Configurazione dell'autenticazione EAP con i controller WLAN (WLC)

Sommario

Introduzione

In questo documento viene spiegato come configurare il controller WLC (Wireless LAN Controller) per l'autenticazione EAP (Extensible Authentication Protocol) con l'utilizzo di un server RADIUS esterno. In questo esempio di configurazione viene utilizzato Cisco Secure Access Control Server (ACS) come server RADIUS esterno per convalidare le credenziali dell'utente.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenze base della configurazione dei Lightweight Access Point (AP) e dei Cisco WLC.
- Conoscenze base di LWAPP (Lightweight AP Protocol).
- Informazioni su come configurare un server RADIUS esterno come Cisco Secure ACS.

Componenti usati

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

- Cisco Aironet serie 1232AG Lightweight AP
- Cisco serie 4400 WLC con firmware 5.1
- Cisco Secure ACS con versione 4.1
- Cisco Aironet 802.11 a/b/g Client Adapter
- Cisco Aironet Desktop Utility (ADU) con firmware 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

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione

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

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Completare questa procedura per configurare i dispositivi per l'autenticazione EAP:

1. Configurare il WLC per il funzionamento di base e registrare i Lightweight AP sul controller.
2. Configurare il WLC per l'autenticazione RADIUS tramite un server RADIUS esterno.
3. Configurare i parametri WLAN.
4. Configurare Cisco Secure ACS come server RADIUS esterno e creare un database utenti per l'autenticazione dei client.

Esempio di rete

In questa configurazione, i Cisco 4400 WLC e i Lightweight AP sono connessi tramite un hub. Allo stesso hub è collegato anche un server RADIUS esterno (Cisco Secure ACS). Tutti i dispositivi si trovano nella stessa subnet. L'access point è inizialmente registrato sul controller. È necessario configurare il WLC e l'access point per l'autenticazione LEAP (Lightweight Extensible Authentication Protocol). I client che si connettono al punto di accesso utilizzano l'autenticazione LEAP per associarsi al punto di accesso. Cisco Secure ACS viene usato per eseguire l'autenticazione RADIUS.

Configurare il WLC per il funzionamento di base e registrare i Lightweight AP sul controller

Per configurare il WLC per il funzionamento di base, usare la configurazione guidata di avvio sull'interfaccia della riga di comando (CLI). In alternativa, è possibile usare la GUI per configurare il WLC. Questo documento spiega la configurazione sul WLC con la configurazione guidata di avvio sulla CLI.

Una volta avviato per la prima volta, il WLC entra direttamente nella configurazione guidata di avvio. Utilizzare la configurazione guidata per configurare le impostazioni di base. È possibile eseguire la procedura guidata dalla CLI o dalla GUI. Questo output mostra un esempio della configurazione guidata di avvio nella CLI:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC-1
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.77.244.204
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 10.77.244.220
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.77.244.220
AP Manager Interface IP Address: 10.77.244.205
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.77.244.220):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Test
Network Name (SSID): Cisco123
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configuration saved!
Resetting system with new configuration..
```

Questi parametri configurano il WLC per il funzionamento di base. Nell'esempio di configurazione, il WLC usa **10.77.244.204** come indirizzo IP dell'interfaccia di gestione e **10.77.244.205** come indirizzo IP dell'interfaccia del gestore dell'access point.

Prima di poter configurare altre funzionalità sui WLC, i Lightweight AP devono registrarsi sul WLC. in questo documento si presume che il Lightweight AP sia registrato sul WLC. Per ulteriori informazioni su come i Lightweight AP si registrano sul WLC, fare riferimento alla registrazione di

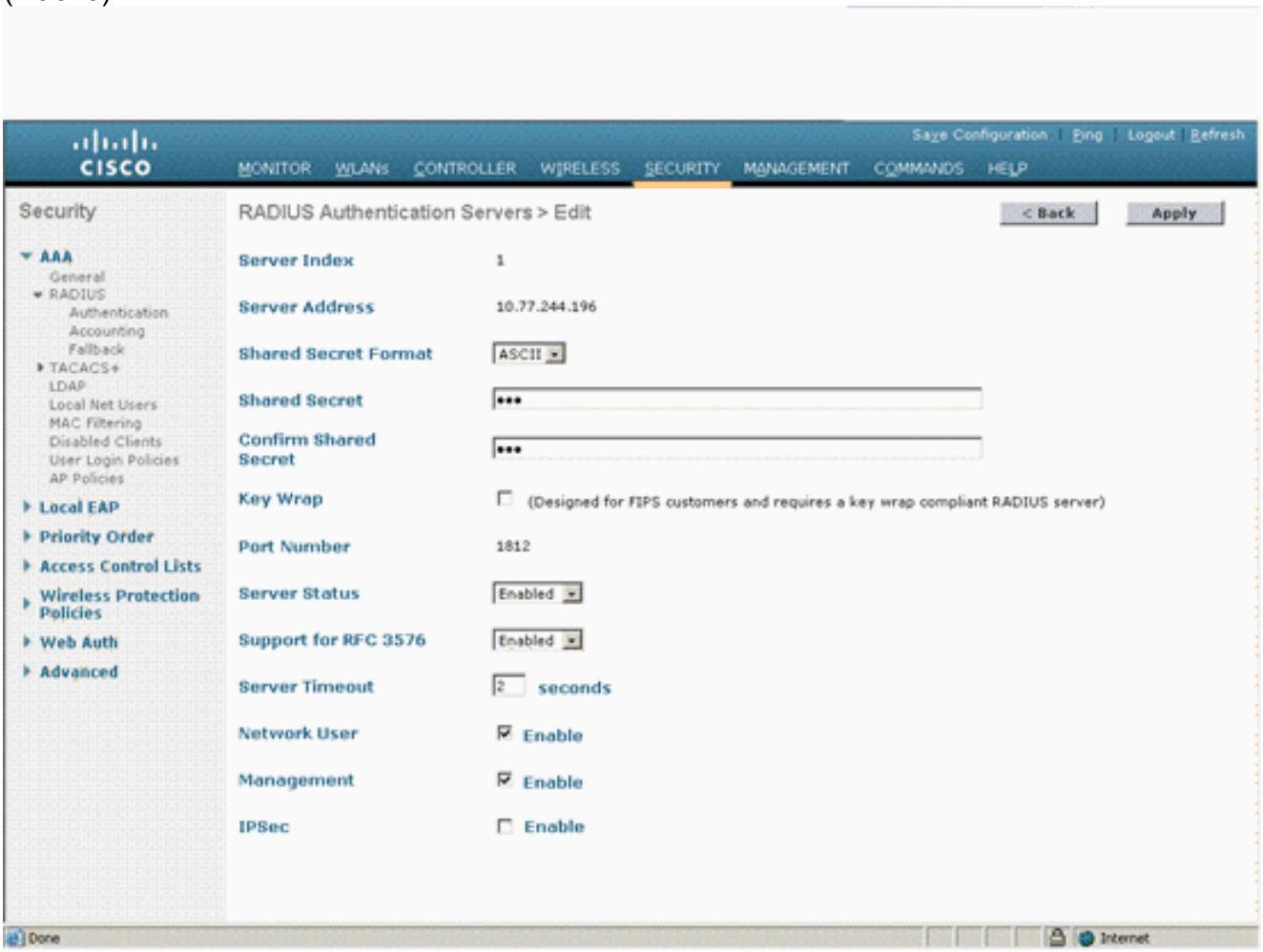
un Lightweight AP (LAP) su un Wireless LAN Controller (WLC) .

Configurazione del WLC per l'autenticazione RADIUS tramite un server RADIUS esterno

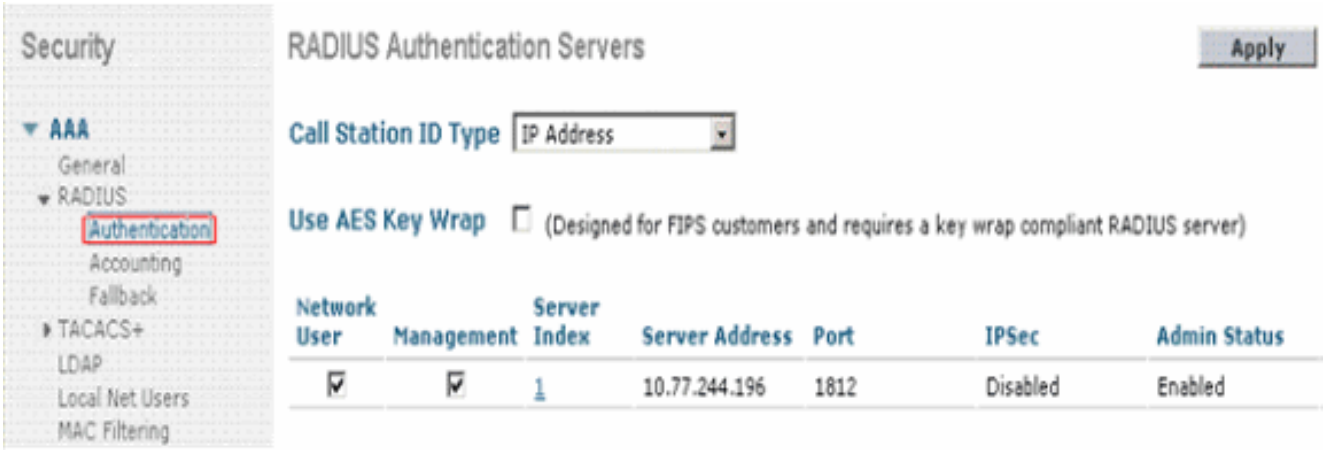
Ènecessario configurare il WLC per inoltrare le credenziali dell'utente a un server RADIUS esterno. Il server RADIUS esterno convalida quindi le credenziali utente e fornisce l'accesso ai client wireless.

Per configurare il WLC per un server RADIUS esterno, completare la procedura seguente:

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



2. Definire i parametri del server RADIUS nella pagina Server di autenticazione RADIUS > Nuovo. Questi parametri includono l'indirizzo IP, il segreto condiviso, il numero di porta e lo stato del server RADIUS.Le caselle di controllo Gestione e utente di rete determinano se l'autenticazione basata su RADIUS è valida per la gestione WLC e gli utenti di rete. In questo esempio viene utilizzato Cisco Secure ACS come server RADIUS con indirizzo IP 10.77.244.196.
3. Il server Radius può ora essere utilizzato dal WLC per l'autenticazione. Se si sceglie **Sicurezza > Radius > Autenticazione**, è possibile trovare il server Radius nell'elenco.



La RFC 3576 è supportata sul server RADIUS Cisco CNS Access Registrar (CAR), ma non sul server Cisco Secure ACS versione 4.0 e precedenti.Èinoltre possibile utilizzare la funzionalità server RADIUS locale per autenticare gli utenti. Il server RADIUS locale è stato introdotto con il codice versione 4.1.171.0. I WLC che eseguono versioni precedenti non dispongono della funzione di raggio locale. EAP locale è un metodo di autenticazione che consente agli utenti e ai client wireless di essere autenticati localmente. 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. EAP locale recupera le credenziali utente dal database degli utenti locale o dal database backend LDAP per autenticare gli utenti. Local EAP supporta LEAP, EAP-FAST con PAC, EAP-FAST con certificati e autenticazione EAP-TLS tra il controller e i client wireless.Il protocollo EAP locale è progettato come sistema di autenticazione di backup. Se nel controller sono configurati server RADIUS, il controller tenta di autenticare prima i client wireless con 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.Per ulteriori informazioni su come configurare il protocollo EAP locale sui controller LAN wireless, consultare l'esempio di autenticazione EAP locale sul controller LAN wireless con EAP-FAST e configurazione del server LDAP.

Configurazione dei parametri WLAN

Quindi, configurare la WLAN usata dai client per connettersi alla rete wireless. Quando sono stati configurati i parametri di base per il WLC, è stato configurato anche il SSID per la WLAN. È possibile usare questo SSID per la WLAN o creare un nuovo SSID. In questo esempio viene creato un nuovo SSID.

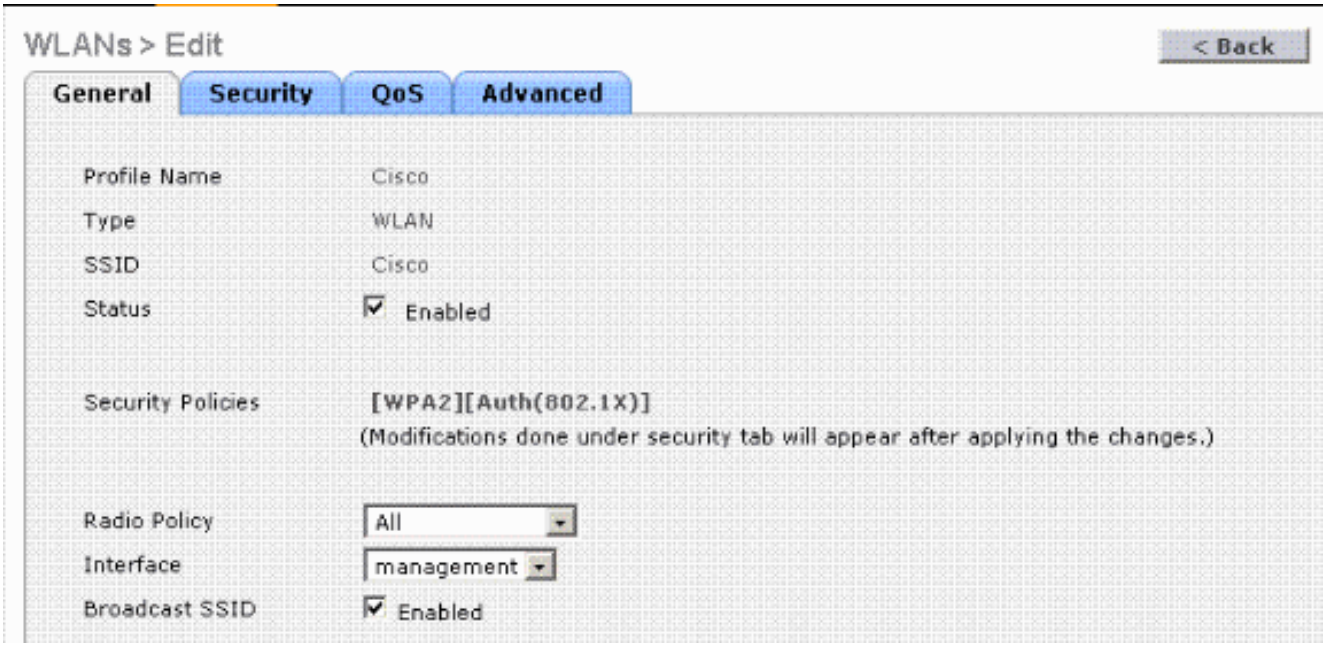
Nota: è possibile configurare fino a sedici WLAN sul controller. La soluzione Cisco WLAN può controllare fino a sedici WLAN per punti di accesso leggeri. A ciascuna WLAN possono essere assegnate policy di sicurezza univoche. I Lightweight Access Point trasmettono tutti gli SSID WLAN delle soluzioni Cisco WLAN attivi e applicano i criteri definiti per ciascuna WLAN.

Completare questa procedura per configurare una nuova WLAN e i relativi parametri:

1. Fare clic su **WLAN** dalla GUI del controller per visualizzare la pagina WLAN.In questa pagina vengono elencate le WLAN esistenti sul controller.
2. Per creare una nuova WLAN, scegliere **Nuovo**. Immettere il nome del profilo e l'SSID della WLAN per la WLAN e fare clic su **Apply** (Applica). In questo esempio viene utilizzato Cisco come

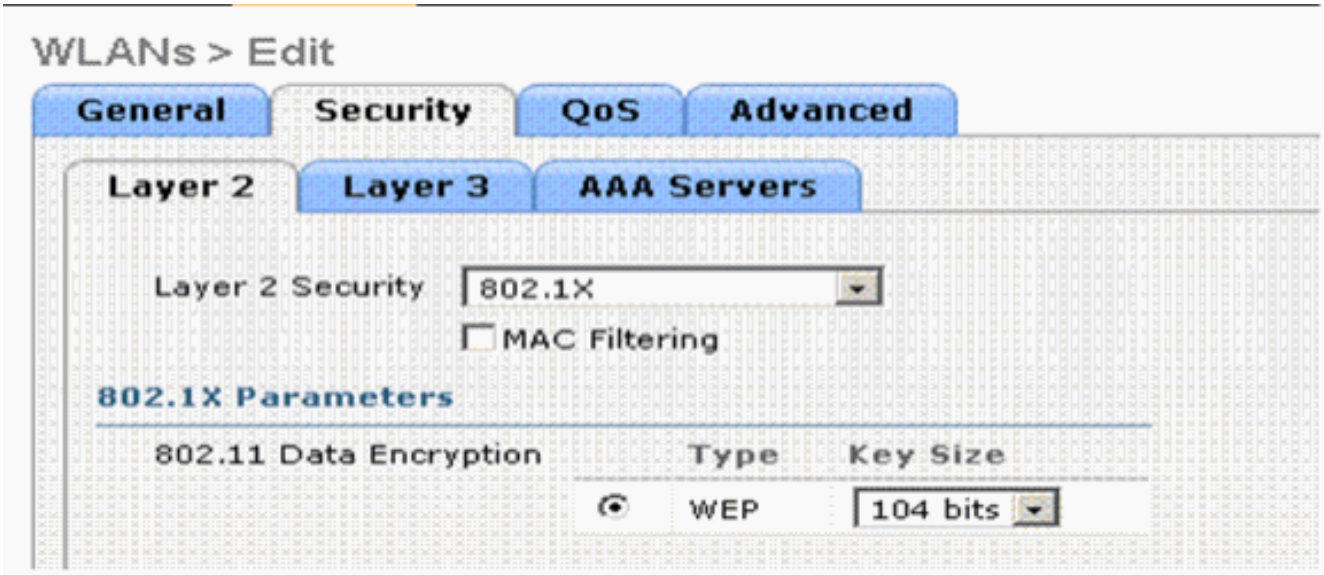
SSID.

3. Dopo aver creato una nuova WLAN, viene visualizzata la pagina WLAN > Modifica per la nuova WLAN. In questa pagina è possibile definire vari parametri specifici per la WLAN, tra cui Criteri generali, Criteri di sicurezza, Criteri QOS e altri parametri avanzati.

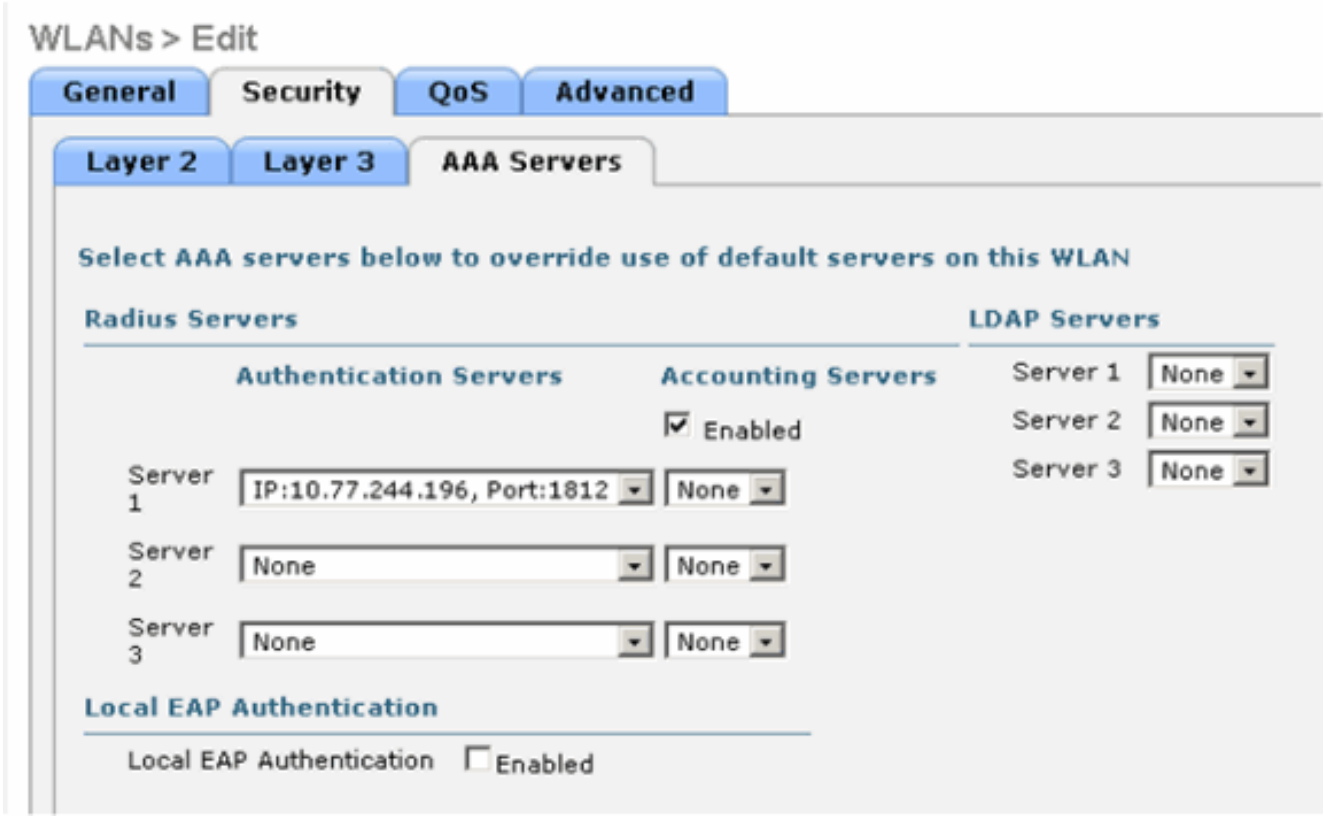


Scegliere l'interfaccia appropriata dal menu a discesa. Gli altri parametri possono essere modificati in base ai requisiti della rete WLAN.Per abilitare la WLAN, selezionare la casella **Status** (Stato) in General Policies (Criteri generali).

4. Fare clic sulla scheda **Protezione** e scegliere **Protezione di livello 2**. Dal menu a discesa Protezione di livello 2, scegliere **802.1x**. Nei parametri 802.1x scegliere la dimensione della chiave WEP. In questo esempio viene utilizzata la chiave WEP a 128 bit, ovvero la chiave WEP a 104 bit più il vettore di inizializzazione a 24 bit.



5. Scegliere la scheda **Server AAA**. Dal menu a discesa Authentication Servers (RADIUS), scegliere il server RADIUS appropriato. Questo server viene utilizzato per autenticare i client wireless.

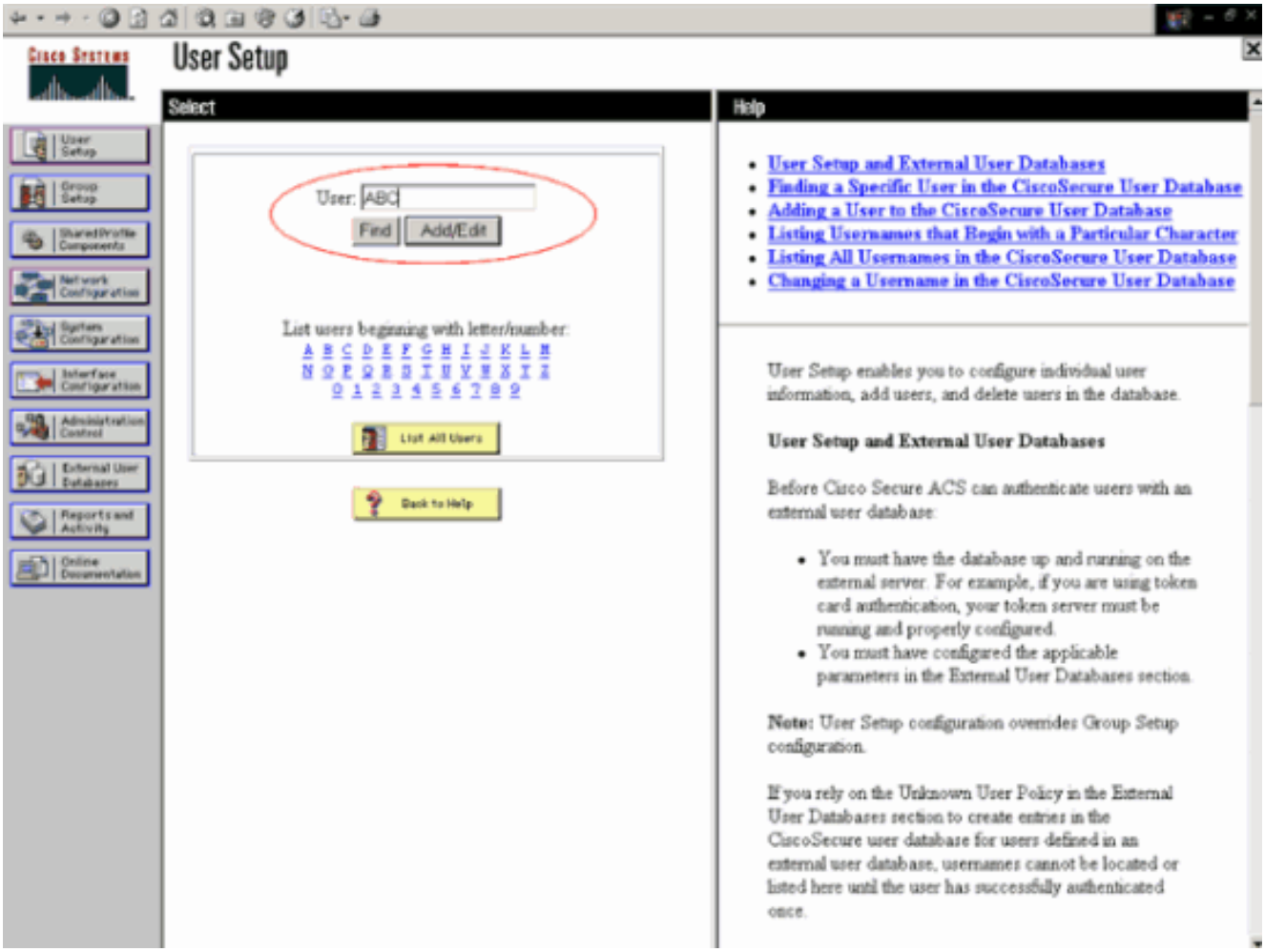


6. Per salvare la configurazione, fare clic su **Apply** (Applica).

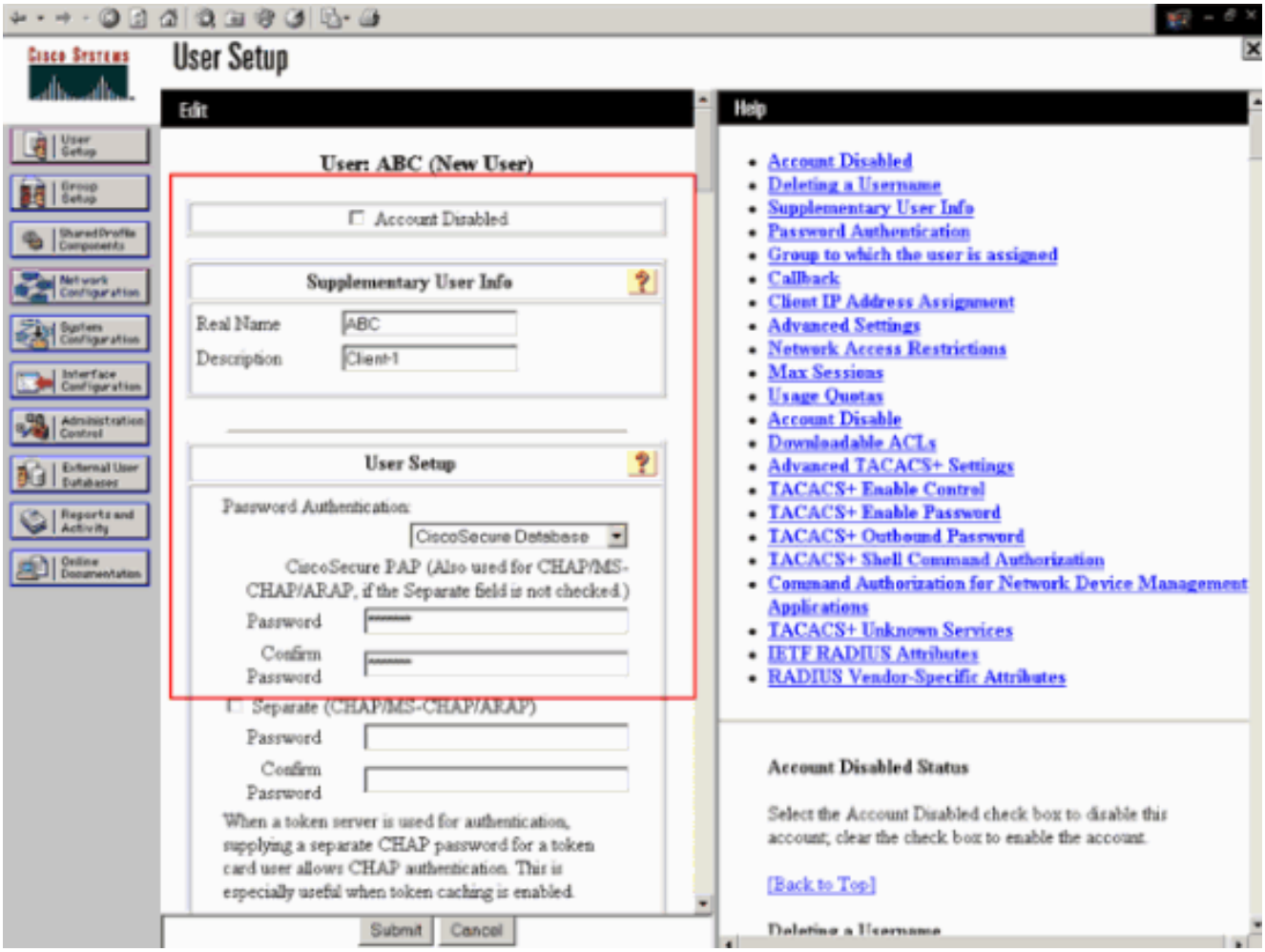
Configurazione di Cisco Secure ACS come server RADIUS esterno e creazione di un database utente per i client di autenticazione

Completare la procedura seguente per creare il database utenti e abilitare l'autenticazione EAP su Cisco Secure ACS:

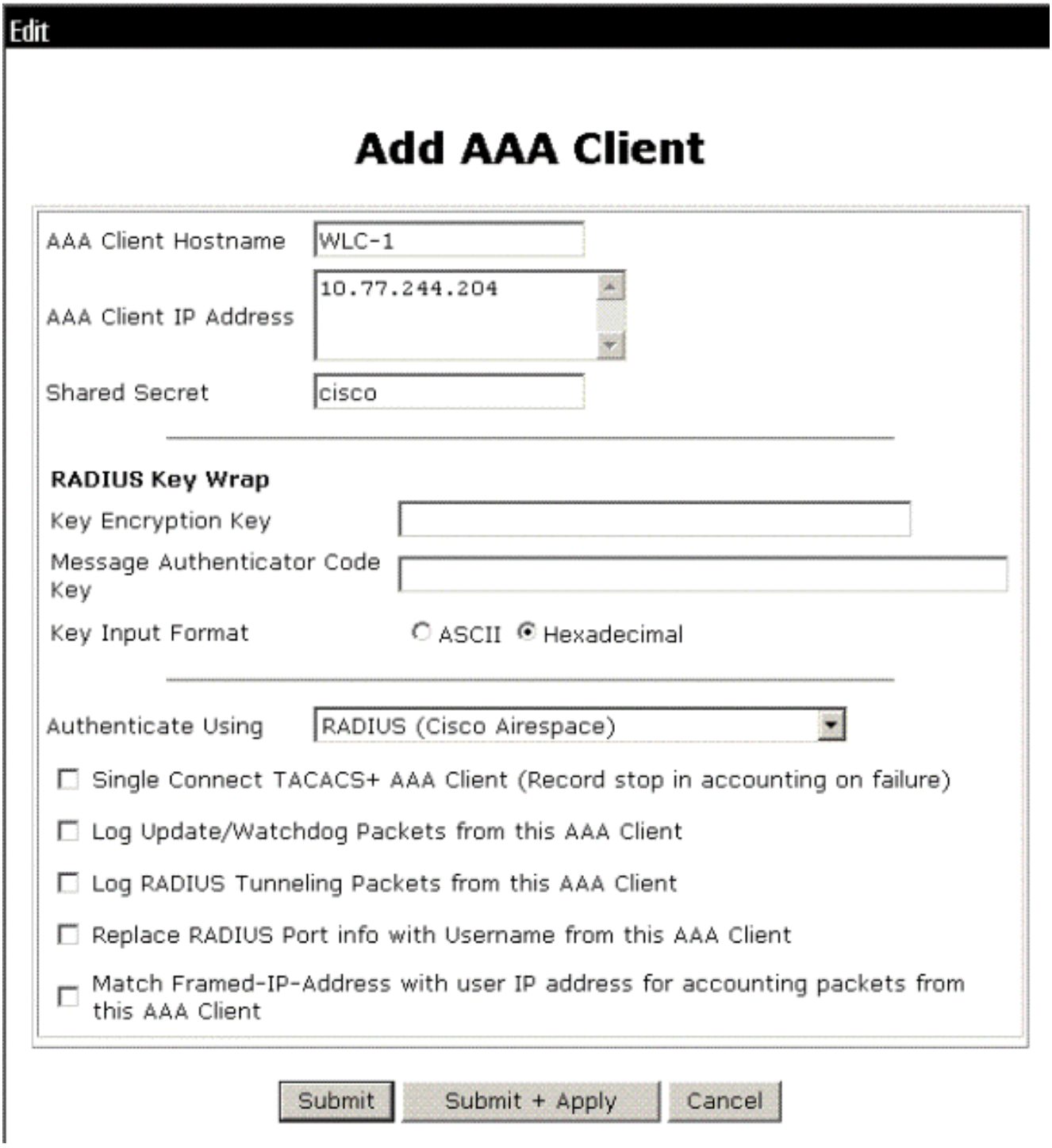
1. Selezionare **User Setup** (Configurazione utente) dall'interfaccia utente di ACS, immettere il nome utente e fare clic su **Add/Edit** (Aggiungi/Modifica). In questo esempio l'utente è **ABC.**



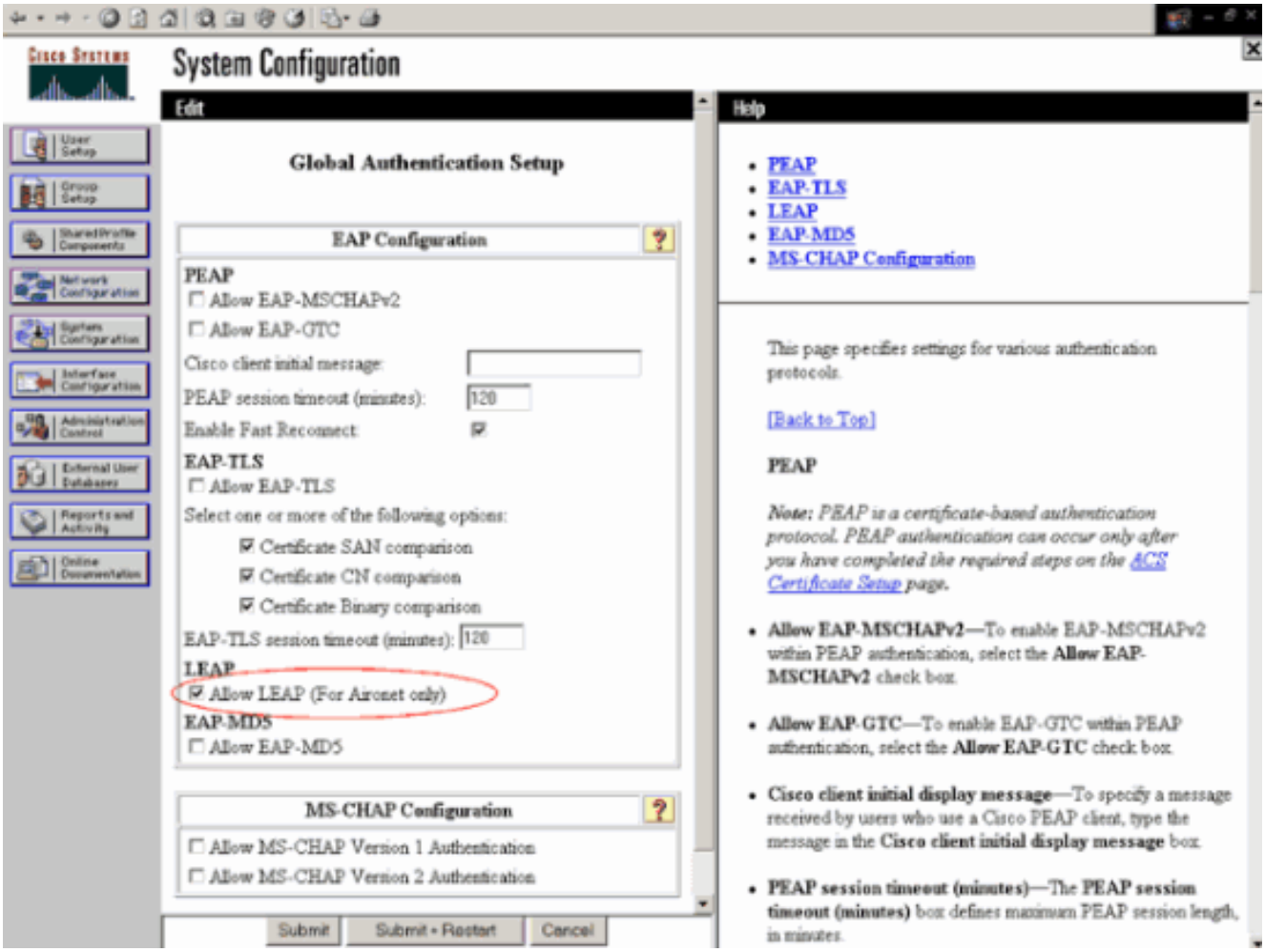
2. Quando viene visualizzata la pagina Impostazione utente, definire tutti i parametri specifici dell'utente. In questo esempio vengono configurati il nome utente, la password e le informazioni utente supplementari, in quanto questi parametri sono necessari solo per l'autenticazione EAP.Fare clic su **Invia** e ripetere la stessa procedura per aggiungere altri utenti al database. Per impostazione predefinita, tutti gli utenti sono raggruppati nel gruppo predefinito e a essi viene assegnato lo stesso criterio definito per il gruppo. Per ulteriori informazioni sull'assegnazione di utenti specifici a gruppi diversi, consultare la sezione User Group Management della Guida dell'utente di Cisco Secure ACS per Windows Server 3.2.



3. Definire il controller come client AAA sul server ACS. Fare clic su **Network Configuration** (Configurazione di rete) dall'interfaccia utente di ACS.Quando viene visualizzata la pagina Configurazione di rete, definire il nome del WLC, l'indirizzo IP, il segreto condiviso e il metodo di autenticazione (RADIUS Cisco Airespace). Per altri server di autenticazione non ACS, consultare la documentazione del produttore.**Nota:** la chiave segreta condivisa configurata sul WLC e sul server ACS deve corrispondere. Il segreto condiviso fa distinzione tra maiuscole e
minuscole.



4. Fare clic su **Configurazione del sistema** e su **Configurazione autenticazione globale** per verificare che il server di autenticazione sia configurato in modo da eseguire il metodo di autenticazione EAP desiderato. In Impostazioni di configurazione EAP scegliere il metodo EAP appropriato. In questo esempio viene utilizzata l'autenticazione LEAP. Al termine, fare clic su **Submit**
(Invia).

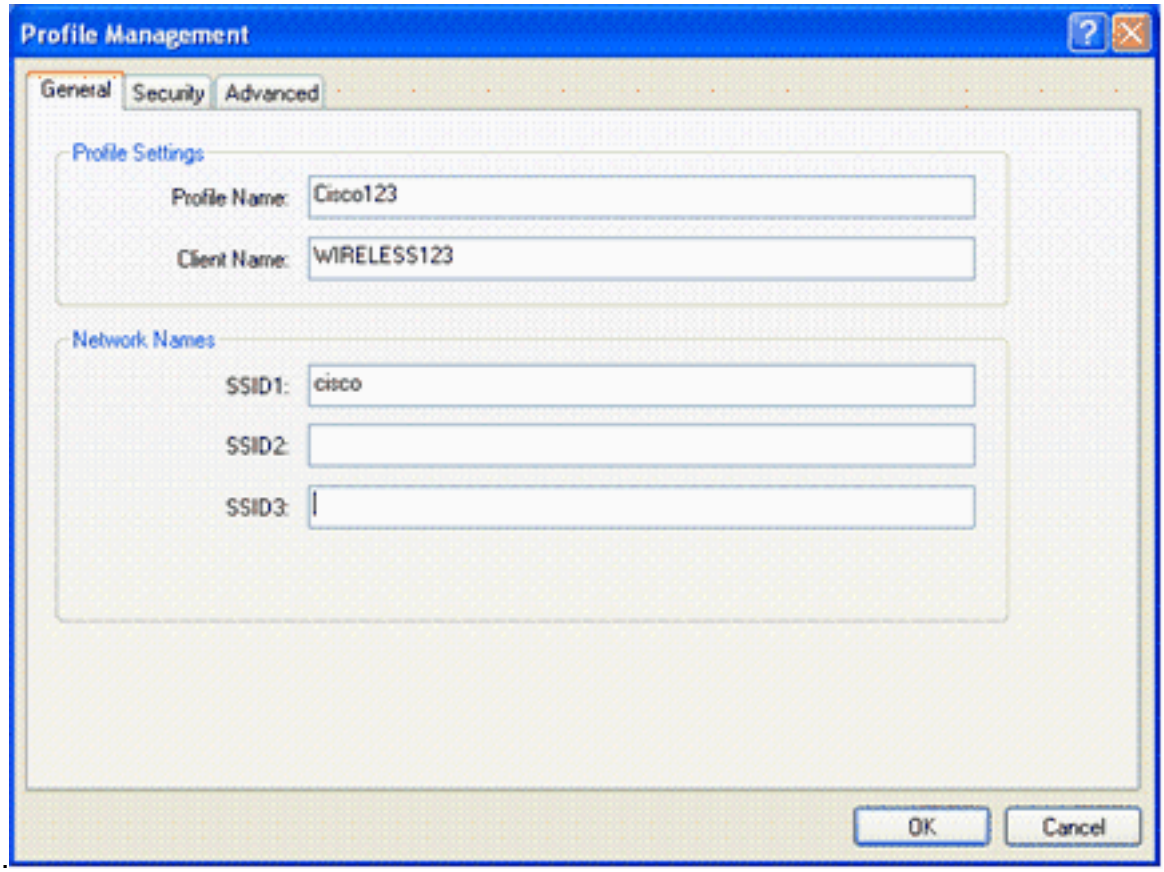


Configurare il client

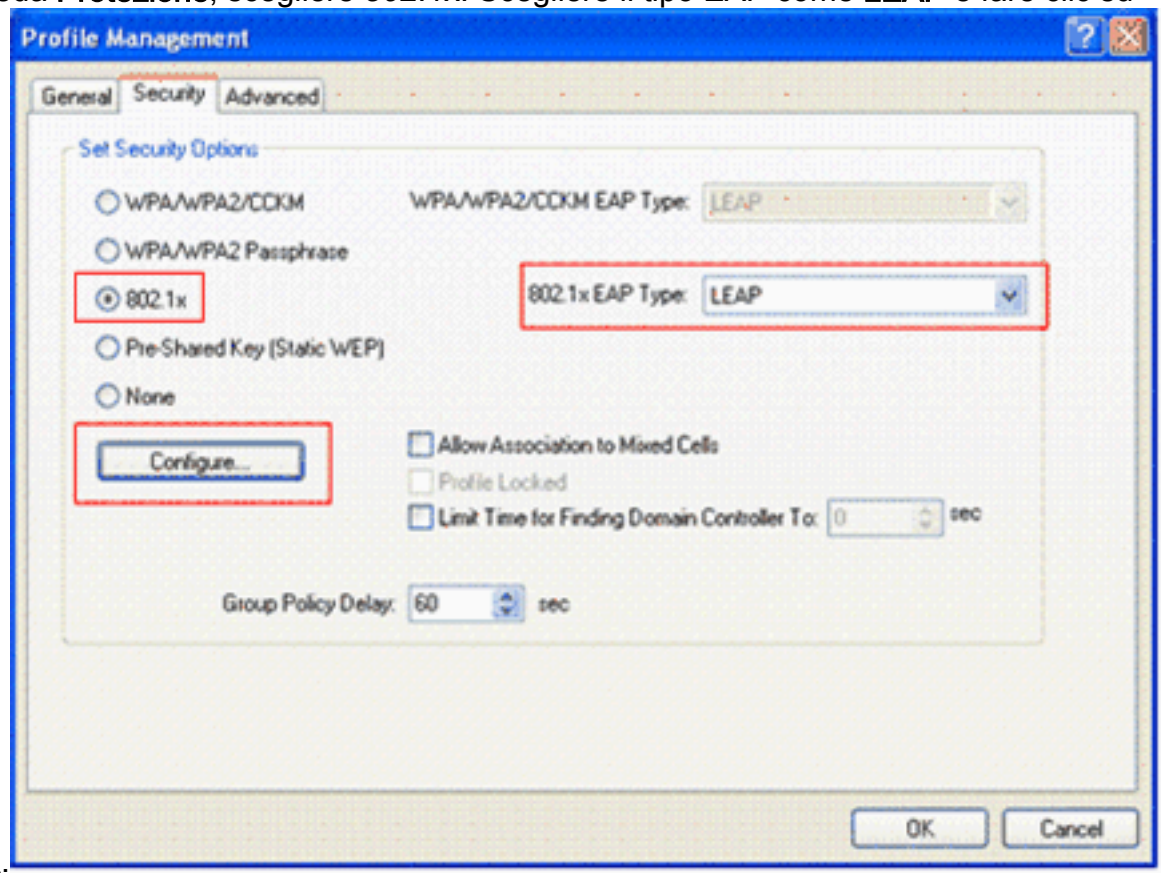
Èinoltre necessario configurare il client per il tipo EAP appropriato. Il client propone il tipo EAP al server durante il processo di negoziazione EAP. Se il server supporta tale tipo EAP, riconosce il tipo EAP. Se il tipo EAP non è supportato, invia un messaggio di conferma negativo e il client negozia nuovamente con un metodo EAP diverso. Questo processo continua finché non viene negoziato un tipo EAP supportato. In questo esempio viene utilizzato LEAP come tipo EAP.

Completare questa procedura per configurare LEAP sul client con Aironet Desktop Utility.

1. Fare doppio clic sull'icona **Aironet Utility** per aprirla.
2. Fare clic sulla scheda **Gestione profili**.
3. Fare clic su un profilo e scegliere **Modifica**.
4. Nella scheda Generale, scegliere un *Nome profilo*. Immettere l'**SSID** della

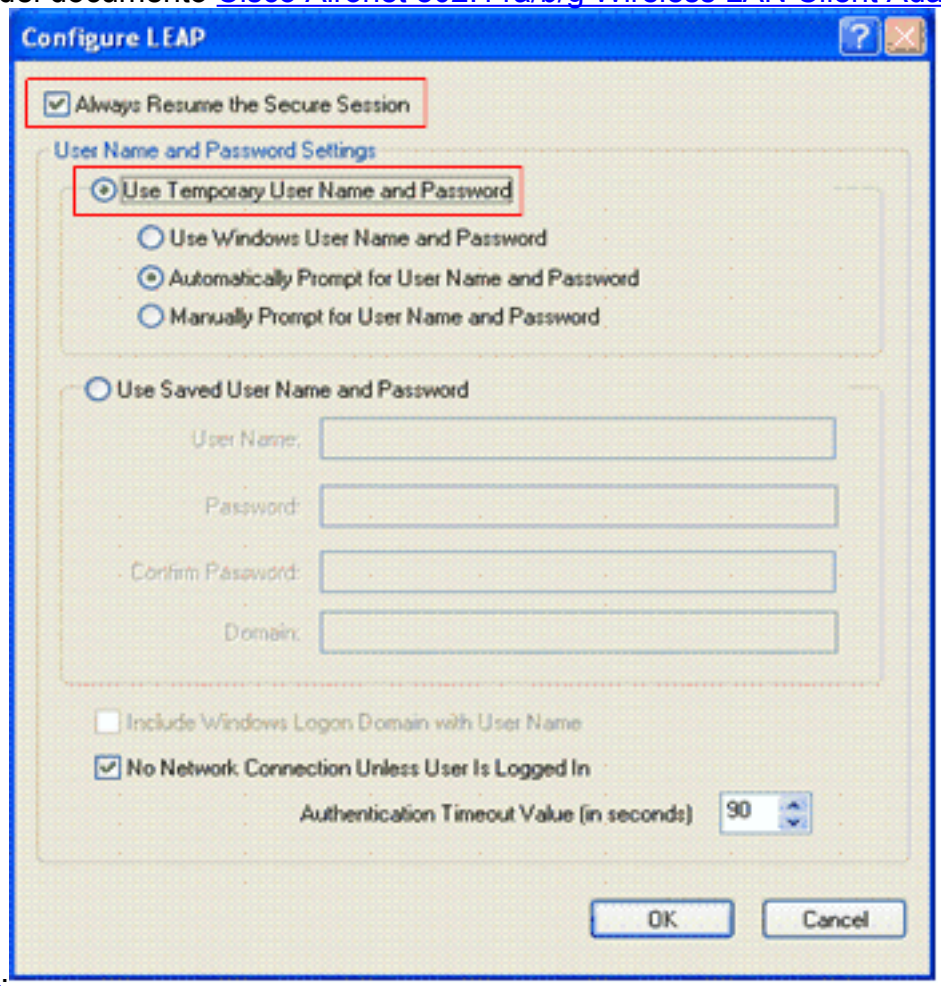
WLAN. 

Nota: per SSID viene fatta distinzione tra maiuscole e minuscole e deve corrispondere esattamente a SSID configurato sul WLC.

5. Nella scheda **Protezione**, scegliere *802.1x*. Scegliere il tipo EAP come **LEAP** e fare clic su **Configura**. 

6. Scegliere **Usa nome utente e password temporanei** per immettere le credenziali utente a ogni riavvio del computer.Selezionare una delle tre opzioni disponibili. In questo esempio vengono utilizzate le opzioni **Richiedi automaticamente nome utente e password** (**Automatically Prompt for Username and Password**), che richiedono l'immissione delle

credenziali utente *LEAP* oltre al nome utente *e alla password di Windows* prima dell'accesso a Windows.Selezionare la casella di controllo **Riprendi sempre la sessione sicura** nella parte superiore della finestra se si desidera che il supplicant LEAP tenti sempre di riprendere la sessione precedente senza che sia necessario richiedere di immettere nuovamente le credenziali ogni volta che la scheda di rete del client si sposta e si riassocia alla rete.**Nota:** per ulteriori informazioni sulle altre opzioni, consultare la sezione Configurazione dell'adattatore client del documento Cisco Aironet 802.11a/b/g Wireless LAN Client Adapter (CB21AG e PI21AG).



7. Nella scheda **Avanzate** è possibile configurare il preambolo, l'estensione Aironet e altre opzioni 802.11 come l'alimentazione, la frequenza e così via.
8. Fare clic su **OK**. Il client tenta ora di associarsi ai parametri configurati.

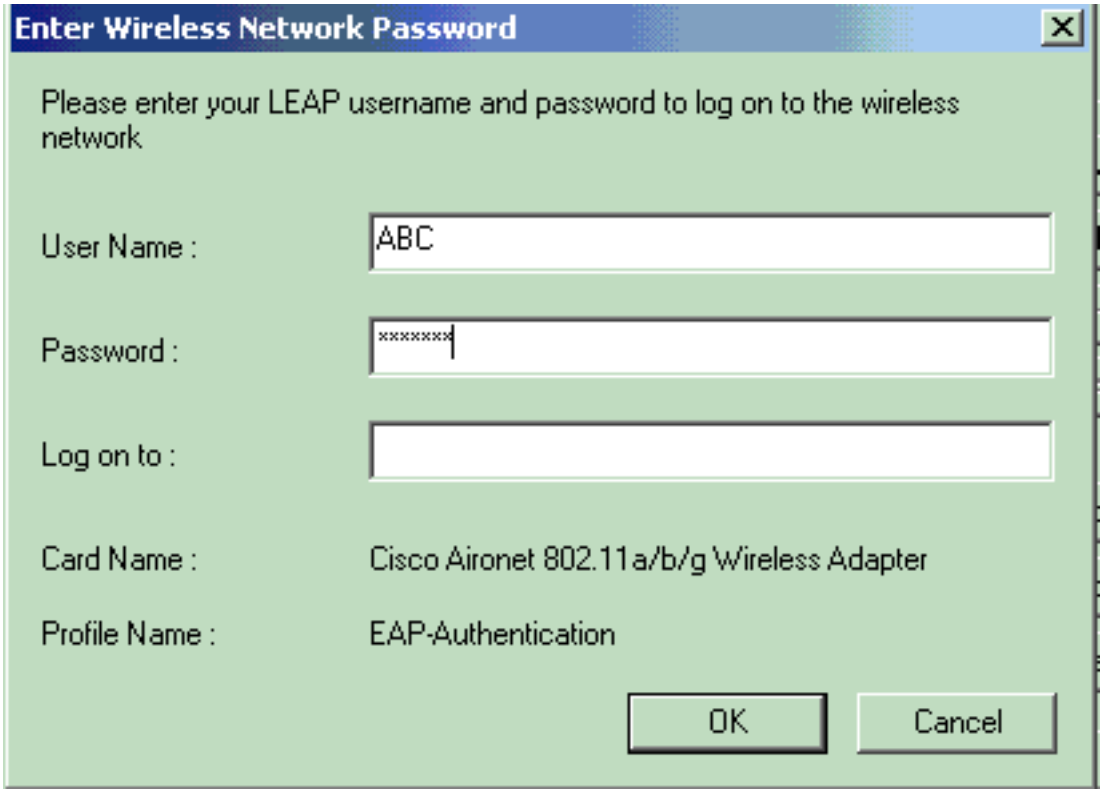
Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

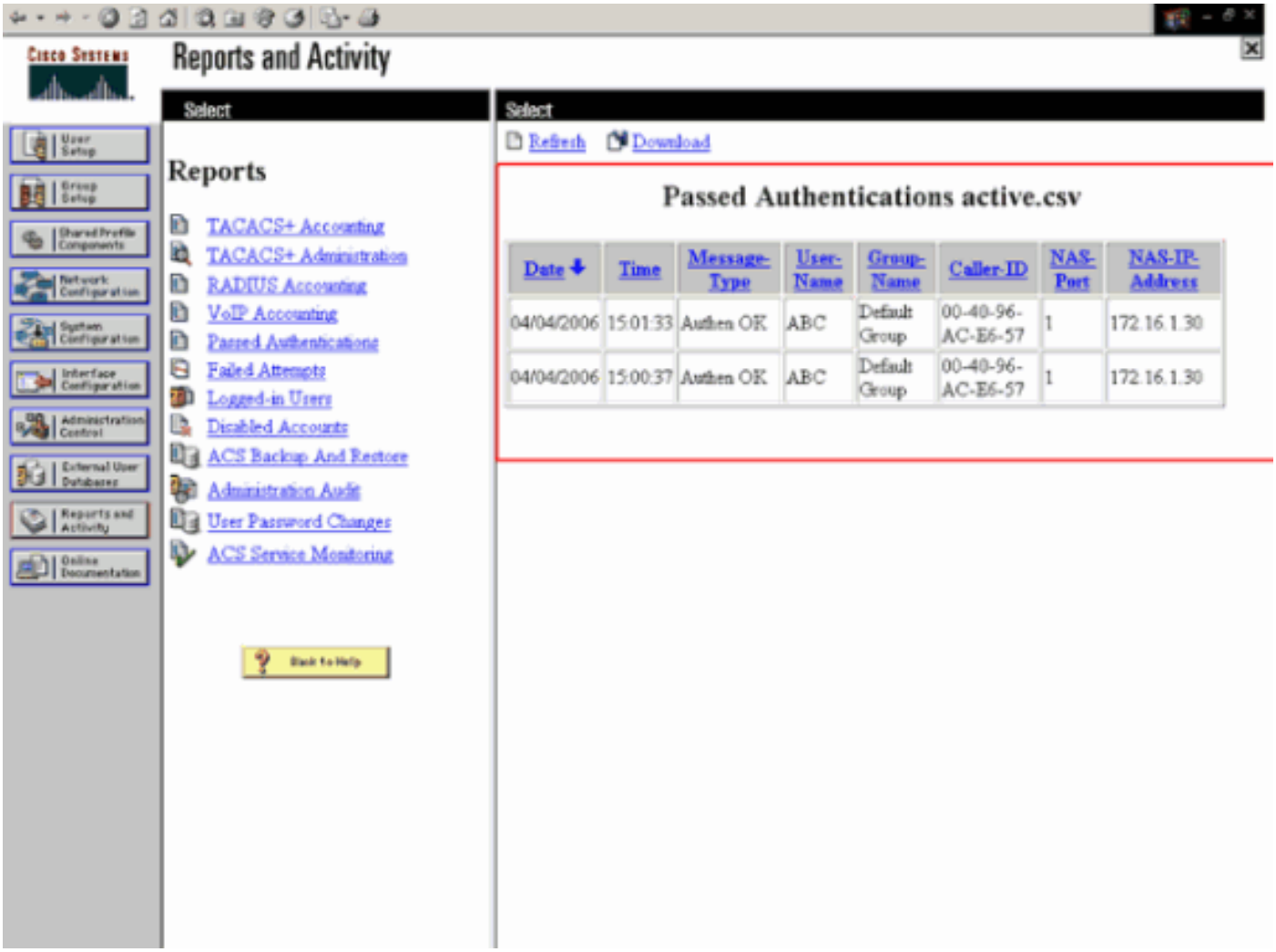
Provare ad associare un client wireless al Lightweight AP utilizzando l'autenticazione LEAP per verificare se la configurazione funziona come previsto.

Nota: in questo documento si presume che il profilo client sia configurato per l'autenticazione LEAP. Per ulteriori informazioni su come configurare l'adattatore client wireless 802.11 a/b/g per l'autenticazione LEAP, fare riferimento a Uso dell'autenticazione EAP.

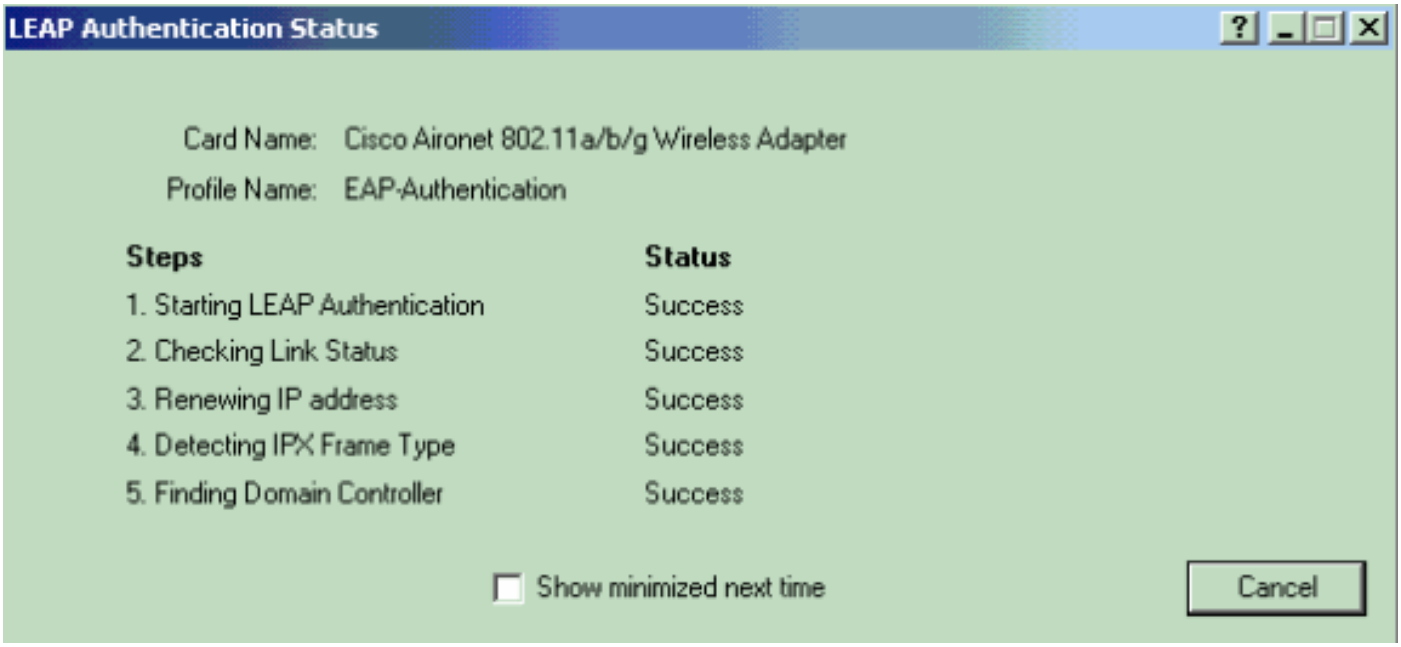
Una volta attivato il profilo per il client wireless, all'utente viene richiesto di fornire il nome utente/password per l'autenticazione LEAP. Di seguito è riportato un esempio:



Il Lightweight AP e quindi il WLC passano le credenziali dell'utente al server RADIUS esterno (Cisco Secure ACS) per convalidarle. Il server RADIUS confronta i dati con il database degli utenti e fornisce l'accesso al client wireless ogni volta che le credenziali utente sono valide per verificarle. Il report Autenticazione passata sul server ACS indica che il client ha superato l'autenticazione RADIUS. Di seguito è riportato un esempio:



Se l'autenticazione RADIUS riesce, il client wireless si associa al Lightweight AP.

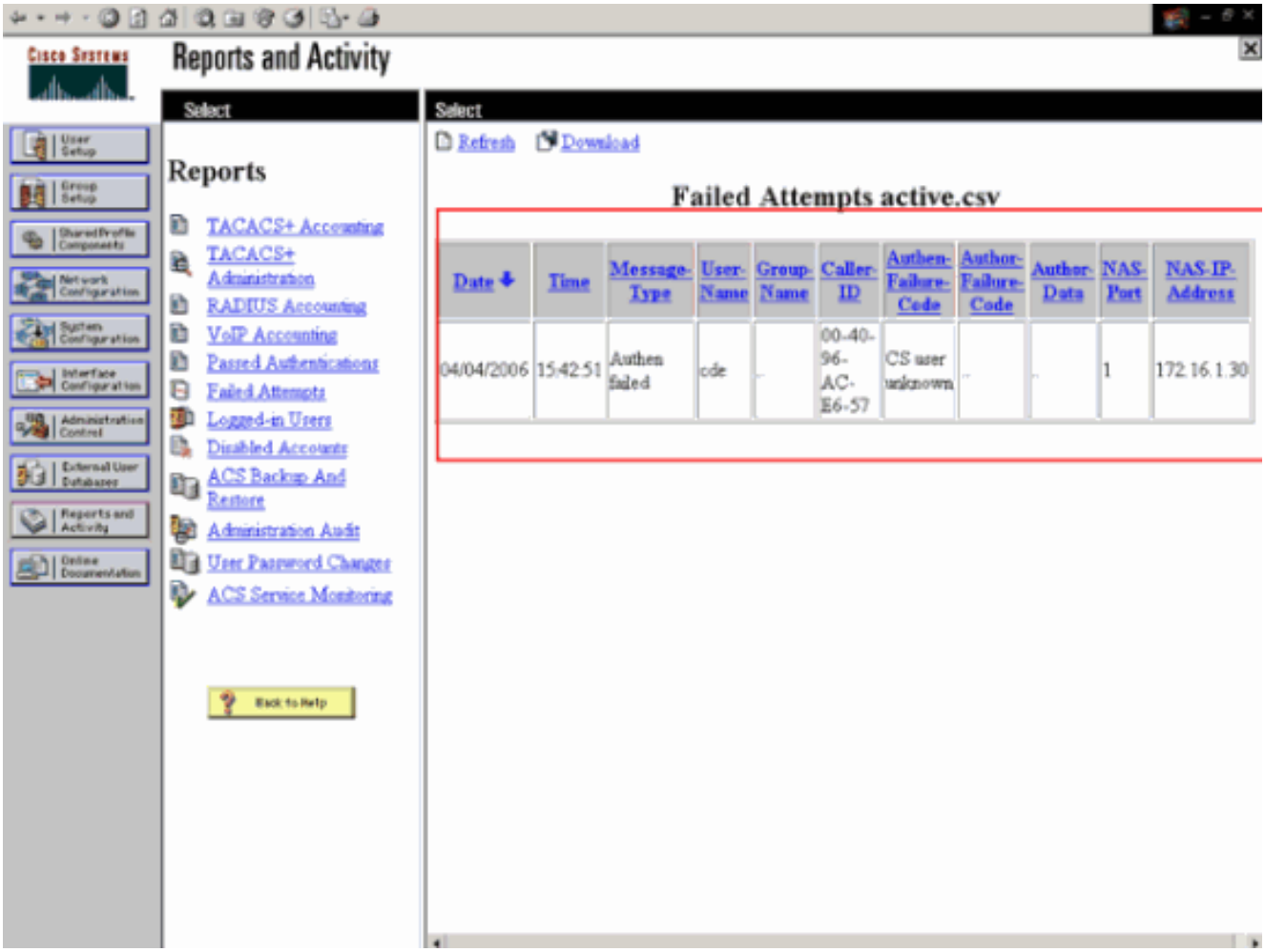


È possibile controllare questa condizione anche nella scheda **Monitor** dell'interfaccia utente del WLC. Scegliere **Monitor > Client** e controllare l'indirizzo MAC del client.

Risoluzione dei problemi

Completare la procedura seguente per risolvere i problemi relativi alle configurazioni:

1. Per controllare se l'access point si registra sul WLC, usare il comando **debug lwapp events enable**.
2. Verificare se il server RADIUS riceve e convalida la richiesta di autenticazione dal client wireless. Controllare l'indirizzo IP-NAS, la data e l'ora per verificare se il WLC è riuscito a raggiungere il server Radius.A tale scopo, controllare i report Autenticazioni superate e Tentativi non riusciti sul server ACS. Questi report sono disponibili in Report e attività sul server ACS. Di seguito è riportato un esempio di errore di autenticazione del server RADIUS:



Nota: per informazioni su come risolvere i problemi e ottenere le informazioni di debug sugli

ACS Cisco sicuri, consultare il documento sul recupero delle informazioni di debug e sulla versione di Cisco Secure ACS per Windows.

3. Per risolvere i problemi di autenticazione AAA, è possibile usare anche i seguenti comandi di **debug**:**debug aaa all enable**: configura il debug di tutti i messaggi AAA.**debug dot1x packet enable**: abilita il debug di tutti i pacchetti dot1x.Di seguito viene riportato un output di esempio del comando **debug 802.1x aaa enable**:

```
(Cisco Controller) >debug dot1x aaa enable

*Sep 23 15:15:43.792: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
    index=1
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
    index=2
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
    index=5
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=11
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=8,
    id=2) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.794: 00000000: 02 02 00 08 01 41 42 43
    .....ABC
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim
    Response'
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received
    for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Received EAP Attribute (code=1,
    length=19,id=3, dot1xcb->id = 2) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.799: 00000000: 01 03 00 13 11 01 00 08  42 3a 8e d1 18 24 e8 9f
    ........B:...
*Sep 23 15:15:43.799: 00000010: 41 42 43
    ABC
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile
    00:40:96:ac:dd:05
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
    index=1
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
    index=2
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
    index=5
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
```

```
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2,
    length=35, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.902: 00000000: 02 03 00 23 11 01 00 18  83 f1 5b 32 cf 65 04 ed
    ...#......[2.e..
*Sep 23 15:15:43.902: 00000010: da c8 4f 95 b4 2e 35 ac  c0 6b bd fa 57 50 f3 13
    ..O...5..k..WP..
*Sep 23 15:15:43.904: 00000020: 41 42 43
    ABC
*Sep 23 15:15:43.904: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim
    Response'
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received
    for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Received EAP Attribute (code=3,
    length=4,id=3, dot1xcb->id = 3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.907: 00000000: 03 03 00 04
    ....
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile
    00:40:96:ac:dd:05
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
    index=1
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
    index=2
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
    index=5
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Sending EAP Attribute (code=1,
    length=19, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.915: 00000000: 01 03 00 13 11 01 00 08  29 23 be 84 e1 6c d6 ae
    ........)#...l..
*Sep 23 15:15:43.915: 00000010: 41 42 43
    ABC
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Success'
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 AAA Message 'Success' received for
    mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[0]: attribute 8,
    vendorId 0, valueLen 4
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[1]: attribute 79,
    vendorId 0, valueLen 35
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 Received EAP Attribute (code=2,
    length=35,id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00000000: 02 03 00 23 11 01 00 18  03 66 2c 6a b3 a6 c3 4c
    ...#.....f,j...L
*Sep 23 15:15:43.918: 00000010: 98 ac 69 f0 1b e8 8f a2  29 eb 56 d6 92 ce 60 a6
    ..i.....).V...`.
*Sep 23 15:15:43.918: 00000020: 41 42 43
    ABC
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[2]: attribute 1,
```

```
    vendorId 9, valueLen 16
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[3]: attribute 25,
    vendorId 0, valueLen 21
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[4]: attribute 80,
    vendorId 0, valueLen 16
```

Nota: alcune righe dell'output del comando debug sono state ritorno a capo a causa di problemi di spazio.

4. Monitorare i log sul WLC per verificare se il server RADIUS riceve le credenziali utente. Fare clic su **Monitor** per controllare i log dall'interfaccia utente del WLC. Dal menu a sinistra, fare clic su **Statistiche**, quindi su **Server Radius** dall'elenco delle opzioni.Questa operazione è molto importante perché in alcuni casi il server RADIUS non riceve mai le credenziali utente se la configurazione del server RADIUS sul WLC non è corretta.Di seguito viene riportato l'aspetto dei log sul WLC se i parametri RADIUS non sono configurati correttamente:

Per riconoscere le WLAN che usano l'autenticazione del server RADIUS, è possibile usare una combinazione del comando **show wlan summary**. Quindi, è possibile visualizzare il comando **show client summary** per verificare quali indirizzi MAC (client) sono stati autenticati correttamente sulle WLAN RADIUS. È inoltre possibile correlare questa condizione ai log dei tentativi passati o non riusciti di Cisco Secure ACS.

Suggerimenti per la risoluzione dei problemi

- Verificare sul controller che il server RADIUS sia in stato `attivo` e non in `standby` o `disabilitato`.
- Usare il comando **ping** per verificare se il server Radius è raggiungibile dal WLC.
- Verificare che il server RADIUS sia selezionato dal menu a discesa della rete WLAN (SSID).
- Se si utilizza WPA, è necessario installare l'aggiornamento rapido Microsoft WPA più recente per Windows XP SP2. È inoltre necessario aggiornare il driver per il supplicant client all'ultimo aggiornamento.
- Se si esegue PEAP, ad esempio certificati con XP, SP2 in cui le schede sono gestite dall'utilità Microsoft wireless-0, è necessario ottenere la patch KB885453 da Microsoft.Se si utilizza Windows Zero Config/client supplicant, disabilitare l'opzione **Abilita riconnessione rapida**. A tale scopo, scegliere **Proprietà Connessione rete senza fili > Reti senza fili > Reti preferite**. Quindi scegliere **SSID > Proprietà > Apri > WEP > Autenticazione > Tipo EAP > PEAP > Proprietà > Abilita riconnessione rapida** . L'opzione per l'attivazione o la disattivazione è disponibile alla fine della finestra.
- Se si dispone di schede Intel 2200 o 2915, fare riferimento alle istruzioni sul sito Web di Intel relative ai problemi noti delle schede:Connessione di rete Intel® PRO/Wireless

2200BGConnessione di rete Intel® PRO/Wireless 2915ABGScaricate i driver Intel più recenti per evitare problemi. È possibile scaricare i driver Intel all'indirizzo http://downloadcenter.intel.com/

- Se la funzione di failover aggressivo è abilitata nel WLC, il WLC è troppo aggressivo per contrassegnare il server AAA come `non rispondente`. Tuttavia, non è consigliabile eseguire questa operazione perché il server AAA potrebbe non rispondere solo a quel determinato client, in caso di eliminazione invisibile all'utente. Può essere una risposta ad altri client validi con certificati validi. Tuttavia, il WLC può ancora contrassegnare il server AAA come `non rispondente` e `non funzionante`.Per risolvere questo problema, disattivare la funzione di failover aggressivo. Per eseguire questa operazione, usare il comando **config radius aggressive-failover disable** dall'interfaccia utente del controller. Se questa opzione è disabilitata, il controller eseguirà il failover sul server AAA successivo solo se sono presenti tre client consecutivi che non sono in grado di ricevere una risposta dal server RADIUS.

Manipolazione dei timer EAP

Durante l'autenticazione 802.1x, l'utente potrebbe visualizzare `DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE: Numero massimo di ritrasmissioni del tasto EAPOL M1 raggiunto per il` messaggio di errore `cellulare xx:xx:xx:xx`.

Questo messaggio di errore indica che il client non ha risposto in tempo al controller durante la negoziazione delle chiavi WPA (802.1x). Il controller imposta un timer per una risposta durante la negoziazione della chiave. In genere, quando viene visualizzato questo messaggio, è dovuto a un problema con il richiedente. Accertarsi di eseguire le versioni più recenti dei driver e del firmware del client. Sul WLC, ci sono alcuni timer EAP che è possibile modificare per facilitare l'autenticazione del client. I timer EAP includono:

```
EAP-Identity-Request Timeout
EAP-Identity-Request Max Retries
EAP-Request Timeout (seconds)
EAP-Request Max Retries
EAPOL-Key Timeout
EAPOL-Key Max Retries
```

Prima di poter manipolare questi valori, è necessario capire cosa fanno e come modificarli influirà sulla rete:

- **Timeout richiesta di identità EAP:**Questo timer influisce sul tempo di attesa tra le richieste di identità EAP. Per impostazione predefinita, questo valore è di un secondo (4.1 e inferiore) e 30 secondi (4.2 e superiore). La ragione di questo cambiamento è stata che alcuni clienti, palmari, telefoni, scanner e così via, hanno avuto difficoltà a rispondere abbastanza velocemente. Dispositivi come i portatili, in genere non richiedono una manipolazione di questi valori. Il valore disponibile è compreso tra 1 e 120.Cosa succede quando l'attributo è impostato sul valore 30? Quando il client si connette per la prima volta, invia un messaggio EAPOL Start alla rete e il WLC invia un pacchetto EAP, richiedendo l'identità dell'utente o del computer. Se il WLC non riceve la risposta all'identità, invia un'altra richiesta di identità 30 secondi dopo la prima. Ciò si verifica alla connessione iniziale e quando il client esegue il roaming.Cosa succede quando si aumenta il timer? Se tutto va bene, non c'è impatto. Tuttavia, se si verifica un problema nella rete (compresi problemi del client, problemi del punto di accesso o problemi di RF), è possibile che si verifichino ritardi nella connettività di rete. Ad

esempio, se si imposta il timer sul valore massimo di 120 secondi, il WLC attende 2 minuti tra le richieste di identità. Se il client è in roaming e la risposta non viene ricevuta dal WLC, è stata creata almeno un'interruzione di due minuti per il client.Il timer consigliato è *5*. Al momento non è necessario impostare il timer sul valore massimo.

- **Numero massimo tentativi EAP-Identity-Request:**Il valore Max Retries è il numero di volte che il WLC invierà la richiesta di identità al client prima di rimuovere la relativa voce da MSCB. Una volta raggiunto il valore di Max Retries, il WLC invia un frame di deautenticazione al client, forzandolo a riavviare il processo EAP. Il valore disponibile è compreso tra 1 e 20. Verrà quindi illustrato in dettaglio.Il valore di Numero massimo tentativi funziona con il timeout dell'identità. Se il valore di Timeout identità è impostato su 120 e il valore di Numero massimo di tentativi è 20, il tempo necessario è 2400 (o 120 * 20). Ciò significa che occorrerebbero 40 minuti per rimuovere il client e per riavviare il processo EAP. Se si imposta il timeout dell'identità su 5, con un valore di Max Retries pari a 12, saranno necessari 60 (o 5 * 12). A differenza dell'esempio precedente, è necessario attendere un minuto prima che il client venga rimosso e riavvii EAP.Il numero massimo di tentativi consigliato è *12*.
- **Timeout tasto EAPOL:**Per il valore di timeout della chiave EAPOL, il valore predefinito è 1 secondo o 1000 millisecondi. Ciò significa che quando le chiavi EAPOL vengono scambiate tra l'access point e il client, l'access point invierà la chiave e attende fino a 1 secondo per impostazione predefinita che il client risponda. Dopo aver atteso il valore di tempo definito, l'access point ritrasmette nuovamente la chiave. Per modificare questa impostazione, è possibile usare il comando **config advanced eap eapol-key-timeout *<time>***. I valori disponibili in 6.0 sono compresi tra 200 e 5000 millisecondi, mentre i codici precedenti a 6.0 consentono valori compresi tra 1 e 5 secondi. Tenere presente che se si dispone di un client che non risponde a un tentativo di chiave, l'estensione dei timeout può concedere loro un po' più di tempo per rispondere. Tuttavia, questa operazione potrebbe anche prolungare il tempo necessario al WLC/AP per deautenticare il client in modo che l'intero processo 802.1x ricominci.
- **Numero massimo tentativi chiave EAPOL:**Per il valore EAPOL-Key Max Retries, il valore predefinito è 2. Ciò significa che il tentativo di chiave originale verrà ripetuto due volte nel client. Per modificare questa impostazione, usare il comando **config advanced eap eapol-key-retries *<retries>*** . I valori disponibili sono compresi tra 0 e 4 tentativi. Utilizzando il valore predefinito per Timeout chiave EAPOL (1 secondo) e il valore predefinito per Riprova chiave EAPOL (2), il processo procederà come segue se un client non risponde al tentativo di chiave iniziale:L'access point invia un tentativo di chiave al client.Aspetta un secondo per una risposta.In assenza di risposta, viene inviato il primo nuovo tentativo EAPOL-Key.Aspetta un secondo per una risposta.In assenza di risposta, viene inviato il secondo tentativo EAPOL-Key.Se il client non risponde e viene raggiunto il valore retry, il client viene deautenticato. Anche in questo caso, come nel caso del timeout della chiave EAPOL, l'estensione del valore dei tentativi della chiave EAPOL potrebbe, in alcune circostanze, essere utile. Tuttavia, se si imposta il valore massimo, il messaggio di disautenticazione verrà prolungato.

Estrazione del file del pacchetto dal server RADIUS ACS per la risoluzione dei problemi

Se si utilizza ACS come server RADIUS esterno, questa sezione può essere utilizzata per risolvere i problemi relativi alla configurazione. Il file package.cab è un file Zip contenente tutti i file necessari per risolvere in modo efficiente i problemi relativi ad ACS. È possibile utilizzare l'utilità CSSupport.exe per creare package.cab oppure raccogliere i file manualmente.

Per ulteriori informazioni su come creare ed estrarre il file del pacchetto da WCS, consultare la sezione Creazione di un file package.cab in *Recupero delle informazioni di debug sulla versione e AAA per Cisco Secure ACS for Windows*.

Informazioni correlate

- Esempio di configurazione del failover del controller WLAN per i Lightweight Access Point
- Aggiornamento del software del Wireless LAN Controller (WLC)
- Guida di riferimento ai comandi di Cisco Wireless LAN Controller
- Documentazione e supporto tecnico – Cisco Systems