

Esempio di limitazione dell'accesso WLAN in base al SSID con WLC e Cisco Secure ACS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Installazione della rete](#)

[Configurazione](#)

[Configurare il WLC](#)

[Configurazione di Cisco Secure ACS](#)

[Configurazione del client wireless e verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento offre un esempio di configurazione per limitare l'accesso per utente a una WLAN in base all'identificatore del set di servizi (SSID).

Prerequisiti

Requisiti

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

- Conoscenza di come configurare il controller WLC (Wireless LAN Controller) e il Lightweight Access Point (LAP) per le operazioni di base
- Conoscenze base di come configurare Cisco Secure Access Control Server (ACS)
- Conoscenza dei metodi LWAPP (Lightweight Access Point Protocol) e di sicurezza wireless

Componenti usati

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

- Cisco serie 2000 WLC con firmware 4.0
- Cisco serie 1000 LAP
- Cisco Secure ACS Server versione 3.2
- Cisco 802.11a/b/g Adattatore client wireless con firmware 2.6
- Cisco Aironet Desktop Utility (ADU) versione 2.6

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](#).

Premesse

Utilizzando l'accesso WLAN basato su SSID, gli utenti possono essere autenticati in base all'SSID che utilizzano per connettersi alla WLAN. Il server Cisco Secure ACS viene utilizzato per autenticare gli utenti. L'autenticazione viene effettuata in due fasi su Cisco Secure ACS:

1. autenticazione EAP
2. Autenticazione SSID basata su NAR (Network Access Restrictions) su Cisco Secure ACS

Se l'autenticazione basata su EAP e SSID ha esito positivo, l'utente può accedere alla WLAN oppure viene dissociato.

Cisco Secure ACS utilizza la funzione NAR per limitare l'accesso degli utenti in base all'SSID. Un NAR è una definizione, creata in Cisco Secure ACS, di condizioni aggiuntive che devono essere soddisfatte prima che un utente possa accedere alla rete. Cisco Secure ACS applica queste condizioni utilizzando le informazioni provenienti dagli attributi inviati dai client AAA. Sebbene sia possibile impostare i NAR in diversi modi, tutti i metodi sono basati sulle informazioni sugli attributi corrispondenti inviate dal client AAA. Pertanto, per utilizzare NAR efficaci, è necessario comprendere il formato e il contenuto degli attributi inviati dai client AAA.

Quando si imposta un NAR, è possibile scegliere se il filtro deve funzionare in modo positivo o negativo. In altre parole, nel NAR si specifica se autorizzare o negare l'accesso alla rete, in base a un confronto tra le informazioni inviate dai client AAA e quelle memorizzate nel NAR. Tuttavia, se un NAR non rileva informazioni sufficienti per funzionare, per impostazione predefinita viene negato l'accesso.

È possibile definire un NAR e applicarlo a un utente o gruppo di utenti specifico. Per ulteriori informazioni, consultare il [white paper Limitazioni dell'accesso alla rete](#).

Cisco Secure ACS supporta due tipi di filtri NAR:

1. **Filtri basati su IP:** i filtri NAR basati su IP limitano l'accesso in base agli indirizzi IP del client dell'utente finale e del client AAA. Per ulteriori informazioni su questo tipo di filtro NAR, fare riferimento a [Informazioni sui filtri NAR basati su IP](#).
2. **Filtri non basati su IP:** i filtri NAR non basati su IP limitano l'accesso in base al semplice confronto tra stringhe di un valore inviato dal client AAA. Il valore può essere il numero

dell'ID della linea chiamante (CLI), il numero DNIS (Dialed Number Identification Service), l'indirizzo MAC o un altro valore proveniente dal client. Affinché questo tipo di NAR funzioni, il valore nella descrizione NAR deve corrispondere esattamente a quello inviato dal client, incluso il formato utilizzato. Ad esempio, (217) 555-4534 non corrisponde a 217-555-4534. Per ulteriori informazioni su questo tipo di filtro NAR, fare riferimento a [Informazioni sui filtri NAR non basati su IP](#).

In questo documento vengono usati filtri non basati su IP per eseguire l'autenticazione basata su SSID. Un filtro NAR non basato su IP, ovvero un filtro NAR basato su DNIS/CLI, è un elenco di posizioni di chiamata/punto di accesso consentite o negate che è possibile utilizzare nella restrizione di un client AAA quando non si dispone di una connessione basata su IP stabilita. La funzione NAR non basata su IP utilizza in genere il numero CLI e il numero DNIS. Sono presenti eccezioni nell'utilizzo dei campi DNIS/CLI. È possibile immettere il nome SSID nel campo DNIS ed eseguire l'autenticazione basata su SSID. Infatti, il WLC invia l'attributo DNIS, ovvero il nome SSID, al server RADIUS. Pertanto, se si genera DNIS NAR nell'utente o nel gruppo, è possibile creare restrizioni SSID per utente.

Se si utilizza RADIUS, i campi NAR elencati di seguito utilizzano i valori seguenti:

- **Client AAA:** viene utilizzato l'indirizzo IP-NAS (attributo 4) o, se l'indirizzo IP-NAS non esiste, l'identificatore-NAS (attributo RADIUS 32).
- **Porta:** la porta NAS (attributo 5) o, se la porta NAS non esiste, l'ID della porta NAS (attributo 87).
- **CLI:** viene utilizzato l'ID della stazione chiamante (attributo 31).
- **DNIS** - Viene utilizzato l'attributo 30 denominato station-ID.

Per ulteriori informazioni sull'uso di NAR, fare riferimento a [Restrizioni di accesso alla rete](#).

Poiché il WLC invia l'attributo DNIS e il nome SSID, è possibile creare restrizioni SSID per utente. Nel caso del WLC, i campi NAR hanno i seguenti valori:

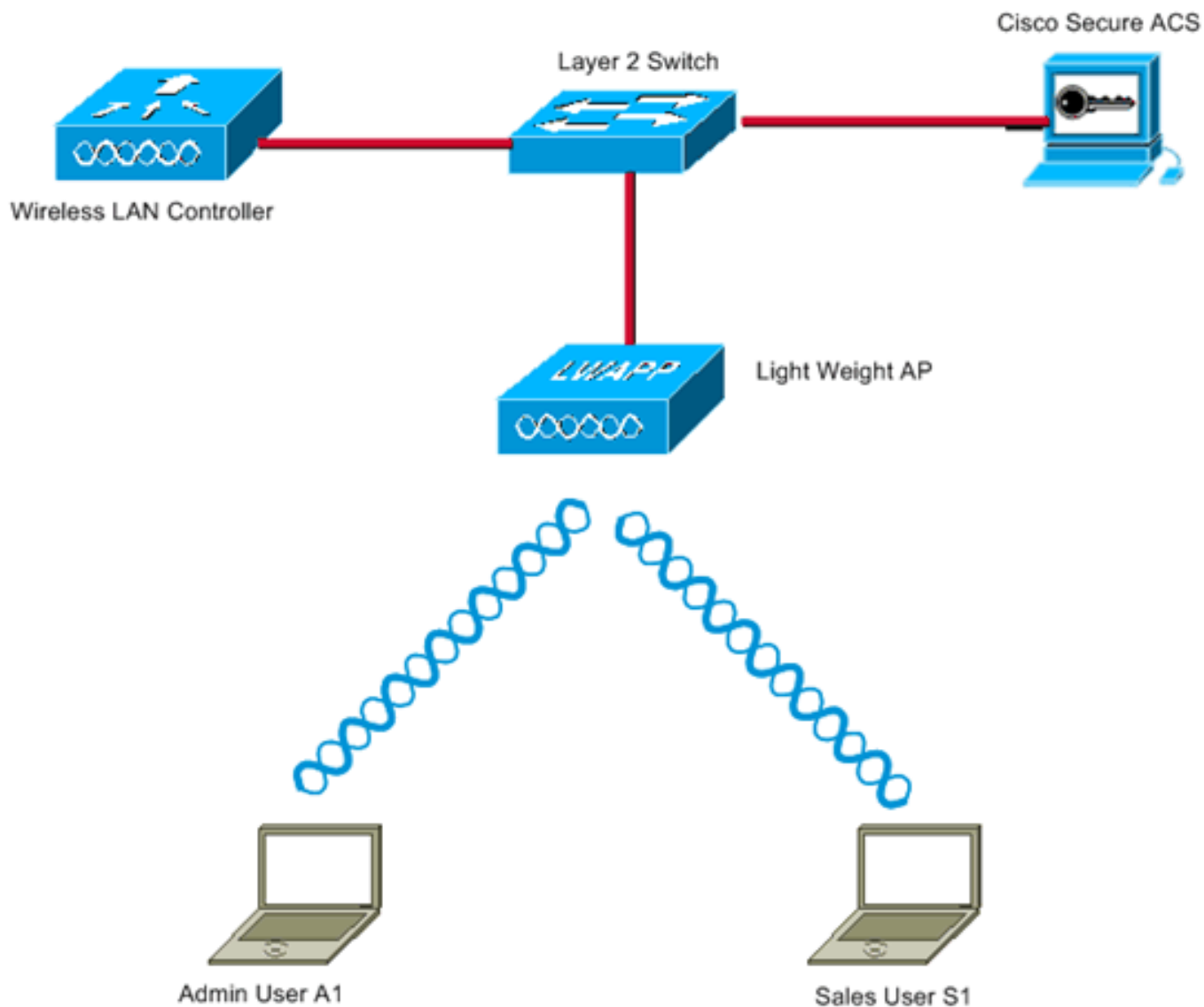
- **Client AAA:** indirizzo IP WLC
- **porta**—*
- **CLI** —*
- **DNIS**—*nomesid

Nella parte restante di questo documento viene fornito un esempio di configurazione.

[Installazione della rete](#)

In questo esempio, il WLC è registrato sul LAP. Vengono utilizzate due WLAN. Una WLAN è destinata agli utenti del reparto amministrativo, l'altra è destinata agli utenti del reparto vendite. Il client wireless A1 (utente Admin) e S1 (utente Sales) si connettono alla rete wireless. È necessario configurare il WLC e il server RADIUS in modo che l'utente Admin A1 possa accedere solo all'**amministratore** WLAN e sia limitato all'accesso alle **vendite** WLAN e l'utente Sales S1 possa accedere alle **vendite** WLAN e abbia limitato l'accesso all'**amministratore** WLAN. Tutti gli utenti utilizzano l'autenticazione LEAP come metodo di autenticazione di livello 2.

Nota: in questo documento si presume che il WLC sia registrato sul controller. Se non si ha familiarità con il WLC e non si sa come configurare il WLC per il funzionamento base, fare riferimento alla [registrazione di un Lightweight AP \(LAP\) su un Wireless LAN Controller \(WLC\)](#).



WLC Management Interface IP address : 172.16.1.30/16

WLC AP-Manager Interface IP address: 172.16.1.31/16

Cisco Secure ACS server IP address: 172.16.1.60/16

SSID for the Admin department users : Admin

SSID for Sales department users: Sales

Configurazione

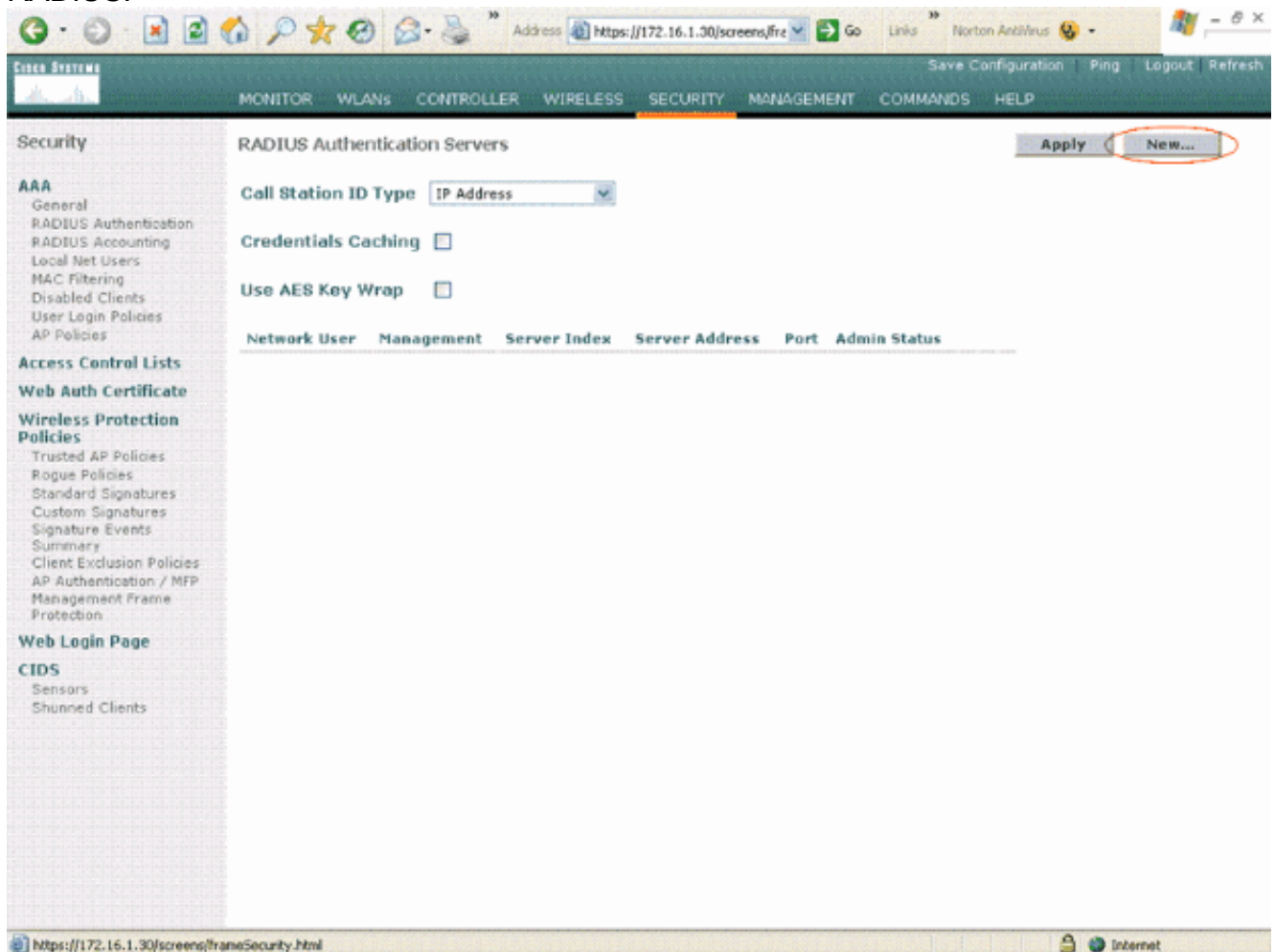
Per configurare i dispositivi per questa installazione, è necessario:

1. [Configurare il WLC per le due WLAN e il server RADIUS.](#)
2. [Configurare Cisco Secure ACS.](#)
3. [Configurare i client wireless e verificare.](#)

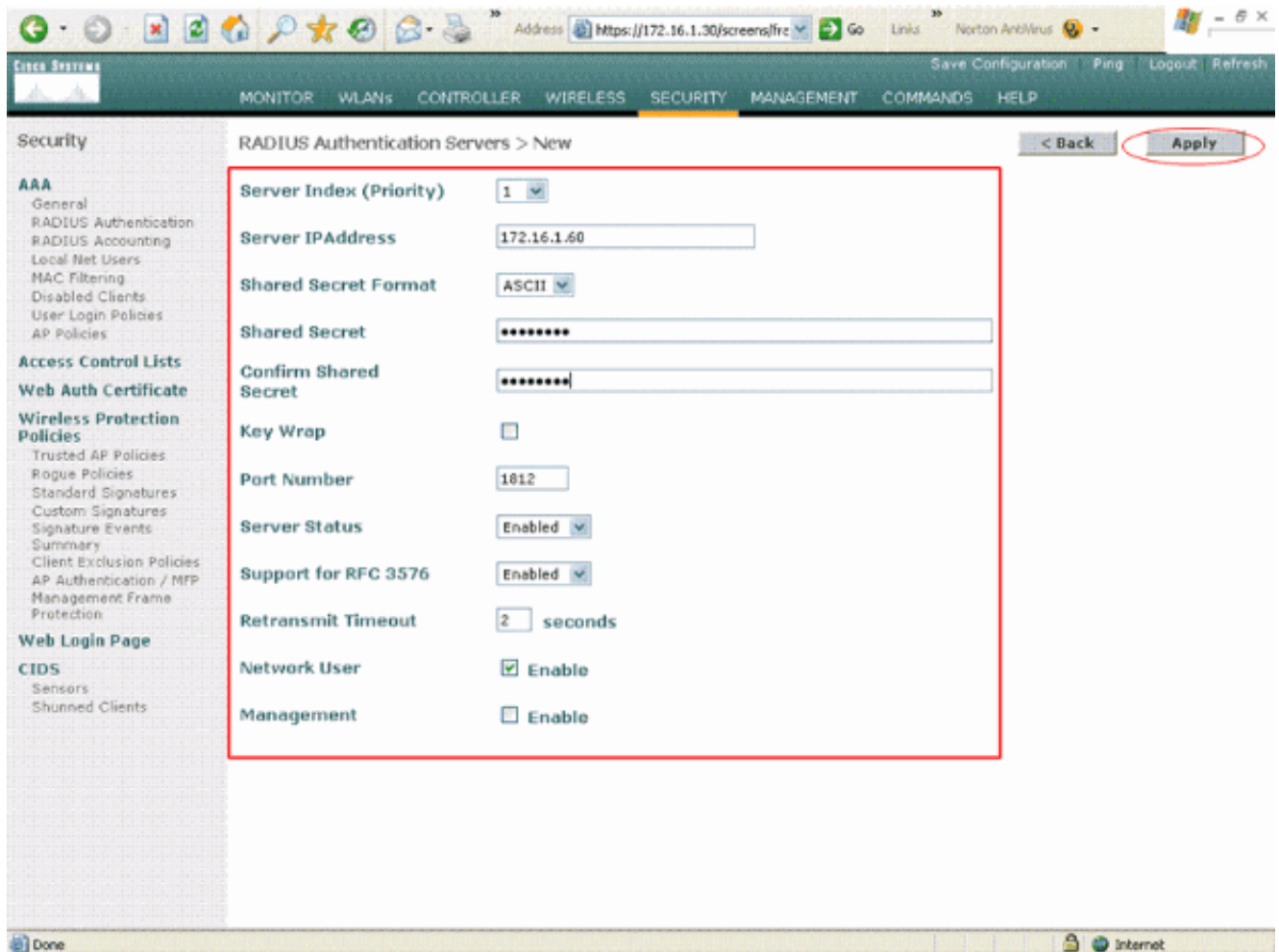
Configurare il WLC

Completare questa procedura per configurare il WLC per questa configurazione:

1. È necessario configurare il WLC per inoltrare le credenziali utente a un server RADIUS esterno. Il server RADIUS esterno (in questo caso Cisco Secure ACS) convalida quindi le credenziali utente e fornisce l'accesso ai client wireless. Attenersi alla seguente procedura: Scegliere **Security > RADIUS Authentication** dall'interfaccia utente del controller per visualizzare la pagina Server di autenticazione RADIUS.

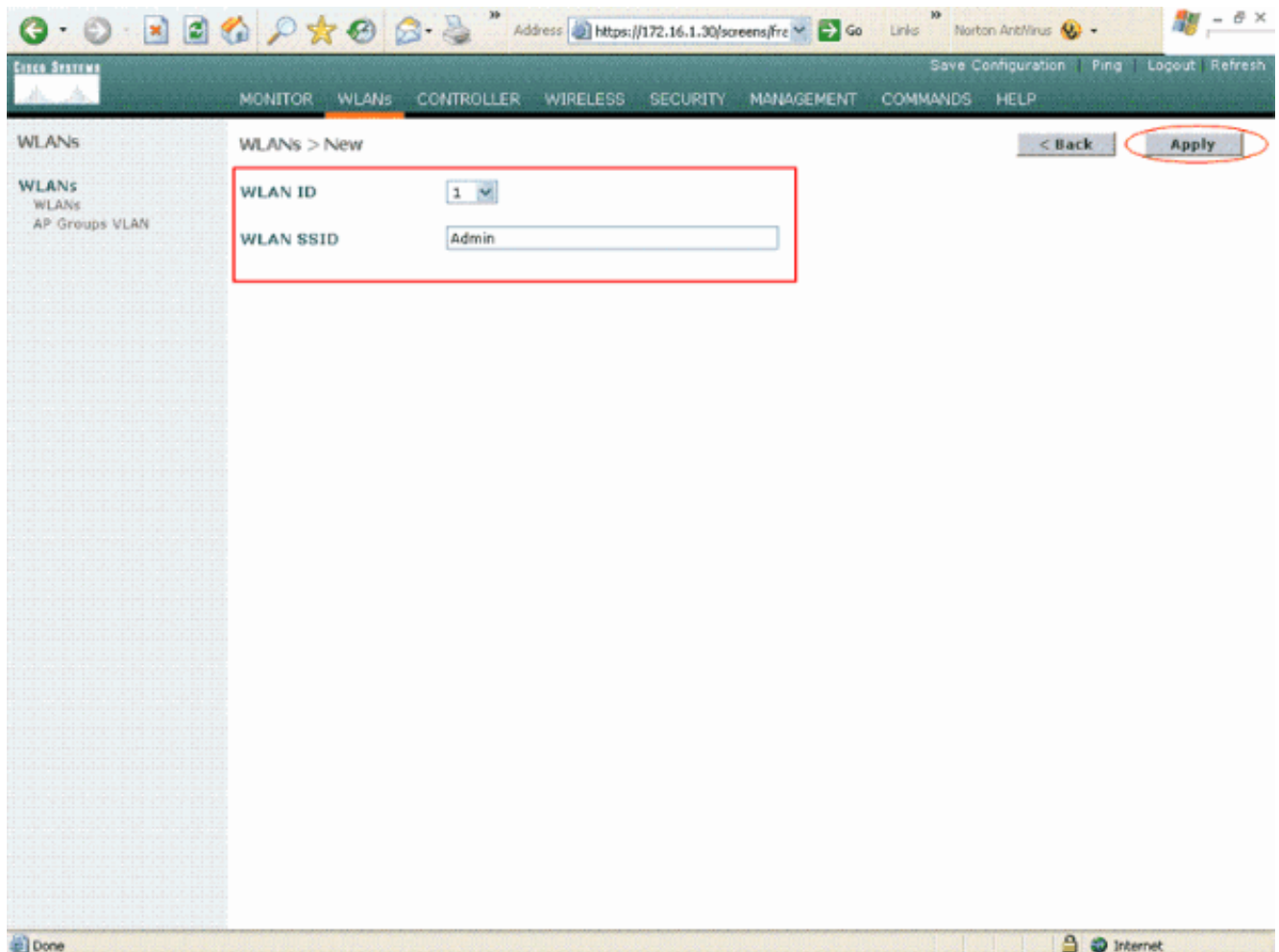


Per definire i parametri del server RADIUS, fare clic su **New** (Nuovo). Questi parametri includono l'indirizzo IP, il segreto condiviso, il numero di porta e lo stato del server RADIUS. Le caselle di controllo Utente di rete e Gestione consentono di determinare se l'autenticazione basata su RADIUS è valida per gli utenti di rete e di gestione. In questo esempio viene utilizzato Cisco Secure ACS come server RADIUS con indirizzo IP 172.16.1.60.

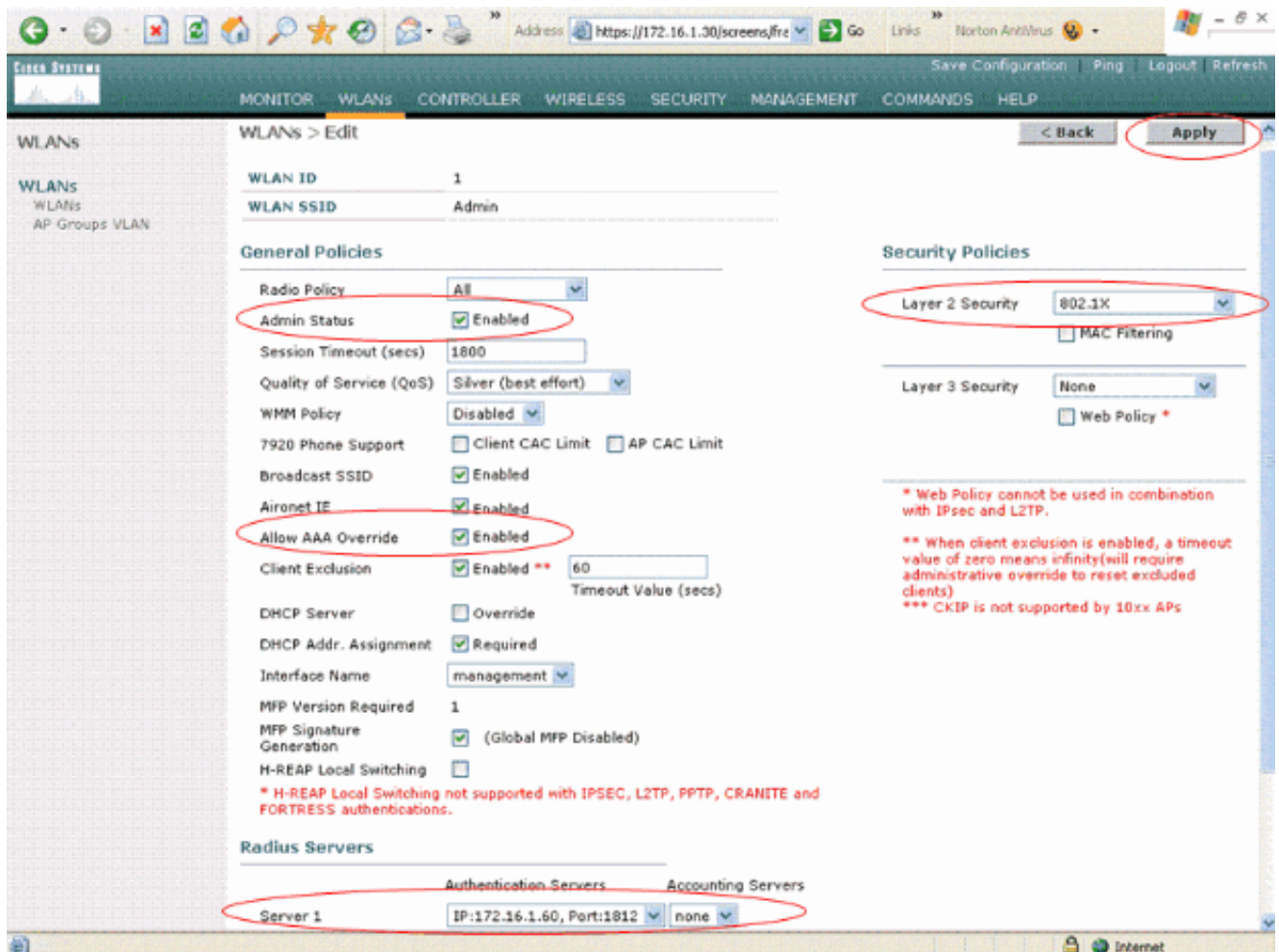


Fare clic su **Apply** (Applica).

2. Configurare una WLAN per il reparto amministrativo con SSID **Admin** e l'altra WLAN per il reparto vendite con SSID **Sales**. A tale scopo, completare i seguenti passaggi: Per creare una WLAN, fare clic su **WLAN** dall'interfaccia utente del controller. Viene visualizzata la finestra WLAN. In questa finestra sono elencate le WLAN configurate sul controller. Per configurare una nuova WLAN, fare clic su **New** (Nuovo). In questo esempio viene creata una WLAN denominata **Admin** per il reparto Admin e l'ID WLAN è 1. Fare clic su **Applica**.



Nella finestra **WLAN > Modifica**, definire i parametri specifici della WLAN: Dal menu a discesa Sicurezza di layer 2, selezionare **802.1x**. Per impostazione predefinita, l'opzione Protezione di livello 2 è 802.1x. Ciò consente l'autenticazione 802.1x/EAP per la WLAN. In Criteri generali selezionare la casella di **selezione alternativa AAA**. Quando l'override AAA è abilitato e un client ha parametri di autenticazione WLAN AAA e controller in conflitto, l'autenticazione client viene eseguita dal server AAA. Selezionare il server RADIUS appropriato dal menu a discesa in Server RADIUS. Gli altri parametri possono essere modificati in base ai requisiti della rete WLAN. Fare clic su **Apply** (Applica).



Analogamente, per creare una WLAN per il reparto vendite, ripetere i passaggi b e c. Ecco gli screenshot.

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

WLANs > New

WLAN ID: 2

WLAN SSID: Sales

< Back | **Apply**

WLANs

WLANs

AP Groups VLAN

Done | Internet

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

WLANs > Edit

WLAN ID: 2

WLAN SSID: Sales

General Policies

Radio Policy: All

Admin Status: Enabled

Session Timeout (secs): 1800

Quality of Service (QoS): Silver (best effort)

WMM Policy: Disabled

7920 Phone Support: Client CAC Limit AP CAC Limit

Broadcast SSID: Enabled

Aironet IE: Enabled

Allow AAA Override: Enabled

Client Exclusion: Enabled ** 60 Timeout Value (secs)

DHCP Server: Override

DHCP Addr. Assignment: Required

Interface Name: management

MFP Version Required: 1

MFP Signature Generation: (Global MFP Disabled)

H-REAP Local Switching:

* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.

Security Policies

Layer 2 Security: 802.1X

MAC Filtering

Layer 3 Security: None

Web Policy *

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

*** CKIP is not supported by 10xx APs

Radius Servers

Authentication Servers | Accounting Servers

Server 1: IP:172.16.1.60, Port:1812 | none

Done | Internet

Configurazione di Cisco Secure ACS

Sul server Cisco Secure ACS è necessario:

1. Configurare il WLC come client AAA.
2. Creare il database utenti e definire NAR per l'autenticazione basata su SSID.
3. Abilitare l'autenticazione EAP.

Completare questi passaggi su Cisco Secure ACS:

1. Per definire il controller come client AAA sul server ACS, fare clic su **Network Configuration** (Configurazione di rete) dall'interfaccia utente di ACS. In Client AAA fare clic su **Add Entry** (Aggiungi voce).

CISCO SYSTEMS Network Configuration

Select

AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

Add Entry Search

AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
tswab-laptop	127.0.0.1	CiscoSecure ACS

Add Entry Search

Back to Help

2. 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).

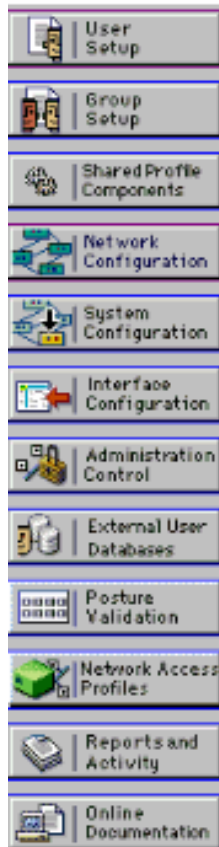
- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Add AAA Client

AAA Client Hostname	<input type="text" value="WLC"/>
AAA Client IP Address	<input type="text" value="172.16.1.30"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco Airespace)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

Back to Help

3. Fare clic su **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 A1.
4. 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 perché questi parametri sono necessari per l'autenticazione LEAP.



User: A1 (New User)

Account Disabled

Supplementary User Info

Real Name
 Description

User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

5. Scorrere la pagina Impostazione utente fino a visualizzare la sezione Limitazioni di accesso alla rete. Nell'interfaccia utente di Limitazione di accesso DNIS/CLI, selezionare **Permitted Calling/Point of Access Locations** e definire i seguenti parametri: **Client AAA**: indirizzo IP WLC (172.16.1.30 nell'esempio) **Porta**—*CLI—*DNIS—*nomesid
6. L'attributo DNIS definisce l'SSID a cui l'utente può accedere. Il WLC invia l'SSID nell'attributo DNIS al server RADIUS. Se l'utente deve accedere solo alla WLAN denominata Admin, immettere *Admin per il campo DNIS. In questo modo, l'utente può accedere solo alla rete WLAN denominata Admin. Fare clic su **Invio**. **Nota**: il SSID deve essere sempre preceduto da *. È obbligatorio.

Advanced Settings

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Network Access Restrictions (NAR) ?

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	Address
remove		

AAA Client: All AAA Clients

Port:

Address:

enter

Define CLI/DNIS-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	CLI	DNIS
remove			

AAA Client: WLC

Port:

CLI:

DNIS:

enter

Submit
Cancel

7. Fare clic su **Invia**.

8. Analogamente, creare un utente per l'utente del reparto vendite. Ecco gli screenshot.



User Setup

Edit

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

User: S1 (New User)

Account Disabled

Supplementary User Info

Real Name
Description

User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

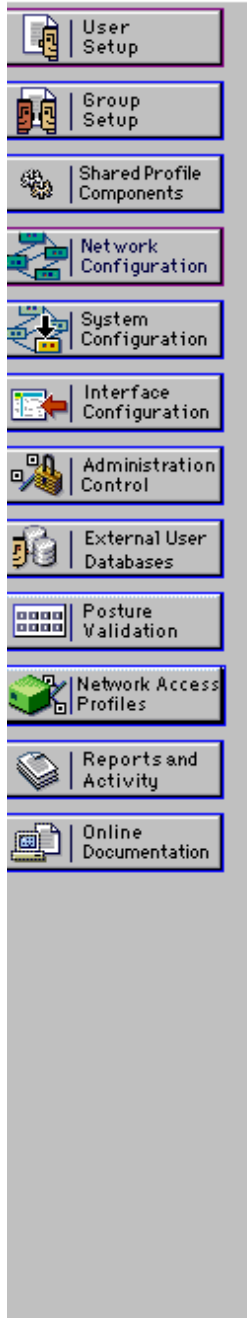
Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:



Network Access Restrictions (NAR) ?

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	Address
remove		

AAA Client: All AAA Clients

Port:

Address:

enter

Define CLI/DNIS-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	CLI	DNIS
remove			

AAA Client: WLC

Port: *

CLI: *

DNIS: *Sales

enter

Submit
Cancel

9. Ripetere la stessa procedura per aggiungere altri utenti al database. **Nota:** per impostazione predefinita, tutti gli utenti sono raggruppati nel gruppo predefinito. Se si desidera assegnare utenti specifici a gruppi diversi, fare riferimento alla sezione [Gestione gruppi utenti](#) della [Guida per l'utente di Cisco Secure ACS per Windows Server 3.2](#). **Nota:** Se la sezione Limitazioni di accesso alla rete non è visualizzata nella finestra Impostazione utente, è possibile che non sia attivata. Per abilitare le Restrizioni di accesso alla rete per gli utenti, scegliere **Interfacce > Opzioni avanzate** dalla GUI di ACS, selezionare **Restrizioni di accesso alla rete a livello utente**, quindi fare clic su **Invia**. In questo modo viene attivato NAR e visualizzato nella finestra Impostazione utente.



Interface Configuration

Edit

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Advanced Options

Note: Only the selected options will appear in the user interface.

- Per-user TACACS+/RADIUS Attributes
- User-Level Shared Network Access Restrictions
- User-Level Network Access Restrictions
- User-Level Downloadable ACLs
- Default Time-of-Day / Day-of-Week Specification
- Group-Level Shared Network Access Restrictions
- Group-Level Network Access Restrictions
- Group-Level Downloadable ACLs
- Group-Level Password Aging
- Network Access Filtering
- Max Sessions
- Usage Quotas
- Distributed System Settings
- Remote Logging
- ACS internal database Replication
- RDBMS Synchronization
- IP Pools
- Network Device Groups
- Voice-over-IP (VoIP) Group Settings
- Voice-over-IP (VoIP) Accounting Configuration
- ODBC Logging

Submit

Cancel

Advanced Settings

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Network Access Restrictions (NAR) ?

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	Address
remove		

AAA Client: All AAA Clients

Port:

Address:

enter

Define CLI/DNIS-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	CLI	DNIS
remove			

AAA Client: WLC

Port:













CLI:

DNIS:

enter

Submit
Cancel

10. Per abilitare l'autenticazione EAP, fare clic su **Configurazione del sistema** e su **Impostazione 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 selezionare il metodo EAP appropriato. In questo esempio viene utilizzata l'autenticazione LEAP. Al termine, fare clic su **Submit** (Invia).

-  User Setup
-  Group Setup
-  Shared Profile Components
-  Network Configuration
-  System Configuration
-  Interface Configuration
-  Administration Control
-  External User Databases
-  Posture Validation
-  Network Access Profiles
-  Reports and Activity
-  Online Documentation

Global Authentication Setup

EAP Configuration ?

PEAP

Allow EAP-MSCHAPv2

Allow EAP-GTC

Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

EAP-FAST

[EAP-FAST Configuration](#)

EAP-TLS

Allow EAP-TLS

Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

LEAP

Allow LEAP (For Aironet only)

EAP-MD5

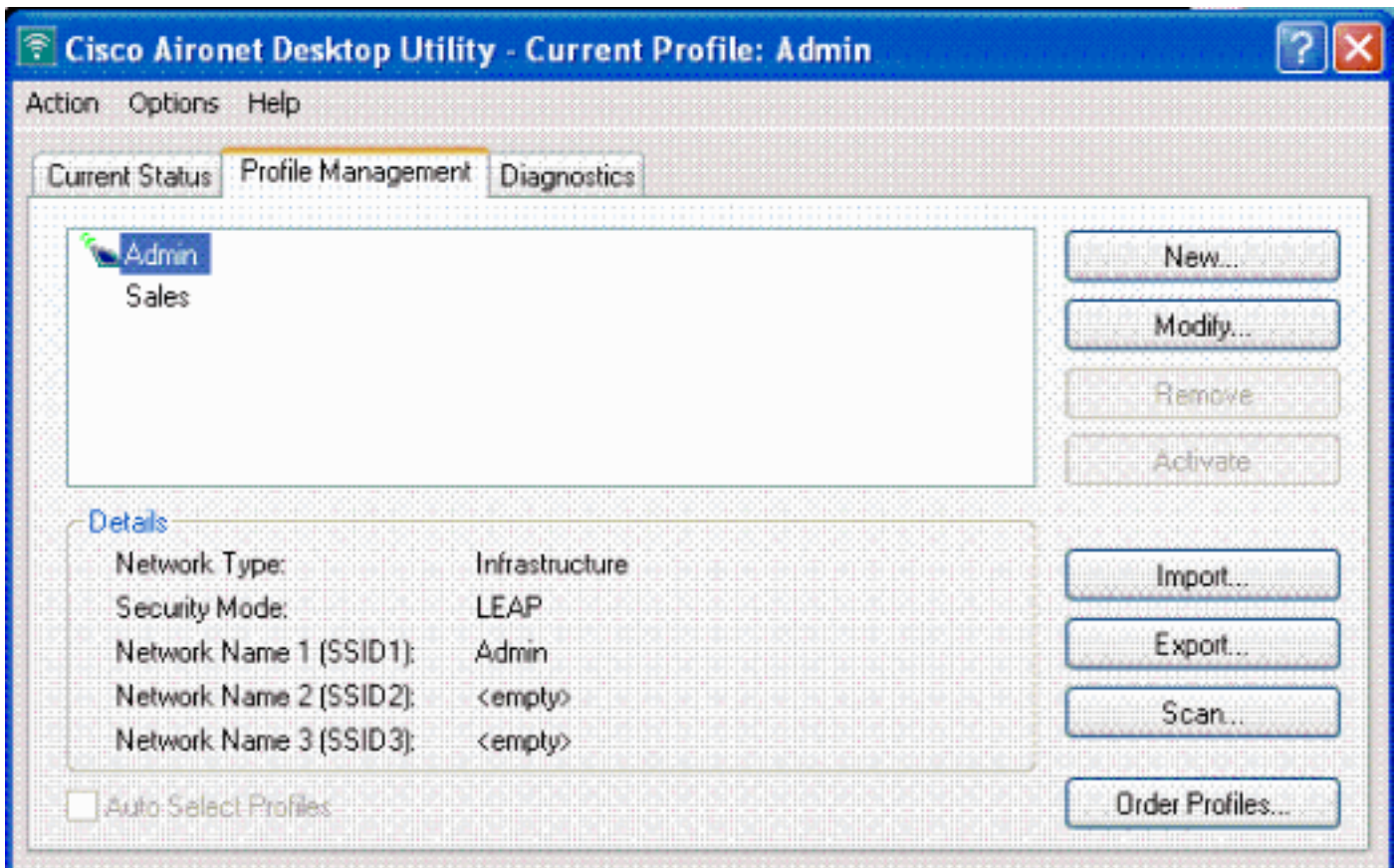
Submit
Submit + Restart
Cancel

Configurazione del client wireless e verifica

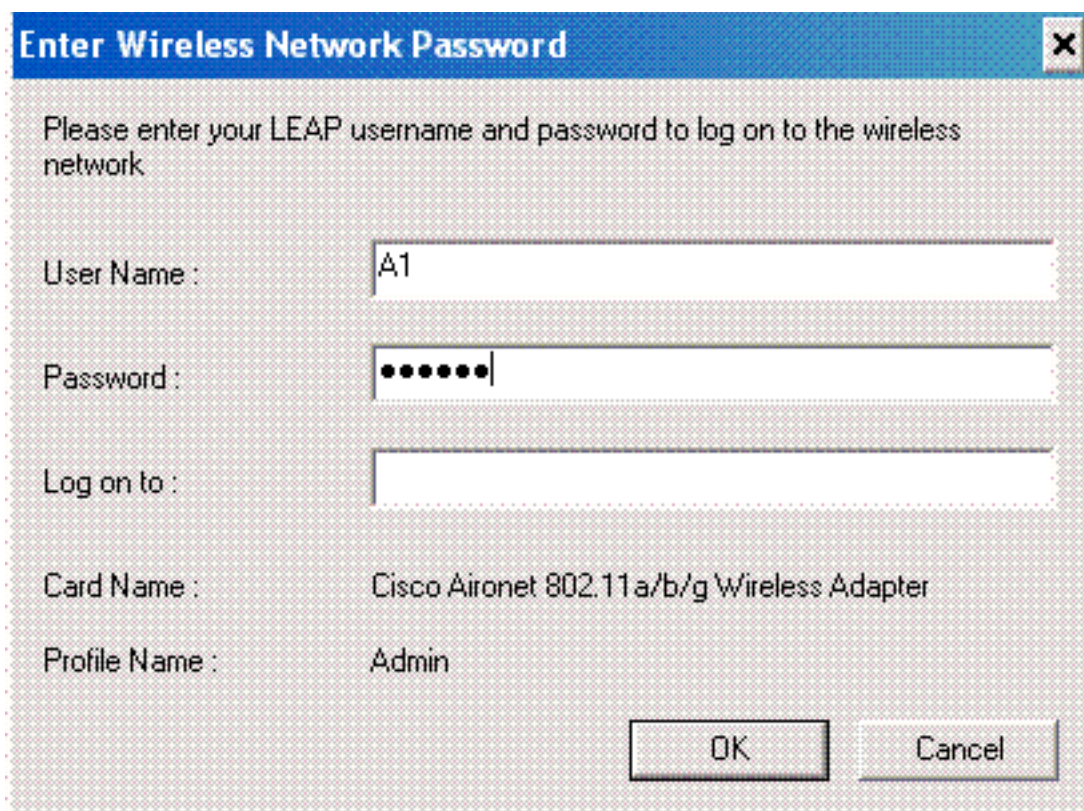
Per verificare che la configurazione funzioni correttamente, consultare questa sezione. Provare ad associare un client wireless al LAP utilizzando l'autenticazione LEAP per verificare se la configurazione funziona come previsto.

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

Nota: dall'ADU si nota che sono stati configurati due profili client. Uno per gli utenti del reparto di amministrazione con **Admin** SSID e l'altro profilo per gli utenti del reparto di vendita con **Sales** SSID. Entrambi i profili sono configurati per l'autenticazione LEAP.



Quando viene attivato il profilo per l'utente wireless del reparto Admin, all'utente viene richiesto di fornire il nome utente/password per l'autenticazione LEAP. Di seguito è riportato un esempio:



Il LAP e quindi il WLC passano le credenziali dell'utente al server RADIUS esterno (Cisco Secure ACS) per convalidarle. Il WLC passa le credenziali, incluso l'attributo DNIS (nome SSID), al server RADIUS per la convalida.

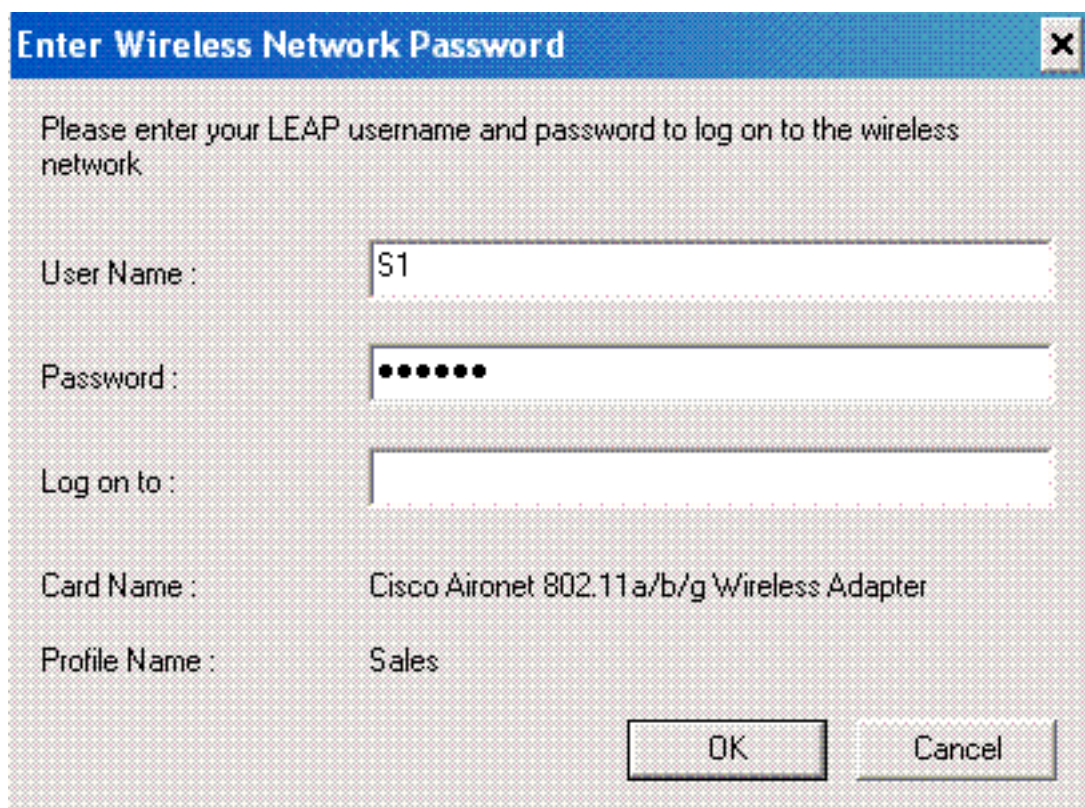
Il server RADIUS verifica le credenziali dell'utente confrontando i dati con il database utente (e i

NAR) e fornisce l'accesso al client wireless ogni volta che le credenziali dell'utente sono valide.

Se l'autenticazione RADIUS ha esito positivo, il client wireless si associa al LAP.



Analogamente, quando un utente del reparto vendite attiva il profilo Sales, l'utente viene autenticato dal server RADIUS in base al nome utente/password LEAP e al SSID.



Il report Autenticazione passata sul server ACS indica che il client ha superato l'autenticazione RADIUS (autenticazione EAP e SSID). Di seguito è riportato un esempio:

Reports and Activity

Select

Passed Authentications active.csv Refresh Download

Regular Expression Start Date & Time End Date & Time Rows per Page

Apply Filter Clear Filter

Filtering is not applied.

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address	Network Access Profile Name	Shared BAC	Downloadable ACL	System-Posture-Token	Application-Posture-Token	Reason	EAP Type	EAP Type Name
10/11/2006	14:48:40	Authen OK	S1	Default Group	00-40-9E-9E-57	1	172.16.1.30	(Default)	17	LEAP
10/11/2006	14:47:05	Authen OK	A1	Default Group	00-40-9E-9E-57	1	172.16.1.30	(Default)	17	LEAP

A questo punto, se l'utente delle vendite tenta di accedere al SSID **Admin**, il server RADIUS nega all'utente l'accesso alla WLAN. Di seguito è riportato un esempio:



In questo modo è possibile limitare l'accesso degli utenti in base al SSID. In un ambiente aziendale, tutti gli utenti che appartengono a un reparto specifico possono essere raggruppati in un unico gruppo e l'accesso alla WLAN può essere fornito in base all'SSID utilizzato, come spiegato in questo documento.

Risoluzione dei problemi

Comandi per la risoluzione dei problemi

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di **debug**.

- **debug dot1x aaa enable:** abilita il debug delle interazioni 802.1x AAA.
- **debug dot1x packet enable:** abilita il debug di tutti i pacchetti dot1x.

- **debug aaa all enable**: configura il debug di tutti i messaggi AAA.

Per risolvere i problemi di configurazione, è inoltre possibile utilizzare il report Autenticazione passata e il report Autenticazione non riuscita sul server Cisco Secure ACS. Questi rapporti si trovano nella finestra **Rapporti e attività** sull'interfaccia grafica ACS.

[Informazioni correlate](#)

- [Esempio di configurazione dell'autenticazione EAP con i controller WLAN \(WLC\)](#)
- [Esempio di configurazione dell'autenticazione Web del controller LAN wireless](#)
- [Esempio di configurazione di VLAN di gruppo AP con controller LAN wireless](#)
- [Pagina di supporto wireless](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)