file. | -64-encoded |
| Request a certificate for a smart card on behalf of another user by using the smart card certificate enrolment station. Note: You must have an enrollment agent certificate to submit a request on behalf of another user. | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | Internet |
| el modulo di richiesta avanzata del certificato scegliere Utente dal menu a discer | sa Modello |

5. Nel modulo di richiesta avanzata del certificato scegliere Utente dal menu a discesa Modello di certificato.Nella sezione Opzioni chiave (Key options), selezionate i seguenti parametri:Immettere la Dimensione chiave nel campo Dimensione chiave. In questo esempio viene utilizzato 1024.Selezionare l'opzione Contrassegna le chiavi come

esportabili.

| oportabili | • | |
|----------------------|---|-----------|
| Microsoft Certi | ficate Services - Microsoft Internet Explorer | |
| Ne Edit View | Favorites Tools Help | |
| iddresis 者 http://10 | 3.77.244.198/certsrv/certrgma.asp | 👻 🄁 😡 |
| Microsoft Codifi | nata Seminan windaan | Home |
| | | Listins . |
| Advanced Ce | rtificate Request | |
| Certificate Tem | plate: | |
| | Basic EFS 💌 | |
| Key Ontions: | Basic EFS | |
| Key Options: | Counte providence and Counter providence from east | |
| 0.82 | Microsoft Enhanced Crystographic Provider vf. 0 | |
| Key Usage: | Exchange | |
| Key Size | 1024 Min: 394 (common key piper \$12 1024 2049 4098 9192 16094.) | |
| ray once | Actomatic key container name Other specified key container name | |
| | Mark keys as exportable | |
| | Export keys to file | J |
| | Enable strong private key protection | |
| | Store certificate in the local computer certificate store Stores the certificate in the local computer atore instead of in the user's certificate atore. Does not install the root GA's certificate. You must be an administrator to generate or use a key in the local machine store. | |
| Additional Optio | ins: | |
| Request Format: | ©CMC OPKCS10 | |
| Hash Algorithm | SHA-1 Confy used to sign request. | |
| | Save request to a file | |
| Attributes: | | |
| Done | | Internet |

6. Configurare tutti gli altri campi necessari e fare clic su

| Invia. | |
|---|------------------------------|
| 🗿 Microsoft Certificate Services - Microsoft Internet Explorer | |
| Plin Edit View Pavortes Tools Help | A # |
| 🔇 Back + 💿 - 📧 🗟 🐔 🔎 Search 👷 Pavortes 🤣 🎯 🖓 🖼 🦓 | |
| Address 🕘 http://10.77.244.198/certary/certarges.app | 💌 🔁 Go |
| Create new key set | |
| CSP: Microsoft RSA SChannel Cryptographic Previder 💙 | |
| Kay Usaga: 🐵 Exchange | |
| Key Size: 1024 Min: 004 (cernmon key size: 512 1024 2088 6395 5192 15306) | |
| Automatic key container name Ouser specified key container name | |
| 🗹 Mark keys as exportable | |
| Export keys to file | |
| Enable strong private key protection | |
| Share certificate in the local computer certificate store instead of in the user's certificate store. Does not install the root GA's certificate. You must be an administrator to generate or use a key in the local machine store. | |
| Additional Options: | |
| Request Format: © CMC | |
| Hash Algorithm: SHA-1 V | |
| Only used to sign request. | |
| Save request to a file | |
| Attributes: | |
| Friendly Name: | |
| Submit > | |
| | |
| | Internet |

 Il certificato del dispositivo del client è ora generato in base alla richiesta. Fare clic su Installa il certificato per installarlo nell'archivio certificati.

| A Microsoft Certificate Services - Microsoft Internet Explorer | - 6 🛛 |
|--|----------|
| File Edit View Favorites Tools Help | 4 |
| Address 📵 http://10.77.244.190/certsrv/certfinsh.asp | 💌 🄁 Go |
| | |
| Microsoff Certificate Senices wireless | Home |
| Certificate Issued | |
| The continent manufacture include to you | |
| The certaincate you requested was issued to you. | |
| Install this certificate | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | <u>M</u> |
| | Internet |

 Dovrebbe essere possibile trovare il certificato del dispositivo del client installato nell'elenco Certificati personali in Strumenti > Opzioni Internet > Contenuto > Certificati sul browser IE del

| client. | | | | |
|--------------|---|------------------------------|--|-----------------------|
| Certificates | 5 | | | ? 🔽 |
| Intended pur | pose: <all< td=""><td>></td><td></td><td>~</td></all<> | > | | ~ |
| Personal | Other People | Intermediate Certification A | uthorities Trusted Ro | oot Certification < 😕 |
| _Issued_I | (o | Issued By | Expiratio Frier | dly Name |
| E 1234 | | wireless | 1/25/2009 <nor< td=""><td>ie></td></nor<> | ie> |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Import | Export. | . Remove | | Advanced |
| Certificate | intended purpor | ses | | |
| Encrypting | File System | | | |
| | | | | View |
| | | | | Close |

Il certificato del dispositivo per il client è installato nel client.

Genera il certificato CA radice per il client

Il passaggio successivo consiste nel generare il certificato CA per il client. Eseguire i seguenti passaggi dal PC client:

 Visitare il sito Web all'indirizzo http://<indirizzo IP del server CA>/certsrv dal client che richiede l'installazione del certificato. Eseguire l'accesso come nome di dominio omeutente al server CA. Il nome utente deve corrispondere al nome dell'utente che utilizza questo computer XP e l'utente deve essere già configurato come parte dello stesso dominio del server

| CA. | |
|-------------------|----------------------|
| Connect to 10. | 77.244.198 🔹 💽 🔀 |
| | |
| Connecting to 10. | 77.244.198 |
| User name: | 🛃 wireless\user2 |
| Password: | |
| | Remember my password |
| | |
| | OK Cancel |

2. Nella pagina risultante è possibile visualizzare i certificati CA correnti disponibili nel server CA nella casella Certificato CA. Selezionate Base 64 come metodo di codifica. Quindi, fare clic su Scarica certificato CA e salvare il file sul PC del client come file .cer. In questo esempio viene utilizzato rootca.cer come nome di

| Wicrosoft Certificate Services - Microsoft Internet Explorer | |
|--|------------|
| File Edt Vies Factorias Tools Telep | |
| Address W Hetpol(10.77.244.198/certsrv/certsarc.asp | دى 🔁 😒 |
| | · |
| Afterosoff Conflictive Screece Assess | Home |
| Download a CA Certificate, Certificate Chain, or CRL | |
| To tout continue to the section of fears the continue of the day install this CA continues their | |
| To trust certificates issued from this certification authority, install this CA certificate chain. | |
| To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method. | |
| CA certificate: | |
| Current hvireless1 | |
| | |
| | |
| | |
| Encoding method: | |
| © DER ® Base 64 | |
| Download CA certificate | |
| Download CA certificate chain | |
| Download latest base CRL | |
| Download latest delta CRL | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | Internet |
| | A MARTINE. |

3. Installare quindi il certificato CA salvato in formato cer nell'archivio certificati del client. Fare doppio clic sul file rootca.cer e fare clic su **Installa certificato**.

| Certificate | ? × |
|---|------------|
| General Details Certification Path | |
| Certificate Information | |
| This certificate is intended for the following purpose(s): • All issuance policies • All application policies | |
| Issued to: wireless | - |
| Issued by: wireless | |
| Valid from 1/23/2008 to 1/23/2013 | |
| Install Certificate Issuer Statem | ok |

4. Fare clic su **Avanti** per importare il certificato dal disco rigido del client all'archivio certificati.

| Certificate Import Wizard | | $\mathbf{\times}$ |
|---------------------------|---|-------------------|
| | Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network certificates are kept. To continue, click Next. | |
| | Cancer | |

5. Scegliere Seleziona automaticamente l'archivio certificati in base al tipo di certificato e fare clic su

Avanti.

| | the second | location to |
|-------------------------------|---|-------------|
| Automatiz | ally select the certificate store based on the type of certifi | icate |
| O Place all co | rtificates in the following store | |
| Certificate | store: | |
| | В | rowse |
| | | |
| | | |

6. Per completare il processo di importazione, fare clic su Finish

| (Fine). | | | |
|---------------------------|---|--|---|
| Certificate Import Wizard | | | X |
| | Completing the C Wizard You have successfully compl wizard. You have specified the follow | Certificate Import | |
| | Certificate Store Selected Content | Automatically determined by t Certificate | |
| - | < Back | Finish Cancel | |

7. Per impostazione predefinita, i certificati CA vengono installati nell'elenco Autorità di certificazione radice attendibili nel browser IE del client in Strumenti > Opzioni Internet > Contenuto > Certificati. Di seguito è riportato l'esempio:

| Issued To | Issued By | Expiratio | Friendly Name |
|---------------------|------------------------|------------|------------------|
| VeriSign Trust Netw | VeriSign Trust Network | 5/19/2018 | VeriSign Class 3 |
| VeriSign Trust Netw | VeriSign Trust Network | 8/2/2028 | VeriSign Class 3 |
| VeriSign Trust Netw | VeriSign Trust Network | 5/19/2018 | VeriSign Class 4 |
| VeriSign Trust Netw | VeriSign Trust Network | 8/2/2028 | VeriSign Class 1 |
| VeriSign Trust Netw | VeriSign Trust Network | 8/2/2028 | VeriSign Class 4 |
| VeriSign Trust Netw | VeriSign Trust Network | 5/19/2018 | VeriSign Class 1 |
| 🕮 wireless | wireless | 1/23/2013 | <none></none> |
| Wireless-CA | Wireless-CA | 12/18/2012 | <none></none> |
| Xcert EZ by DST | Xcert EZ by DST | 7/11/2009 | Xcert EZ by DST |
| Import Export | Remove | | Advanc |

Tutti i certificati richiesti vengono installati sul WLC e sul client per l'autenticazione EAP locale EAP-FAST. Il passaggio successivo è configurare il WLC per l'autenticazione EAP locale.

Configurazione di EAP locale sul WLC

Completare questa procedura dalla **modalità GUI** del **WLC** per configurare l'autenticazione EAP locale sul WLC:

1. Fare clic su **Protezione > EAP**

| Weic2006 - Microsoft Internet Explorer Ne Edit Vew Poworkes Tools Help Sage Configuration Eine Legouit Befress CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP Security AAA Call Station ID Type IP Address M Caneral RADIUS Authentication Accounting TACACS+ LDAP Locol Nat Users Magement Server Index Server Address Port IPSec Admin Status Verteork User Management Server Index Server Address Port IPSec Admin Status Verteork User Management Server Index Server Address Port IPSec Admin Status |
|--|
| Pie Edit View Pavortes Tools Help Security MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP Security RADIUS Authentication Security Apply New * AAA Call Station ID Type IP Address Y General RADIUS Use AES Key Wrop (Designed for FIPS customers and requires a key wrap compliant RADIUS server) Authentication Accounting Network User Nanagement Server Index Server Address Port IPSec Admin Status User Login Polities User Login Polities Floreal EAP Floreal EAP Network User Nanagement Server Address Port IPSec Admin Status |
| Sage Configuration Eing Legeut Befrest CISCO MONITOR WLANS CONTROLLER WIRELESS GECURITY MANAGEMENT COMMANDS HELP Security RADIUS Authentication Servers Apply New Ceneral RADIUS Call Station ID Type IP Address M Ceneral RADIUS Use AES Key Wrop (Designed for FIPS customers and requires a key wrap compliant RADIUS server) Authentication Accounting Network User Nanagement Server Index Server Address Port IPSec Admin Status User Login Policies User Login Policies Network User Nanagement Server Address Port IPSec Admin Status User Login Policies User Login Policies Network User Nanagement Server Address Port IPSec Admin Status |
| CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP Security RADIUS Authentication Servers Apply New * AAA Call Station ID Type IP Address * General * RADIUS Use AES Key Wrop (Designed for FIPS customers and requires a key wrap compliant RADIUS server) Authentication Accounting Network User Nanagement Server Address Port IPSec Admin Status User Login Polities User Login Polities Network User Nanagement Server Address Port IPSec Admin Status User Login Polities User Login Polities Apply Network User Nanagement Server Address Port IPSec Admin Status |
| Security RADIUS Authentication Servers Apply New * AAA General * Call Station ID Type IP Address * * RADIUS Authentication Accounting * * Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server) * TACACG4 Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server) Network User Nanagement Server Index Server Address Port IPSec Admin Status User Login Polities User Login Polities Server Login Polities Server Address Port IPSec Admin Status |
| AAA Call Station ID Type IP Address General RADIUS Use AES Key Wrop (Designed for FIPS customers and requires a key wrap compliant RADIUS server) Authentication Authentication Use AES Key Wrop (Designed for FIPS customers and requires a key wrap compliant RADIUS server) > TACACS+ Network User Nanagement Server Index Server Address Port IPSec Admin Status USAF Filtering Disabled Clients User Login Policies Server Login Policies AB Policies AB Policies AB Policies Server Login Policies Server Login Policies Server Login Policies |
| Authentication Use AES Key Wrop (Designed for FIPS customers and requires a key wrap compliant RADIUS server) Accounting Network User Network User LDAP Network User Management Local Net Users MAC Filtering Disabled Clients User Lopin Policies LP Policies Accounting |
| Image: Note of the server labor of |
| MAC Filtering Disabled Clients User Login Policies BP Policies |
| User Login Policies |
| P Local FAP |
| Priority Order |
| Access Control Lists |
| Wireless Protection Policies |
| > Web Auth |
| ▶ Advanced |
| |
| |
| |
| |
| |
| |
| |
| a) b) b) b) b) b) b) b) b) b) b |

2. In EAP locale fare clic su **Profili** per configurare il profilo EAP locale.



- 3. Per creare un nuovo profilo EAP locale, fare clic su New (Nuovo).
- Configurare un nome per il profilo e fare clic su Applica. In questo esempio, il nome del profilo è Idap. In questo modo è possibile accedere ai profili EAP locali creati sul WLC.

| wic2006 - Microsoft Inter | rnet Explorer | | | | | | | |
|--|---------------|---------------|----------|----------|------------|----------|-------------------------|----------------------|
| File Edit View Favorites | Tools Help | | | | | | | ** |
| ababa | | | | | | | nfiguration <u>P</u> in | p Logout Befresh |
| CISCO | MONITOR WLA | Ws CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | |
| Security | Local EAP Pre | ofiles > New | | | | | < Back | Apply |
| AAA General « RADIUS Authentication Accounting TACACS+ Local Net Users HAC Filtering Disabled Clients User Login Policies AP Policies EAP-FAST Parameters Authentication Priority Priority Order Access Control Lists Wireless Protection Policies Wireless Protection Policies Wireless Protection Policies | Profile Name | | Idap | | | | | |
| a) Done | | | | | | | ● ● | Internet |

 Fare clic sul profilo Idap appena creato, che viene visualizzato nel campo Nome profilo della pagina Profili EAP locali. Viene visualizzata la pagina Profili EAP locali > Modifica.

| wic2006 - Microsoft Inter | net Explorer | | | | | | | | |
|--|--------------|-----------|------------|-----------------|----------|------------|----------|--------------------------|----------------|
| File Edit View Pavorites | Tools Help | _ | | 10. A 10. A 10. | | | | | |
| ahaha | | | | | | | | nfiguration <u>P</u> ing | Logout Befresh |
| CISCO | MONITOR | WLANS | CONTROLLER | W]RELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | |
| Security | Local EA | P Profile | 9 | | _ | | | New | Apply |
| - AAA | Profile Na | me | | LEAP | CAP-PAST | EAP-TLS | PEAP | | |
| General * RADIUS Authentication Accounting * TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies | Ideo | | | | | | | 0 | |
| Local EAP General Profiles EAP-FAST Parameters Authentication Priority | | | | | | | | | |
| ▶ Priority Order | | | | | | | | | |
| ▶ Access Control Lists | | | | | | | | | |
| Wireless Protection Policies | | | | | | | | | |
| Web Auth | | | | | | | | | |
| ► Advanced | | | | | | | | | sharped |

6. Configurare i parametri specifici del profilo nella pagina Profili EAP locali > Modifica.Scegliere EAP-FAST come metodo di autenticazione EAP locale.Selezionare le caselle di controllo Certificato locale richiesto e Certificato client richiesto.Selezionare Fornitore come Autorità di certificazione perché il documento utilizza un server CA di terze parti.Selezionare la casella di controllo accanto a Controlla rispetto ai certificati CA per consentire la convalida del certificato in ingresso dal client rispetto ai certificati CA sul controller.Se si desidera che il nome comune (CN) nel certificato in ingresso venga convalidato rispetto al CN dei certificati CA nel controller, selezionare la casella di controllo Verifica identità CN certificato. L'impostazione predefinita è disattivata. Per consentire al controller di verificare che il certificato del dispositivo in ingresso sia ancora valido e non sia scaduto, selezionare la casella di controllo Controlla validità data certificato.Nota: la validità della data del certificato viene verificata in base all'ora UTC (GMT) corrente configurata sul controller. La differenza di fuso orario viene ignorata.Fare clic su Apply (Applica).



7. Il profilo EAP locale con autenticazione EAP-FAST viene ora creato sul

| WLC. | | | | | | | | | |
|---|-------------------|------------|-------------|----------|--|----------|------|---------|--|
| 🗿 wic2006 - Microsoft Inter | net Explorer | | | | | | | . • 🛛 | |
| File Edit View Pavorites 1 | tools Help | | a Carl Carl | | | | | | |
| ahaha | | | | | Sage Configuration Ping Logaut Befresh | | | | |
| CISCO | MONITOR WLANS | CONTROLLER | W]RELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | | |
| Security | Local EAP Profile | 8 | | | | | New | Apply | |
| * AAA | Profile Name | | LEAP E | AP-PAST | EAP-TLS | PEAP | | | |
| RADIUS Authentication | Ideo | | | 1 | | | | | |
| Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies | | | | | | | | | |
| Cocal EAP General Profiles EAP-FAST Parameters Authentication Priority | | | | | | | | | |
| ▶ Priority Order | | | | | | | | | |
| ▶ Access Control Lists | | | | | | | | | |
| Wireless Protection Policies | | | | | | | | | |
| Web Auth | | | | | | | | | |
| Advanced | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| 10 Date: | | | | | | | A | toos at | |
| Looné | | | | | | | | vernet | |

8. Il passaggio successivo è la configurazione di parametri specifici di EAP-FAST sul WLC. Nella pagina Sicurezza WLC, fare clic su EAP locale > Parametri EAP-FAST per passare alla pagina Parametri del metodo EAP-FAST.Deselezionare la casella di controllo Provisioning anonimo in quanto in questo esempio viene spiegato come utilizzare i certificati EAP-FAST. Mantenere tutti gli altri parametri ai valori predefiniti. Fare clic su Apply (Applica).

| wic2006 - Microsoft Inter | net Explorer Iods - Helo | | | |
|---|-----------------------------|------------|--------------|----------------------------------|
| alada | | | Saye Configu | ration Ping Logout Befresi |
| Security | EAP-FAST Method Parameters | | COMMANDS HE | Apply |
| | Server Key (in hex) | •••• | | |
| RADIUS Authentication | Confirm Server Key | •••• | | |
| TACACS+ | Time to live for the PAC | 10 doys | | |
| NAC Filtering Disabled Clients | Authority ID (in hex) | 436973636f | | |
| User Login Policies AP Policies | Authority ID Information | Cisco A-ID | | |
| Profiles EAP-FAST Parameters Abhaptication Priorier | Anonymous Provision | Enabled | | |
| E Priority Order | | | | |
| Access Control Lists | | | | |
| Wireless Protection Policies | | | | |
| E Web Auth | | | | |
| E Advanced | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| n | | | | 🚔 👄 Internet |

Configura WLC con dettagli del server LDAP

Ora che il WLC è stato configurato con il profilo EAP locale e le informazioni correlate, il passaggio successivo è configurare il WLC con i dettagli del server LDAP. Completare questi passaggi sul WLC:

 Nella pagina Sicurezza del WLC, selezionare AAA > LDAP dal riquadro attività a sinistra per passare alla pagina di configurazione del server LDAP. Per aggiungere un server LDAP, fare clic su Nuovo. Viene visualizzata la pagina Server LDAP > Nuovo.



2. Nella pagina Server LDAP: Modifica, specificare i dettagli del server LDAP, ad esempio l'indirizzo IP del server LDAP, il numero di porta, lo stato Abilita server e così via. Scegliere un numero dalla casella a discesa Indice server (priorità) per specificare l'ordine di priorità di questo server in relazione agli altri server LDAP configurati. È possibile configurare fino a diciassette server. Se il controller non riesce a raggiungere il primo server, proverà con il secondo nell'elenco e così via.Immettere l'indirizzo IP del server LDAP nel campo Indirizzo **IP server**.Immettere il numero della porta TCP del server LDAP nel campo **Numero porta**. L'intervallo valido è compreso tra 1 e 65535 e il valore predefinito è 389.Nel campo DN base utente, immettere il nome distinto (DN) della sottostruttura nel server LDAP che contiene un elenco di tutti gli utenti. Ad esempio, ou=unità organizzativa, ou=unità organizzativa successiva e o=corporation.com. Se la struttura contenente gli utenti è il DN di base, immettere o=corporation.com o dc=corporation, dc=com.In guesto esempio, l'utente si trova nell'unità organizzativa Idapuser che a sua volta viene creata come parte del dominio Wireless.com.II DN di base dell'utente deve puntare al percorso completo in cui si trovano le informazioni utente (credenziali utente in base al metodo di autenticazione EAP-FAST). In questo esempio, l'utente si trova nel DN di base OU=ldapuser, DC=Wireless, DC=com.Per ulteriori informazioni sull'unità organizzativa e sulla configurazione degli utenti, vedere la sezione Creazione di utenti sul controller di dominio in questo documento.Nel campo Attributo utente, immettere il nome dell'attributo nel record utente che contiene il nome utente.Nel campo Tipo oggetto utente, immettere il valore dell'attributo objectType LDAP che identifica il record come utente. I record utente dispongono spesso di diversi valori per l'attributo objectType, alcuni dei quali sono univoci per l'utente e altri sono condivisi con altri tipi di oggetto. Nota: è possibile ottenere il valore di questi due campi dal server delle directory con l'utilità browser LDAP, inclusa negli strumenti di supporto di Windows 2003. Questo strumento del browser LDAP Microsoft è denominato LDP. Con l'aiuto di guesto strumento, è possibile conoscere i campi DN base utente, Attributo utente e Tipo oggetto

utente di questo particolare utente. Per informazioni dettagliate sull'utilizzo di LDP per conoscere questi attributi specifici dell'utente, vedere la sezione <u>Utilizzo di LDP per</u> <u>identificare gli attributi utente</u> in questo documento.Selezionare **Protetto** dall'elenco a discesa Modalità server se si desidera che tutte le transazioni LDAP utilizzino un tunnel TLS sicuro. In caso contrario, scegliere **Nessuno**, che è l'impostazione predefinita.Nel campo **Timeout server**, immettere il numero di secondi che devono intercorrere tra le ritrasmissioni. L'intervallo valido è compreso tra 2 e 30 secondi e il valore predefinito è 2 secondi.Selezionare la casella di controllo **Abilita stato server** per abilitare il server LDAP oppure deselezionarla per disabilitarlo. Il valore predefinito è disattivato.Fare clic su **Applica** per eseguire il commit delle modifiche.Di seguito è riportato un esempio già configurato con queste

informazioni:

| Abe Edit Vew Paverbs Took Help Sage Configuration Perg Logout Refrest CISCO MONITOR VLAN'S CONTROLLER WIRELESS SECURITY MONAGEMENT COMMANDS HELP Security IDAP Serverbas Edit Central * AAA General I General IServer Index I Attribute Server Index I Security Server Index I Server Index I Server Index Server Index I Server Index Server Index I Server Index User Retring Dise Tober ON Oddindepaser,DC=com User Number 389 Server Index Server Mole Server Index I Server Mole None Server Mole None Server Index Server Index Server Index ID Server Index ID Server Index ID Server Index Server Index Server Index ID Server Index Server Index Server Index ID Server Index Server Index AP Folicies Virteless Protection Server Index Server Index | 🗈 wic2006 - Microsoft Inter | met Explorer | | | | | | | | |
|--|---|---|--|---|--|------------------|------------|----------|-------------------------|-------------------------------|
| Cliption Save Configuration Bog Legod Befreit Cisco MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP Security # AA General * RADIDS Accounting * TACACCE Load * Arbitiss | File Edit View Favorites 1 | Tools Help | | | | | | | | A1 |
| CISCO MONITOR WLANE CONTROLLER WIPELESS SECURITY MONAGEMENT COMMANDS HEP Security AAA Omeral Image: Controller Image: Controller Apply * AAA Omeral Server Lindex 1 Server Lindex Image: Controller Apply * RADIUS Authentication Authentication Authentication Controller Server Lindex 1 Server Lindex Apply * Control Server Lindex 1 Server Lindex 1 Server Lindex Apply * Control Server Lindex 1 Server Lindex 1 Server Lindex Apply * Control Server Lindex 1 Server Lindex 1 Server Lindex Apply * Local EAP Server Timeout Imable Server Status Server Timeout Server Status | սիսիս | | | | | | | | nfiguration <u>P</u> ir | ng Logout <u>R</u> efresh |
| Security AAA Goord Acception Acception Babled Clients User Address AC Filen Berker Timeout Berker Status Berker S | CISCO | MONITOR | WLANS | CONTROLLER | W1RELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | |
| | Security C AAA General C AAA Authentication Accounting T TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies P Infority Order ACCESS Centrol Lists Wireless Protection Policies W Web Auth Advanced | LDAP Se Server A Port Num User Bass User Attri User Obje Server M Server Ti Enable Se | rvers > E wdex ddress ber e DN ibute ect Type ode imeout erver Status | sciit 1 10.77 389 OU= SAMJ Perso 30 s | 7.244.198 Idepuser,DC=w IccountName seconds | ireless, DC = co | m | | < Back | Apply |
| Done 🗎 🔮 Internet | Done | | | | | | | | A 4 | Internet |

Ora che i dettagli sul server LDAP sono stati configurati sul WLC, il passo successivo consiste nel configurare LDAP come database backend di priorità in modo che il WLC cerchi innanzitutto le credenziali utente nel database LDAP anziché in qualsiasi altro database.

Configurare LDAP come database backend di priorità

Completare questi passaggi sul WLC per configurare LDAP come database backend di priorità:

 Nella pagina Protezione, fare clic su EAP locale > Priorità di autenticazione. Nella pagina Ordine di priorità > Autenticazione locale è possibile trovare due database (Locale e LDAP) in grado di memorizzare le credenziali dell'utente.Per impostare LDAP come database con priorità, scegliere LDAP dalla casella di sinistra delle credenziali utente e fare clic sul pulsante > per spostare LDAP nella casella di destra dell'ordine di priorità.

| Wic2006 - Microsoft Intern File File View Fewerites Tr | et Explorer vis Help | | | | | | | |
|---|-------------------------|-----------------|----------|----------|------------|----------|---------------------|--------------------|
| ale de | | | | | | Saye Co | viguration <u>P</u> | ing Logout Befresh |
| cisco | | LANS CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | |
| Security | Priority Orde | r > Local-Auth | | | | | | Apply |
| ★ AAA General # RADIUS Authentication Authentication | User Credent | ials | р. | | | | | |
| IN TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies | | < Do | wn | | | | | |
| Local EAP General Profiles PRO-FAST Parameters Auto-FAST Parameters Auto-FAST Parameters Priority Ocdas | | | | | | | | |
| E Access Control Lists | | | | | | | | |
| E Wireless Protection Policies | | | | | | | | |
| I: Web Auth | | | | | | | | |
| E Advanced | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| <i>論</i> | | | | | | | - A (| Internet |

 Questo esempio mostra chiaramente che LDAP è selezionato nella casella laterale sinistra e che il pulsante > è selezionato. Di conseguenza, LDAP viene spostato nella casella sul lato destro che decide la priorità. Il database LDAP viene scelto come database con priorità di autenticazione.Fare clic su Apply

| (Applica). | | | | | | | | | |
|---|--------------|---------------|------------|-----------|----------|------------|----------|------|-------------------------|
| wic2006 - Microsoft Inter | net Explorer | | | | | | | | E 🖻 🛛 |
| File Edit View Favorites T | ools Help | | | | | | | | |
| | | | | | | | | | Ping Logout Befrash |
| CISCO | MONITOR | <u>W</u> LANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | |
| Security | Priority O | rder > Lo | ocal-Auth | | | | | | Apply |
| Ceneral General RADIUS Authentication Accounting TACACS÷ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies | User Cred | entials | | IP IWD | | | | | |
| Local EAP General Profiles EAP-FAST Parameters Authentication Priority | | | | | | | | | |
| E.Priority Order | | | | | | | | | |
| ⊨ Access Control Lists | | | | | | | | | |
| F Wireless Protection Policies | | | | | | | | | |
| E Web Auth | | | | | | | | | |
| F Advanced | | | | | | | | | |
| | | | | | | | | | |
| 4 0 | | | | | | | | | A Internet |
| | | | | | | | | | a arene. |

Nota: se sia LDAP che LOCAL vengono visualizzati nella casella Credenziali utente di destra con LDAP nella parte superiore e LOCAL nella parte inferiore, Local EAP tenta di autenticare i client utilizzando il database backend LDAP e esegue il failover al database utente locale se i server LDAP non sono raggiungibili. Se l'utente non viene trovato, il tentativo di autenticazione verrà rifiutato. Se LOCAL si trova nella parte superiore, EAP locale tenta di

eseguire l'autenticazione utilizzando solo il database degli utenti locale. Non esegue il failover nel database back-end LDAP.

Configurazione della WLAN sul WLC con autenticazione EAP locale

naaaaari

L'ultimo passaggio del WLC è configurare una WLAN che utilizza l'EAP locale come metodo di autenticazione con LDAP come database backend. Attenersi alla procedura seguente:

- Dal menu principale del controller, fare clic su WLAN per passare alla pagina di configurazione delle WLAN. Per creare una nuova WLAN, nella pagina WLAN fare clic su New (Nuova). In questo esempio viene creato un nuovo LDAP WLAN.Fare clic su Apply (Applica). Il passaggio successivo consiste nel configurare i parametri WLAN nella pagina WLAN > Edit (Modifica).
- 2. Nella pagina di modifica della WLAN, abilitare lo stato della WLAN. Configurare tutti gli altri parametri

| necessan. | | | | | | | |
|----------------------------|---|---|---------------------------------|--------------------------------------|--------------------|---------------------|-----------------|
| 🕼 wic2006 - Microsoft Inte | ernet Explorer | | | | | | |
| File Edit View Favorites. | Tools Help | | | | | | |
| - alabe - | | | | | | figuration Eing | Logout Befresh |
| cisco | MONITOR WLANS CO | NTROLLER WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | |
| WLANs | WLANs > Edit | | | | | < Back | Apply |
| - WLANS | General Security | QoS Advanced | | | | | |
| WLANS | | | | | | | |
| E Advanced | Profile Name | Idapuser | | | | | |
| | Туре | WLAN | | | | | |
| | SSID | Idap | | | | | |
| | Status | Enabled | | | | | |
| | Founder Policies | Furna all analytica and | | | | | |
| | Security Policies | (Modifications done under | risecurity tably | vill appear after op | plying the chang | es.) | |
| | | | | | | | |
| | Radio Policy | All 💌 | | | | | |
| | Interface | management 🛩 | | | | | |
| | Broadcast SSID | Enabled | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | Foot Notes | | | | | | |
| | 1 CKIP is not supported t | y 10xx model APs | | | | | |
| | 3 H-REAP Local Switching 4 When obent exclusion is | is not supported with IPsec. enabled, a Timeout Value of | , CRANITE auti of zero means | hendiastion Infinity (will requir | e administrative a | wernide to reset ex | cluded clients) |
| | 5 Client AIPP is not active | unless WPA2 is configured | | | | | |
| | | | | | | | |
| | | | | | | | |
| 10 | | | | | | | |
| 101 | | | | | | 💾 🎱 Iv | ternet. |
| | | | | | | | |

- 3. Per configurare i parametri relativi alla sicurezza per la WLAN, fare clic su Sicurezza. In questo esempio viene utilizzata la sicurezza di layer 2 come 802.1x con WEP dinamico a 104 bit.Nota: questo documento utilizza 802.1x con l'esempio di WEP dinamico. Si consiglia di utilizzare metodi di autenticazione più sicuri, ad esempio WPA/ WPA2.
- 4. Nella pagina Configurazione della sicurezza WLAN, fare clic sulla scheda Server AAA. Nella pagina Server AAA, abilitare il metodo di autenticazione EAP locale e scegliere Idap dall'elenco a discesa corrispondente al parametro Nome profilo EAP. Questo è il profilo EAP locale creato in questo esempio.

| CLSCO MONITOR VLANS CONTROLLER VIRLERS SECURITY MANAGEMENT COMMANDS HELP VLANS VLANS VLANS Security QS Advanced Imply Imply VVLANS VLANS Security QS Advanced Imply Imply VVLANS Security QS Advanced Imply Imply Imply Security QS Advanced Imply | wic2006 - Microsoft Inter File File View Feweries | rnet Explorer | |
|--|--|--|--|
| WLANS WLANS WLANS Commai Security Op Advanced WLANS WLANS AAA Servers AAA Servers Lower 2 AAA Servers Server 2 AAA Servers Server 3 AAA Servers Server 1 None Server 2 None Yes Server 1 None Server 1 None Server 1 None Server 2 None Server 1 None Server 2 None Server 2 Server 1 None Server 2 Server 1 None Server 2 None Server 3 Server 1 None Server 2 Server 1 None Server 1 | alialia cisco | MONITOR WLANS CONTROLLER WIRELESS SECURITY | Sage Configuration Eing Logout Befresh MANAGEMENT COMMANDS HELP |
| | WLANS WLANS WLANS It Advanced | WLANS > Edit General Security QoS Advanced Lover 2 Lover 3 AAA Servers Select AAA servers below to override use of default servers Radius Servers Enabled Server 1 None V Enabled Server 2 None V Enabled Server 3 None V None V Local EAP Authentication Enabled EAP Profile Name Local EAP Authentication Enabled Eap V Local EAP Authentication Enabled Eap V <tr< th=""><th>< Back Apply S on this WLAN LDAP Servers Server None Server None Server None with the server s</th></tr<> | < Back Apply S on this WLAN LDAP Servers Server None Server None Server None with the server s |

5. Selezionare il server LDAP (precedentemente configurato sul WLC) dalla casella a discesa. Verificare che il server LDAP sia raggiungibile dal WLC.Fare clic su **Apply** (Applica).

| wic2006 - Microsoft Intern | net Explorer | 26 |
|-------------------------------------|---|----------------------------|
| uludu cisco | Save Configuration <u>P</u> i MONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY MANAGEMENT C <u>O</u> MMANDS HELP | ng Logout <u>R</u> efr |
| VLANs WLANs WLANs Advanced | WLANS > Edit < Back | Apply |

6. Il nuovo Idap WLAN è stato configurato sul WLC. Questa WLAN autentica i client con l'autenticazione EAP locale (in questo caso EAP-FAST) ed esegue query su un database backend LDAP per la convalida delle credenziali client.

| wic2006 - Microsoft Inte | ernet Explorer | | | | | | |
|--------------------------|----------------|----------------|-----------------|--------------|-----------------|-----------------------------|----------------------|
| File Edit View Favorites | Tools Help | | | | | | 4 |
| ahaha Cisco | MONITOR WEAR | CONTROLLER WIT | | MANAGEMENT (| Save Centig | iuration Eing Logi Ici o | ut i <u>B</u> efresi |
| CISCO | BOULLOK WORKS | CONTROLLER W1 | Recess geoordin | Manadement (| -Onimetrico L | (CD) | _ |
| WLANS | WLANs | | | | | Nev | v |
| WLANS WLANS | Profile Name | Туре | WLAN SSID | Adm | nin tus Secu | rity Policies | |
| Advanced | Tawee | WLAN | TSWED | Enal | Hed (WPA | 2][Auth(002.1×)] | • |
| | Idepuser | WLAN | ldep | Enab | oled 002.5 | LX | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| Done | | | | | | 🙆 🍲 Internet | |

Configura server LDAP

Ora che il protocollo EAP locale è stato configurato sul WLC, il passaggio successivo consiste nel configurare il server LDAP che funge da database back-end per autenticare i client wireless al completamento della convalida del certificato.

Il primo passo nella configurazione del server LDAP consiste nel creare un database utenti sul server LDAP in modo che il WLC possa eseguire query su questo database per autenticare l'utente.

Creazione di utenti nel controller di dominio

In questo esempio viene creato un nuovo **Idapuser** dell'unità organizzativa e l'utente **user2** viene creato in questa unità organizzativa. Configurando l'utente per l'accesso LDAP, il WLC può eseguire query in questo database LDAP per l'autenticazione utente.

Il dominio utilizzato in questo esempio è wireless.com.

Creazione di un database utenti in un'unità organizzativa

In questa sezione viene illustrato come creare una nuova unità organizzativa nel dominio e creare un nuovo utente in questa unità organizzativa.

1. Nel controller di dominio fare clic su Start > Programmi > Strumenti di amministrazione > Utenti e computer di Active Directory per avviare la console di gestione Utenti e computer di Active Directory.

 Fare clic con il pulsante destro del mouse sul nome di dominio (wireless.com, in questo esempio), quindi selezionare Nuovo > Unità organizzativa dal menu di scelta rapida per creare una nuova unità



3. Assegnare un nome all'unità organizzativa e fare clic su OK.

| New Object | - Organiza | tional Unit | | X |
|----------------|------------|---------------|----|--------|
| S | Create in: | Wireless.com/ | | |
| N <u>a</u> me: | | | | |
| Idapuser | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | OK | Cancel |

Ora che il nuovo **ldapuser** dell'unità organizzativa è stato creato sul server LDAP, il passaggio successivo consiste nel creare l'utente **user2** in questa unità organizzativa. A tale scopo, effettuare i seguenti passaggi:

1. Fare clic con il pulsante destro del mouse sulla nuova unità organizzativa. Per creare un nuovo utente, selezionare **Nuovo > Utente** dai menu di scelta rapida risultanti.



 Nella pagina Impostazione utente, compilare i campi obbligatori come illustrato in questo esempio. In questo esempio, il nome di accesso dell'utente è user2.Questo è il nome utente che verrà verificato nel database LDAP per l'autenticazione del client. In questo esempio vengono utilizzati il nome e il cognome abcd. Fare clic su Next (Avanti).

| New Object - User | × |
|-------------------------------------|-----|
| Create in: Wireless.com/Idapuser | |
| Eirst name: abcd Initials: | |
| Last name: | |
| Full name: abcd | |
| gser logon name: | |
| user2 @Wireless.com | |
| User logon name (pre-Windows 2000): | |
| WIRELESS\ user2 | |
| | |
| < Back Next > Cance | ы [|

3. Immettere una password e confermarla. Selezionare l'opzione **Nessuna scadenza password** e fare clic su

| Password: | | | |
|-------------------|------------------|-----------|---|
| Confirm password: | | | _ |
| User must chan | ge password at n | ext logon | |
| User cannot ch | ange password | | |
| Password neve | expires | | |
| Account is disal | oled | | |

 Fare clic su Finish (Fine). Un nuovo utente user2 viene creato nell'utente LDAP dell'unità organizzativa. Credenziali utente: nome utente: user2password: notebook123



Dopo aver creato l'utente in un'unità organizzativa, il passaggio successivo consiste nel configurare l'utente per l'accesso LDAP.

Configurare l'utente per l'accesso LDAP

Eseguire la procedura descritta in questa sezione per configurare un utente per l'accesso LDAP.

Attivare la funzione di binding anonimo su Windows 2003 Server

Affinché le applicazioni di terze parti possano accedere a Windows 2003 AD sul server LDAP, è necessario attivare la funzione di binding anonimo su Windows 2003. Per impostazione predefinita, le operazioni LDAP anonime non sono consentite nei controller di dominio di Windows 2003.

Per abilitare la funzione di binding anonimo, effettuare le operazioni riportate di seguito.

- 1. Avviare lo strumento di **modifica ADSI** dalla posizione Start > Esegui > Tipo: **ADSI Edit.msc**. Questo strumento fa parte degli strumenti di supporto di Windows 2003.
- Nella finestra Modifica ADSI, espandere il dominio radice (Configuration [tsweblapt.Wireless.com]).Espandere CN=Servizi > CN=Windows NT > CN=Servizio directory. Fare clic con il pulsante destro del mouse sul contenitore CN=Directory Service e selezionare proprietà dal menu di scelta rapida.



3. Nella finestra CN=Directory Service Properties, fare clic sull'attributo dsHeuristics sotto il campo Attribute e scegliere Modifica. Nella finestra Editor attributi stringa di questo attributo, immettere il valore 0000002, quindi fare clic su Applica e OK. La funzionalità di binding anonimo è attivata nel server Windows 2003.Nota: l'ultimo (settimo) carattere controlla il modo in cui è possibile eseguire l'associazione al servizio LDAP. "0" o nessun settimo carattere indica che le operazioni LDAP anonime sono disabilitate. Se si imposta il settimo carattere su "2", viene attivata la funzione di associazione anonima.

| CN=Directory Service Pr | operties | | ? X | | |
|-------------------------------------|--------------------------|--------------------|-------|-----------|----------|
| Attribute Editor Security | 1 | | | Class | Distingu |
| Show mandatory attri | ibutes | | | concanter | 01-00 |
| Show optional attribu | ites | | | | |
| Show only attributes | that have <u>v</u> alues | | | | |
| Attributes: | | | | | |
| Attribute | Syntax | Value | ▲ | | |
| directReports | String Attrib | ute Editor | | | × |
| displayName displayNamePrintable | Attribute: dSF | Heuristics | | | |
| dSASignature | ⊻alue: | | | | |
| dSCorePropagationD | 0000002 | | | | |
| extensionName flags fromEntry | Clear | | Ç | ок | Cancel |
| frsComputerReferenc | Distinguished | <not set=""></not> | | | |
| fRSMemberReferenc | Distinguished | <not set=""></not> | -1 | | |
| | Distribuished | (not set | | | |
| Edit | | | | | |
| | OK | Cancel | Apply | | |

Nota: se questo attributo contiene già un valore, assicurarsi di modificare solo il settimo carattere da sinistra. Questo è l'unico carattere da modificare per abilitare le associazioni anonime. Ad esempio, se il valore corrente è "0010000", sarà necessario modificarlo in "0010002". Se il valore corrente è inferiore a sette caratteri, sarà necessario inserire degli zeri nelle posizioni non utilizzate: "001" diventerà "0010002".

Concessione dell'accesso ANONIMO all'utente "user2"

Il passaggio successivo consiste nel concedere l'accesso **ANONIMO** all'utente **user2**. A tale scopo, completare i seguenti passaggi:

- 1. Aprire Utenti e computer di Active Directory.
- 2. Accertarsi che l'opzione Visualizza funzioni avanzate sia selezionata.
- Individuare l'utente user2 e fare clic con il pulsante destro del mouse su di esso. Selezionare Proprietà dal menu di scelta rapida. Questo utente è identificato dal nome "abcd".

| 🖃 🔤 🖬 useri | | |
|-------------|--|----------|
| | | |
| | <u>C</u> opy Add to a group Name Mappings Disable Account | |
| | Mo <u>v</u> e Open Home Page | |
| | Send M <u>a</u> il Find | |
| | All Tas <u>k</u> s | <u>•</u> |
| | <u>v</u> jew New <u>W</u> indow from Here | - |
| | Cu <u>t</u> Delete | |
| | Rena <u>m</u> e Refresh | |
| R / | Export List | |
| 💽 us | P <u>r</u> operties | |
| i 🕵 alas | Help | |
| (| | |

4. Passare alla sezione Protezione nella finestra Proprietà -

| d. cd Properties | |
|--|---|
| Published Certificates Environment Session General Address | Member Of Dial-in Object Security Bemote control Terminal Services Profile. COM Account Profile Telephones Organization |
| 🛃 abcd | |
| <u>F</u> irst name: | abcd Initials: |
| Last name: | |
| Digplay name: | abcd |
| Description: | |
| Offi <u>c</u> e: | 1 |
| <u>I</u> elephone number: | <u>O</u> ther |
| E- <u>m</u> ail: | [|
| Web page: | Other |
| | |
| | OK Cancel Apply |

- 5. Fare clic su Add nella finestra risultante.
- 6. Immettere ACCESSO ANONIMO nella casella Immettere i nomi degli oggetti da selezionare e confermare la finestra di dialogo.

| <u>?×</u> |
|--------------|
| |
| Object Types |
| |
| Locations |
| |
| Check Names |
| |
| |
| K Cancel |
| |

7. Nell'ACL, si noterà che **ANONYMOUS LOGON** ha accesso ad alcuni set di proprietà dell'utente. Fare clic su **OK**. Accesso ANONIMO concesso all'utente

| ocd Properties | | 22 |
|--|---|---|
| Environment Sessions Remote control General Address Account Profi Published Certificates Member Of | Terminal Service le Telephones Dial-in Obje | es Profile COM+ Organization ect Security |
| Group or user names: | | |
| Account Operators (WIRELESS Ac Administrators (WIRELESS Adminis | count Operators) trators) | |
| ANONYMOUS LOGON | | |
| Cert Publishers (WIRELESS\Cert Publishers | ublishers) | - |
| | Add | <u>R</u> emove |
| Permissions for ANONYMOUS LOGON | Allow | Deny |
| Full Control | | |
| Read | | |
| Create All Child Objects | H | |
| Delete All Child Objects | | |
| Allowed to Authenticate | | |
| For special permissions or for advanced s click Advanced. | ettings, | Advanced |
| ОК | Cancel | |

Concessione dell'autorizzazione Contenuto elenco per l'unità organizzativa

Il passaggio successivo consiste nel concedere almeno l'autorizzazione **Elenco contenuti** all'**ACCESSO ANONIMO** nell'unità organizzativa in cui si trova l'utente. In questo esempio, "user2" si trova sull'unità organizzativa "Idapuser". A tale scopo, completare i seguenti passaggi:

1. In Utenti e computer di Active Directory fare clic con il pulsante destro del mouse sul

Idapuser dell'unità organizzativa e scegliere **Proprietà**.



2. Fare clic su **Protezione** e quindi su **Avanzate**.

| apuser Properties | | ? |
|--|---------------|---------------|
| General Managed By Object Security C | OM+ Group F | Policy |
| Group or user names: | | |
| Account Operators (WIRELESS Account | nt Operators) | ^ |
| Administrators (WIRELESS \Administrato | rs) | |
| 🚮 Authenticated Users | | |
| 🗾 👧 Domain Admins (WIRELESS\Domain Ad | dmins) | |
| Enterprise Admins (WIRELESS\Enterprise) | se Admins) | -1 |
| | 10 A | |
| | Add | <u>Remove</u> |
| Permissions for Account Operators | Allow | Deny |
| Full Control | | |
| Read | | |
| Write | | |
| Create All Child Objects | | |
| Delete All Child Objects | | |
| Generate Resultant Set of Policy(Logging) | | |
| For special permissions or for advanced setting click Advanced. | gs, 🧲 | Advanced |
| ОК | Cancel | Apply |

3. Fare clic su Add. Nella finestra di dialogo visualizzata immettere ACCESSO ANONIMO.

| Advanced Security Settings for Idapuser | |
|---|--------------|
| Select User, Computer, or Group | <u>? ×</u> |
| Select this object type: | |
| User, Group, or Built-in security principal | Object Types |
| From this location: | |
| Wireless.com | Locations |
| Enter the object name to select (examples): | |
| ANONYMOUS LOGON | Check Names |
| | |
| | |
| Advanced | Cancel |

- 4. Riconosci il dialogo. Verrà aperta una nuova finestra di dialogo.
- 5. Nella casella di riepilogo a discesa **Applica a** selezionare **Solo questo oggetto** e selezionare la casella di controllo Consenti **contenuto elenco**.

| Permission Entry for Idapuser | | 1 | Ľ |
|---|-------|----------------|---|
| Object Properties | | | |
| Name: ANONYMOUS LOGON | | <u>C</u> hange | 1 |
| Apply onto: This object only | | - | |
| Permissions: | Allow | Deny | _ |
| Full Control List Contents Read All Properties Write All Properties Delete Delete Subtree Read Permissions Modify Permissions Modify Owner All Validated Writes All Extended Rights Create All Child Objects Delete Subtree Read Permissions to objects a containers within this container only | | | |
| | οκ | Cancel | |

Utilizzo di LDP per identificare gli attributi utente

Questo strumento GUI è un client LDAP che consente agli utenti di eseguire operazioni (come la connessione, il binding, la ricerca, la modifica, l'aggiunta e l'eliminazione) su qualsiasi directory compatibile con LDAP, come Active Directory. LDP viene utilizzato per visualizzare gli oggetti archiviati in Active Directory insieme ai relativi metadati, ad esempio i descrittori di protezione e i metadati di replica.

Lo strumento LDP GUI è incluso quando si installano gli strumenti di supporto di Windows Server 2003 dal CD del prodotto. In questa sezione viene illustrato l'utilizzo dell'utilità LDP per identificare gli attributi specifici associati all'utente **user2**. Alcuni di questi attributi vengono utilizzati per compilare i parametri di configurazione del server LDAP sul WLC, ad esempio il tipo di attributo utente e il tipo di oggetto utente.

- 1. Sul server Windows 2003 (anche sullo stesso server LDAP), fare clic su **Start > Esegui** e immettere **LDP** per accedere al browser LDP.
- Nella finestra principale di LDP, fare clic su Connessione > Connetti e connettersi al server LDAP immettendo l'indirizzo IP del server LDAP.

| i Ldp | _ 🗆 🗵 |
|--|-------|
| Connection Browse View Options Utilities | Help |
| Connect Bind Cbrl+B Disconnect Disconnect <td>*</td> | * |
| Save As | |
| Print Print Pregiew Pgint Setup | |
| Egt | |
| | X |
| Connect to specified server | |

3. Una volta connessi al server LDAP, selezionare **Visualizza** dal menu principale e fare clic su **Albero**.

| Idap://tsweb-lapt.Wireless.com/EC=Wireless,DC=com | |
|--|--|
| Connection Browse View Options Utilities | Ba |
| Ince Ctrl+T Enterprise Configuration ✓ Status Bar Set Eont | <pre>1.2.840.113556.1.4.473; 1.2.840.113556.1.4.528; 1.2.840.113556.1.4.417; 1.2.840.113556.1.4.613; 1.2.840.113556.1.4.841; 1.2.840.113556.1.4.523; 1.2.840.113556.1.4.805; 1.2.840.113556.1.4.474; 1.2.840.113556.1.4.1339; 1.2.840.113556.1.4.1340; 1.2.840.113556.1.4.474; 1.2.840.113556.1.4.1339; 1.2.840.113556.1.4.1340; 1.2.840.113556.1.4.1504; 1.2.840.113556.1.4.1952; 1.2.840.113556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1952; 1.2.840.113556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1952; 1.2.840.113556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1948; 2) supportedLDAPVersion: 3; 2; 1.2 supportedSASLMechanisms: GSSAPU; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 1.2 domsiftedUSN: 16926; 4.3 supportedSASLMechanisms: GSSAPU; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 1.2 ldapServiceName: Wireless.com; 1.3 ldapServiceName: Wireless.com; 1.3 ldapServiceName: CN=TSWEB-LAPT,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration ,DC=Wireless,DC=com; 3.3 supportedCapabilities: 1.2.840.113556.1.4.800; 1.2.840.113556.1.4.1670; 1.2.840.113556.1.4.1791; 1.3 isGlobalCatalogReady: TRUE; 1.3 isGlobalCatalogReady: TRUE; 1.4 isdmainControllerFunctionality: 2 = (DS_BEHAVIOR_WIN2000]; 1.5 i</pre> |
| | |

 Nella finestra Visualizzazione struttura risultante, immettere il nome distinto di base dell'utente. In questo esempio, l'utente 2 si trova nell'unità organizzativa "Idapuser" nel dominio Wireless.com. Il nome di dominio di base per l'utente user2 è OU=Idapuser, dc=wireless, dc=com. Fare clic su OK.

| Midap://tsweb-lapt.Wireless.com/DC=Wireless,DC=com | | - 🗆 🗵 |
|---|---|-----------------|
| Connection Browse View Options Utilities | | Help |
| Tree View BaseDN: DU-Idapuser.do-wireless.do-com Cancel | X 3556.1.4.473; 1.2.840.113556.1.4.528; 1.2.840.113556.1.4.417; 13556.1.4.619; 1.2.840.113556.1.4.841; 1.2.840.113556.1.4.529; 13556.1.4.805; 1.2.840.113556.1.4.621; 1.2.840.113556.1.4.1339; 13556.1.4.1330; 1.2.840.113556.1.4.474; 1.2.840.113556.1.4.1339; 13556.1.4.1340; 1.2.840.113556.1.4.41413; 2.16.840.1.113730.3.4.9; 1.113730.3.4.10; 1.2.840.113556.1.4.1504; 1.2.840.113556.1.4.1852; 13556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1852; 13556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1948; 2> supportedLDAPVersion: 3; 2; 12> supportedLDAPVersion: 3; 2; 13> highestCommittedUSN: 16926; 4> supportedSASLMechanisms: GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 1> dnsHostName: tsweb-lapt.Wireless.com; 1> ldapServiceName: Wireless.com; 1> ldapServiceName: Wireless.com; 1> ldapServiceName: Wireless.com; 3> supportedCapabilities: 1.2.840.113556.1.4.800; 1.2.840.113556.1.4. 1.2.840.113556.1.4.1791; 1> isSinchronized: TRUE; 1> isGlobalCatalogReady: TRUE; 1> isGlobalCatalogReady: TRUE; 1> domainFunctionality: 0 = [DS_BEHAVIOR_WIN2000]; 1> forestFunctionality: 0 = [DS_BEHAVIOR_WIN2000]; 1> domainControllerFunctionality: 2 = [DS_BEHAVIOR_WIN2003]; | ration 1670; |
| Ready | | 1. |

5. Sul lato sinistro del browser LDP viene visualizzata l'intera struttura sotto il nome di dominio di base specificato (OU=Idapuser, dc=wireless, dc=com). Espandere la struttura ad albero per individuare l'utente user2. Questo utente può essere identificato con il valore CN che rappresenta il nome dell'utente. Nell'esempio, questo valore è CN=abcd. Fare doppio clic su CN=abcd. Nel riquadro a destra del browser LDP, LDP visualizzerà tutti gli attributi associati all'utente 2. Questo esempio spiega questo passo:



In questo esempio, osservare i campi circondati a destra.

- 6. Come indicato nella sezione <u>Configurazione WLC con dettagli del server LDAP</u> di questo documento, nel campo Attributo utente immettere il nome dell'attributo nel record utente che contiene il nome utente.Da questo output LDP, è possibile vedere che sAMAccountName è un attributo che contiene il nome utente "user2". Pertanto, immettere l'attributo sAMAccountName che corrisponde al campo Attributo utente sul WLC.
- 7. Nel campo Tipo oggetto utente, immettere il valore dell'attributo objectType LDAP che identifica il record come utente. I record utente dispongono spesso di diversi valori per l'attributo objectType, alcuni dei quali sono univoci per l'utente e altri sono condivisi con altri tipi di oggetto.Nell'output LDP, CN=Person è un valore che identifica il record come utente. Pertanto, specificare Person come attributo User Object Type sul WLC.

Configura client wireless

L'ultimo passaggio consiste nel configurare il client wireless per l'autenticazione EAP-FAST con certificati client e server. A tale scopo, completare i seguenti passaggi:

 Avviare Cisco Aironet Desktop Utility (ADU). Per creare un nuovo profilo client wireless, nella finestra principale di ADU fare clic su Gestione profili > Nuovo.

| 🕾 Cisco Aironet Desktop U | ility - Current Profile: sdreteretet | ? 🛛 |
|--------------------------------|--------------------------------------|----------------|
| Action Options Help | | |
| Current Status Profile Manager | Diagnostics | |
| Sdreteretet | | New |
| | | Modify |
| | | Remove |
| | | Activate |
| ∠ Details | | |
| Network Type: | Infrastructure | Import |
| Security Mode: | Disabled | |
| Network Name 1 (SSID1): | teert | Export |
| Network Name 2 (SSID2): | <empty></empty> | Scan |
| Network Name 3 (SSID3): | <empty></empty> | Scart |
| Auto Select Profiles | | Order Profiles |
| | | |

2. Specificare un nome di profilo e assegnare un nome SSID a questo profilo. Questo nome SSID deve essere lo stesso configurato sul WLC. In questo esempio, il nome SSID è

| Profile Settir | Profile Name: Client Name: | Idapuser CLIENT1 | |
|----------------|-------------------------------|---------------------|--|
| - Network Na | ssiD1 ssiD2: ssiD3 | ldap | |
| | 00100. | | |

- 3. Fare clic sulla scheda **Security** (Protezione) e scegliere **802.1x/EAP** come protezione di livello 2. Scegliere **EAP-FAST** come metodo EAP e fare clic su **Configura**.
- 4. Nella pagina di configurazione di EAP-FAST, scegliere **Certificato client TLS** dall'elenco a discesa Metodo di autenticazione EAP-FAST e fare clic su **Configura**.

| Configure EAP-FAST | ? 🔀 |
|--|-----------|
| EAP-FAST Authentication Method | |
| MSCHAPv2 User Name and Password | Configure |
| GTC Token/Password | |
| TLS Client Certificate | |
| Select One or More PAC Authorities | 1 |
| | Manage |
| | |
| | |
| | |
| | |
| Use Any PAC Belonging to the Same Group | |
| Allow Automatic PAC Provisioning | |
| | |
| | |
| Use Machine Information for Domain Logon | |
| | |
| No Network Connection Unless User Is Logged In | |
| | |
| | DK Cancel |

5. Nella finestra Configurazione certificato client TLS:Selezionare la casella di controllo Convalida identità server e selezionare il certificato CA installato nel client (illustrato nella sezione <u>Generazione del certificato CA radice per il client</u> di questo documento) come Autorità di certificazione radice attendibile.Selezionare il certificato del dispositivo installato sul client (come illustrato nella sezione <u>Generazione di un certificato del dispositivo per il</u> <u>client</u> di questo documento) come certificato del client.Fare clic su OK.Questo esempio spiega questo

| ✓ Validate Server Identity | |
|--|---|
| Trusted Root Certification Authorities | |
| wireless | ~ |
| Select a Certificate | |
| 1234 [Issued by: wireless 1/26/2008] | ~ |
| Server/Domain Name | |
| Wireless.com | |
| Login Name | |
| user2 | |
| | |

Viene creato il profilo client wireless.

Verifica

Per verificare che la configurazione funzioni correttamente, attenersi alla seguente procedura.

1. Attivare il SSID **Idap** sull'ADU.

 Fare clic su Sì o OK come richiesto nelle finestre successive. Per avere successo nell'ADU, dovrebbe essere possibile visualizzare tutti i passaggi dell'autenticazione client e dell'associazione.

Per verificare che la configurazione funzioni correttamente, consultare questa sezione. Usare la modalità CLI del WLC.

 Per verificare se il WLC è in grado di comunicare con il server LDAP e individuare l'utente, specificare il comando debug aaa Idap enable dalla CLI del WLC. In questo esempio viene illustrato un processo LDAP di comunicazione riuscito:Nota: parte dell'output di questa sezione è stato spostato su altre righe per motivi di spazio.(Cisco Controller) >debug aaa Idap enable

```
Sun Jan 27 09:23:46 2008: AuthenticationReguest: 0xba96514
Sun Jan 27 09:23:46 2008:
                         Callback.....0x8
344900
Sun Jan 27 09:23:46 2008:
                            protocolType.....0x0
0100002
Sun Jan 27 09:23:46 2008:
                            proxyState.....00:
40:96:AC:E6:57-00:00
Sun Jan 27 09:23:46 2008:
                            Packet contains 2 AVPs (not shown)
Sun Jan 27 09:23:46 2008: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to INIT
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_bind (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to CONNECTED
Sun Jan 27 09:23:46 2008: LDAP server 1 now active
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: UID Search (base=OU=ldapuser, DC=wireless,
DC=com, pattern=(&(objectclass=Person)(sAMAccountName=user2)))
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: Returned msg type 0x64
Sun Jan 27 09:23:46 2008: ldapAuthRequest [1] called lcapi_query base="OU=ldapus
er, DC=wireless, DC=com" type="Person" attr="sAMAccountName" user="user2" (rc = 0
- Success)
Sun Jan 27 09:23:46 2008: LDAP ATTR> dn = CN=abcd,OU=ldapuser,DC=Wireless,DC=com
 (size 38)
Sun Jan 27 09:23:46 2008: Handling LDAP response Success
```

Dalle informazioni evidenziate in questo output di debug, è chiaro che il WLC esegue una query sul server LDAP con gli attributi utente specificati sul WLC e che il processo LDAP ha esito positivo.

 Per verificare se l'autenticazione EAP locale ha esito positivo, specificare il comando debug aaa local-auth eap method events enable dalla CLI del WLC. Di seguito è riportato un esempio:(Cisco Controller) >debug aaa local-auth eap method events enable Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: New context

```
(EAP handle = 0x1B000009)
```

Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: Allocated new EAP-FAST context
(handle = 0x22000009)

```
Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)
```

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Received Identity

Sun Jan 27 09:38:28 2008: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV (436973636f00000000000000000000)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Sending Start

Sun Jan 27 09:38:29 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Start

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Local certificate found Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: TLS_DHE_RSA_AES_128_CEC_SHA proposed... Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Proposed ciphersuite(s): Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CEC_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_AES_128_CEC_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_AES_128_CEC_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_RC4_128_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Selected ciphersuite: Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CEC_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Selected ciphersuite: Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CEC_SHA

Sun Jan 27 09:38:29 2008: eap_fast_crypto.c-EVENT: Starting Diffie Hellman phase 1 ...

Sun Jan 27 09:38:30 2008: eap_fast_crypto.c-EVENT: Diffie Hellman phase 1 complete

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Sent provisioning Server Hello

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Certificate handshake Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 1 to chain Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 2 to chain Sun Jan 27 09:38:32 2008: eap fast.c-EVENT: Successfully validated received certificate Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Rx'd I-ID: "EAP-FAST I-ID" from Peer Cert Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Key Exchange handshake Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT: Starting Diffie Hellman phase 2 ... Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT: Diffie Hellman phase 2 complete. Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Certificate Verify handshake Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT: Sign certificate verify succeeded (compare) Anche il comando debug aaa local-auth db enable è molto utile. Di seguito è riportato un esempio:(Cisco Controller) >debug aaa local-auth db enable Sun Jan 27 09:35:32 2008: LOCAL_AUTH: EAP: Received an auth request Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Creating new context Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Local auth profile name for context 'ldapuser' Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Created new context eap session handle fb000007 Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet (id 2) to EAP subsys Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found matching context for id - 8 Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP) Sending user credential request username 'user2' to LDAP Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found context matching MAC address - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet (id 12) to EAP subsys
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8 Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) ---> [KEY AVAIL] send_len 64, recv_len 0 Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) received keys waiting for success Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8 Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8 Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event

 Per visualizzare i certificati installati nel WLC da utilizzare per l'autenticazione locale, usare il comando show local-auth certificates dalla CLI del WLC. Di seguito è riportato un esempio:(Cisco Controller) >mostra certificati di autenticazione locale Certificates available for Local EAP authentication:

Certificate issuer vendor CA certificate: Subject: DC=com, DC=Wireless, CN=wireless Issuer: DC=com, DC=Wireless, CN=wireless Valid: 2008 Jan 23rd, 15:50:27 GMT to 2013 Jan 23rd, 15:50:27 GMT Device certificate: Subject: 0=cisco, CN=ciscowlc123 Issuer: DC=com, DC=Wireless, CN=wireless Valid: 2008 Jan 24th, 12:18:31 GMT to 2010 Jan 23rd, 12:18:31 GMT Certificate issuer cisco CA certificate: Subject: 0=Cisco Systems, CN=Cisco Manufacturing CA Issuer: 0=Cisco Systems, CN=Cisco Root CA 2048 Valid: 2005 Jun 10th, 22:16:01 GMT to 2029 May 14th, 20:25:42 GMT Device certificate:

Not installed.

 Per visualizzare la configurazione dell'autenticazione locale sul WLC dalla modalità CLI, usare il comando show local-auth config. Di seguito è riportato un esempio:(Cisco Controller) >show local-auth config

User credentials database search order:

| Primary | | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | | Ι | JD. | A | Ρ |
|---------|--|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|--|---|-----|---|---|
|---------|--|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|--|---|-----|---|---|

| Timer: | |
|-----------------------------------|-------------------|
| Active timeout 3 | 300 |
| Configured EAP profiles: | |
| Name 1 | ldapuser |
| Certificate issuer v | vendor |
| Peer verification options: | |
| Check against CA certificates E | Enabled |
| Verify certificate CN identity I | Disabled |
| Check certificate date validity I | Disabled |
| EAP-FAST configuration: | |
| Local certificate required Y | les |
| Client certificate required Y | les |
| Enabled methods f | fast |
| Configured on WLANs 2 | 2 |
| | |
| EAP Method configuration: | |
| EAP-FAST: | |
| More or (q)uit | |
| Server key < | <hidden></hidden> |
| TTL for the PAC 1 | LO |
| Anonymous provision allowed N | No. |
| | |
| | |
| Authority Information C | Cisco A-ID |

Risoluzione dei problemi

Per risolvere i problemi relativi alla configurazione, è possibile utilizzare i seguenti comandi:

- debug aaa local-auth eap method events enable
- debug aaa all enable

abilitazione pacchetto debug dot1x

Informazioni correlate

- Esempio di autenticazione EAP-FAST con i controller LAN wireless e la configurazione del server RADIUS esterno
- PEAP in Unified Wireless Networks con Microsoft Internet Authentication Service (IAS)
- Esempio di configurazione del mapping delle VLAN dinamiche con WLC basati su ACS ad <u>Active Directory</u>
- Guida alla configurazione di Cisco Wireless LAN Controller Configurazione delle soluzioni di sicurezza
- Guida alla configurazione di Cisco Wireless LAN Controller Gestione del software e delle configurazioni dei controller
- Esempio di configurazione dell'autenticazione EAP con i controller WLAN (WLC)
- Domande frequenti sul design e le caratteristiche del controller WLC (Wireless LAN Controller)
- <u>Cisco Secure Services Client con autenticazione EAP-FAST</u>
- Domande frequenti sui Wireless LAN Controller (WLC)
- Domande frequenti sui controller WLC (Wireless LAN Controller) e sui messaggi di sistema
- 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).