

Restrinja el acceso de la red inalámbrica (WLAN) basado en el SSID con el WLC y el ejemplo de configuración del Cisco Secure ACS

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configuración de la red](#)

[Configurar](#)

[Configure el WLC](#)

[Configure el Cisco Secure ACS](#)

[Configure al cliente de red inalámbrica y verifíquelo](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona un ejemplo de configuración para restringir el acceso por usuario a una WLAN basada en el SSID (Service Set Identifier).

[prerrequisitos](#)

[Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar el regulador del Wireless LAN (WLC) y el Lightweight Access Point (REVESTIMIENTO) para la operación básica
- Conocimiento básico en cómo configurar el Cisco Secure Access Control Server (ACS)
- Conocimiento de los métodos del protocolo (LWAPP) y de la seguridad de red inalámbrica del Lightweight Access Point

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC de las Cisco 2000 Series que funciona con el firmware 4.0
- REVESTIMIENTO de las Cisco 1000 Series
- Versión del servidor 3.2 del Cisco Secure ACS
- Adaptador de red inalámbrica de cliente de Cisco 802.11a/b/g que funciona con el firmware 2.6
- Versión 2.6 de la utilidad de escritorio del Cisco Aironet (ADU)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

[Antecedentes](#)

Con el uso del acceso SSID-basado de la red inalámbrica (WLAN), los usuarios pueden ser autenticados sobre la base del SSID que utilizan para conectar con la red inalámbrica (WLAN). El servidor del Cisco Secure ACS se utiliza para autenticar a los usuarios. La autenticación sucede en dos etapas en el Cisco Secure ACS:

1. Autenticación EAP
2. Autenticación SSID basada en las restricciones del acceso a la red (NAR) en el Cisco Secure ACS

Si el EAP y la autenticación SSID-basada son acertados, se permite al usuario acceder la red inalámbrica (WLAN) o bien desasocian al usuario.

El Cisco Secure ACS utiliza la característica NAR para restringir el acceso del usuario basado en el SSID. Un NAR es una definición, que usted hace en el Cisco Secure ACS, de las condiciones adicionales que deben ser cumplidas antes de que un usuario pueda acceder la red. El Cisco Secure ACS aplica estas condiciones usando la información de los atributos enviados por sus clientes AAA. Aunque haya varias maneras que usted puede configurar los NAR, todos se basan en la información de atributo que corresponde con enviada por el cliente AAA. Por lo tanto, usted debe entender que el formato y el contenido de los atributos que sus clientes AAA envían si usted quiere emplear los NAR eficaces.

Cuando usted configura un NAR, usted puede elegir si el filtro actúa positivamente o negativamente. Es decir, en el NAR usted especifica si al acceso a la red del permit or deny, sobre la base de una comparación de la información enviada de los clientes AAA a la información salvada en el NAR. Sin embargo, si un NAR no encuentra la información suficiente para actuar, omite el acceso negado.

Usted puede definir un NAR para, y aplica lo, a un usuario o a un grupo de usuarios específico. Refiera al [White Paper de las restricciones del acceso a la red](#) para más información.

El Cisco Secure ACS apoya dos tipos de filtros NAR:

1. **Filtros basados en IP** — Acceso basado en IP del límite de los filtros NAR basado sobre los IP Addresses del cliente del usuario final y del cliente AAA. Refiérase [sobre los filtros basados en IP NAR](#) para más información sobre este tipo de filtro NAR.
2. **filtros NON-IP-basados** — acceso NON-IP-basado del límite de los filtros NAR basado sobre la comparación de cadenas simple de un valor enviado del cliente AAA. El valor puede ser el número de la línea de llamada ID (CLI), el número del Dialed Number Identification Service (DNIS), la dirección MAC, o el otro valor que origina del cliente. Para este tipo de NAR a actuar, el valor en la descripción NAR debe hacer juego exactamente incluyendo qué se envía del cliente, se utiliza cualquier formato. Por ejemplo, el (217) 555-4534 no hace juego 217-555-4534. Refiérase [sobre los filtros NON-IP-basados NAR](#) para más información sobre este tipo de filtro NAR.

Este documento utiliza los filtros NON-IP-basados para hacer la autenticación SSID-basada. Un filtro NON-IP-basado NAR (es decir, un filtro DNIS/CLI-based NAR) es una lista de permitido o el Denied Calling/Point of Access Locations que usted puede utilizar en la restricción de un cliente AAA cuando usted no tiene una conexión basada en IP establecida. La característica NON-IP-basada NAR utiliza generalmente el número CLI y el número DNIS. Hay excepciones en el uso de los campos DNIS/CLI. Usted puede ingresar el nombre SSID en el campo DNIS y hace autenticación SSID-basada. Esto está porque el WLC envía en el atributo DNIS, el nombre SSID, al servidor de RADIUS. Tan si usted construye DNIS NAR en el usuario o el grupo, usted puede crear por usuario las restricciones SSID.

Si usted utiliza el RADIUS, los campos NAR enumerados aquí utilizan estos valores:

- **Cliente AAA** — El Nas-ip-address (se utiliza el atributo 4) o, si no existe el Nas-ip-address, el NAS-identificador (atributo de RADIUS 32).
- **Puerto** — El NAS-puerto (se utiliza el atributo 5) o, si no existe el NAS-puerto, el nas-port-id (atributo 87).
- **CLI** — Se utiliza El llamar-estación-ID (atributo 31).
- **DNIS** — Se utiliza El llamar-estación-ID (atributo 30).

Refiera a las [restricciones del acceso a la red](#) para más información sobre el uso del NAR.

Puesto que el WLC envía en el atributo DNIS y el nombre SSID, usted puede crear por usuario las restricciones SSID. En el caso del WLC, los campos NAR tienen estos valores:

- **Cliente AAA** — Dirección IP del WLC
- **puerto** — *
- **CLI** — *
- **DNIS** — *ssidname

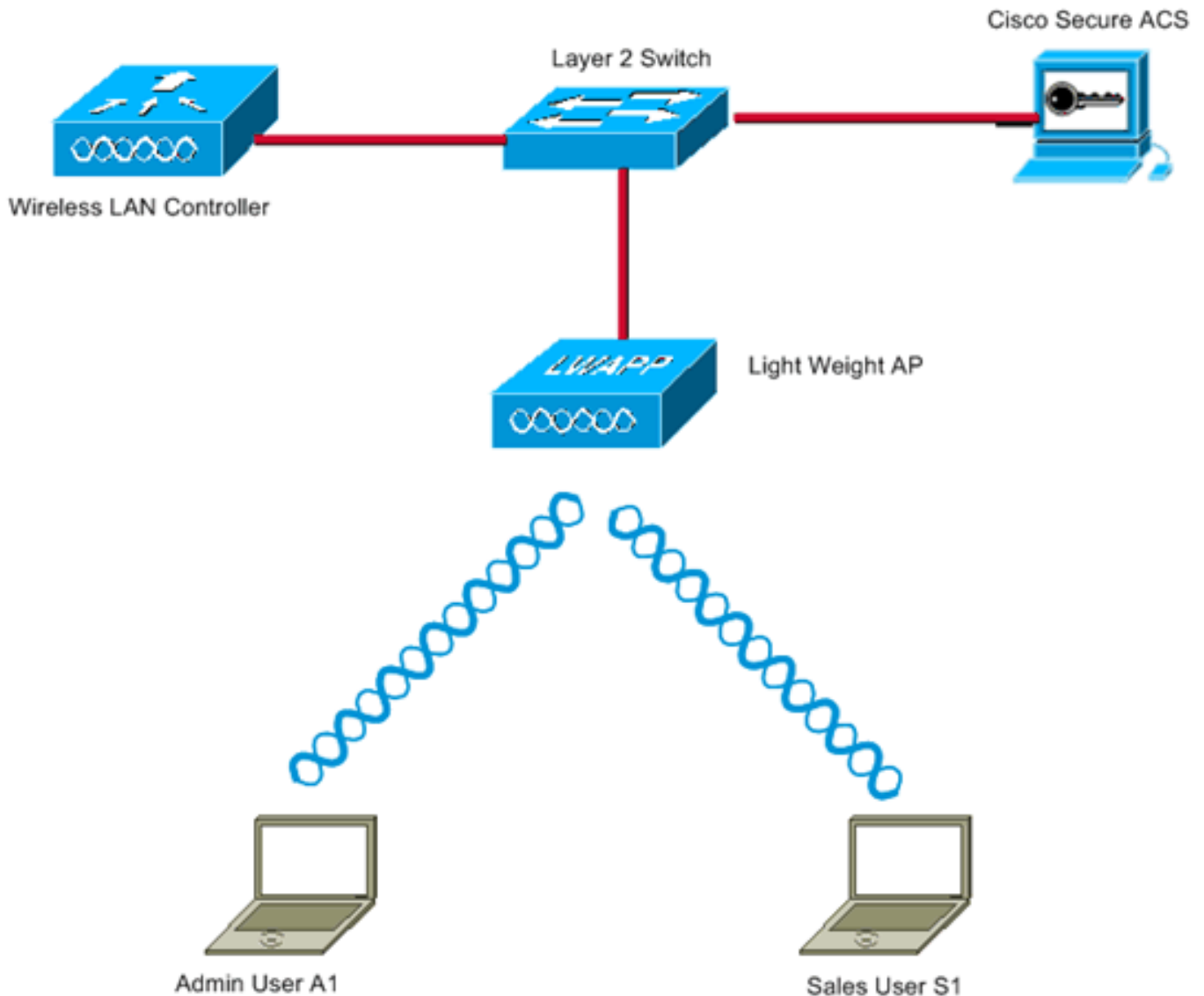
El recordatorio de este documento proporciona un ejemplo de configuración en cómo lograr esto.

[Configuración de la red](#)

En esta configuración del ejemplo, el WLC se registra al REVESTIMIENTO. Se utilizan dos WLAN. Una red inalámbrica (WLAN) está para los usuarios del departamento administrativos y la otra red inalámbrica (WLAN) está para los usuarios del Departamento de ventas. El cliente de red inalámbrica A1 (Usuario administrador) y el s1 (usuario de las ventas) conectan con la red inalámbrica. Usted necesita configurar el WLC y el servidor de RADIUS de una manera tal que el

Usuario administrador A1 pueda acceder solamente la red inalámbrica (WLAN) **Admin** y sea acceso restringido a las **ventas de la** red inalámbrica (WLAN) y al s1 del usuario de las ventas debe poder acceder las **ventas de la** red inalámbrica (WLAN) y debe tener acceso restringido a la red inalámbrica (WLAN) **Admin**. Todos los usuarios utilizan la autenticación LEAP como método de autenticación de la capa 2.

Nota: Este documento asume que el WLC está registrado al regulador. Si usted es nuevo al WLC y no sabe configurar el WLC para la operación básica, refiere al [registro ligero AP \(REVESTIMIENTO\) a un regulador del Wireless LAN \(WLC\)](#).



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

Configurar

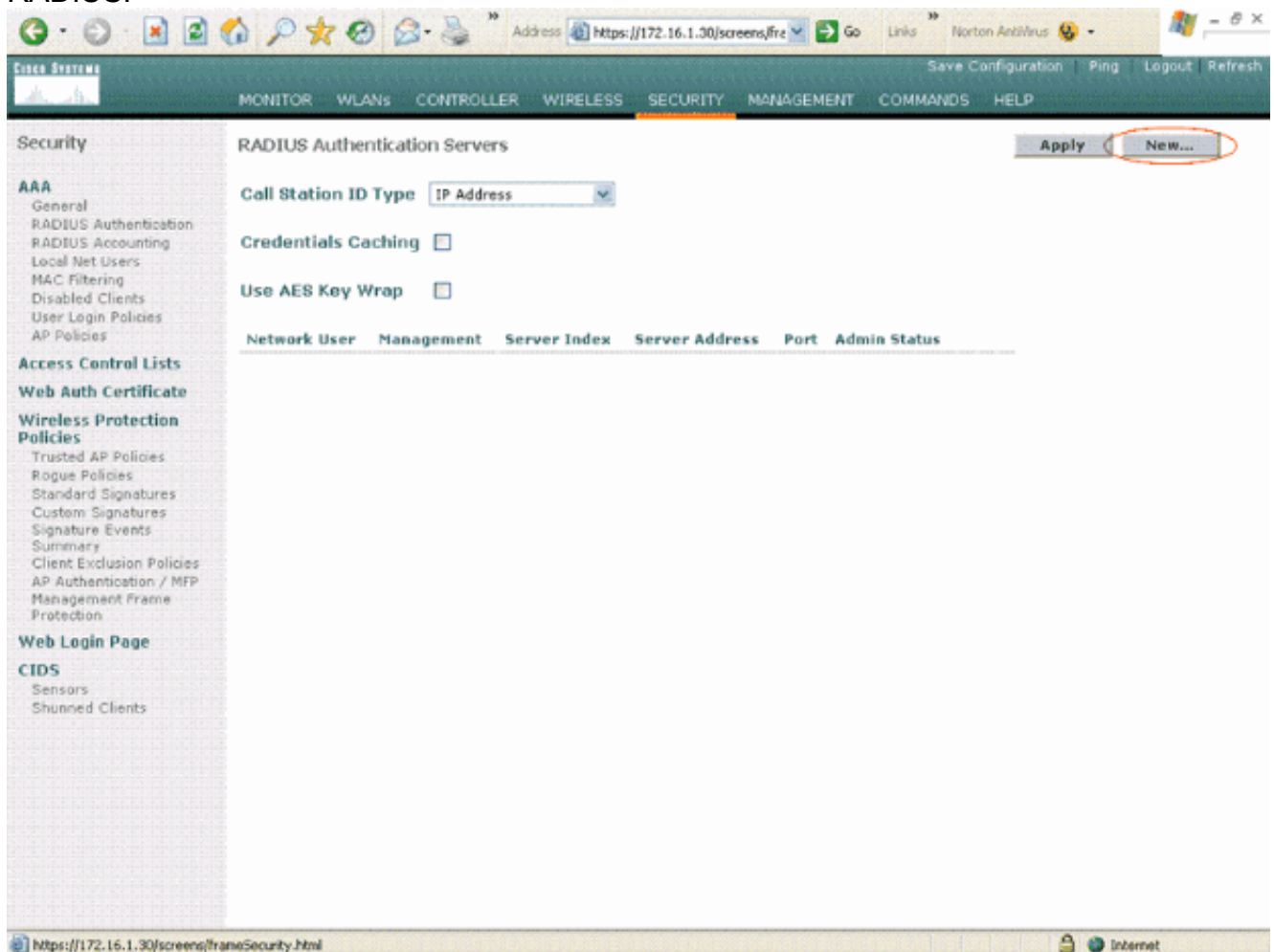
Para configurar los dispositivos para esta configuración, usted necesita:

1. [Configure el WLC para los dos WLAN y servidores de RADIUS.](#)
2. [Configure el Cisco Secure ACS.](#)
3. [Configure a los clientes de red inalámbrica y verifíquelos.](#)

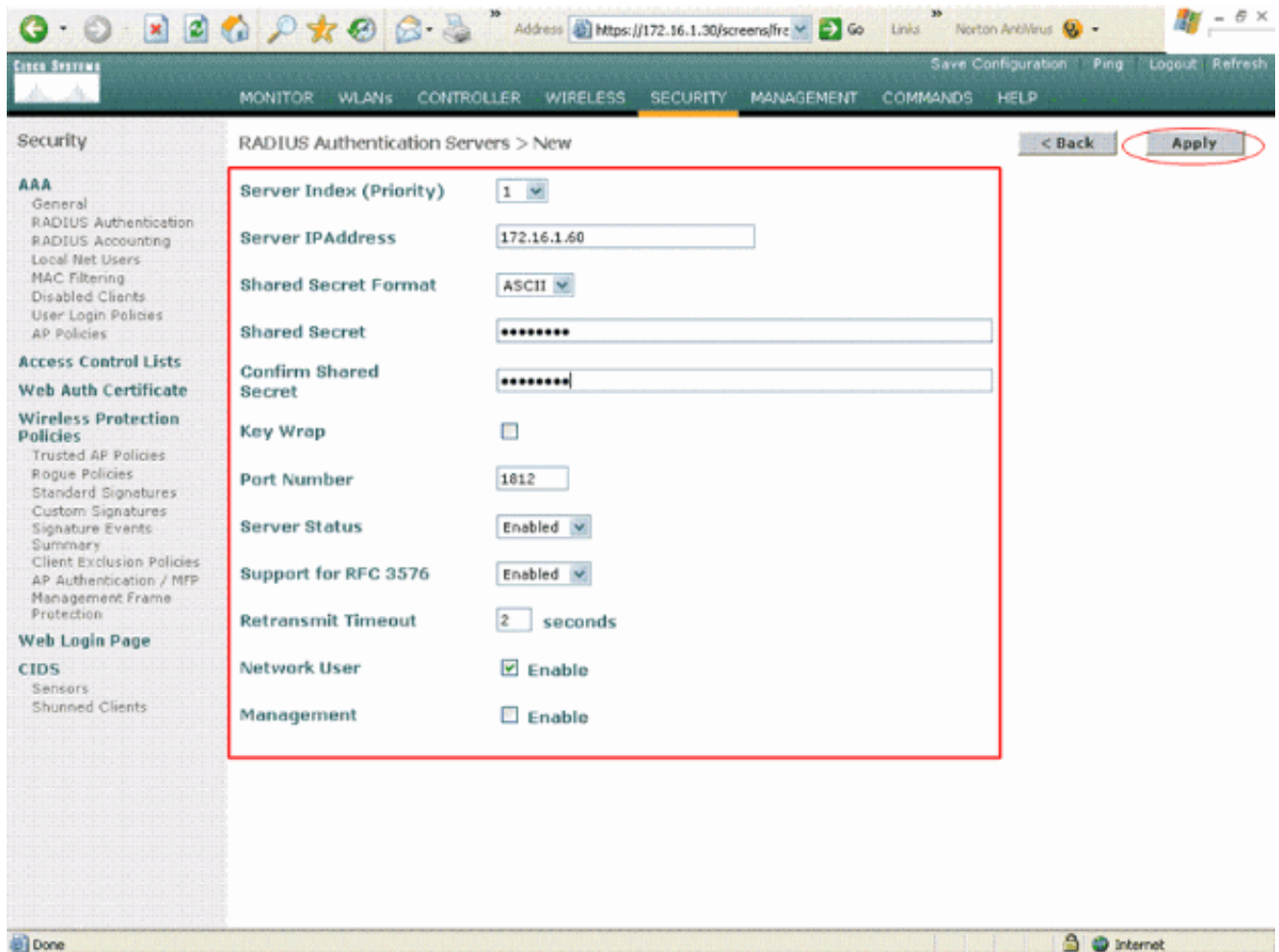
Configure el WLC

Complete estos pasos para configurar el WLC para esta configuración:

1. El WLC necesita ser configurado para remitir los credenciales de usuario a un servidor RADIUS externo. El servidor RADIUS externo (Cisco Secure ACS en este caso) después valida los credenciales de usuario y proporciona el acceso a los clientes de red inalámbrica. Complete estos pasos: Elija la **Seguridad** > la **autenticación de RADIUS** del regulador GUI para visualizar la página de los servidores de autenticación de RADIUS.

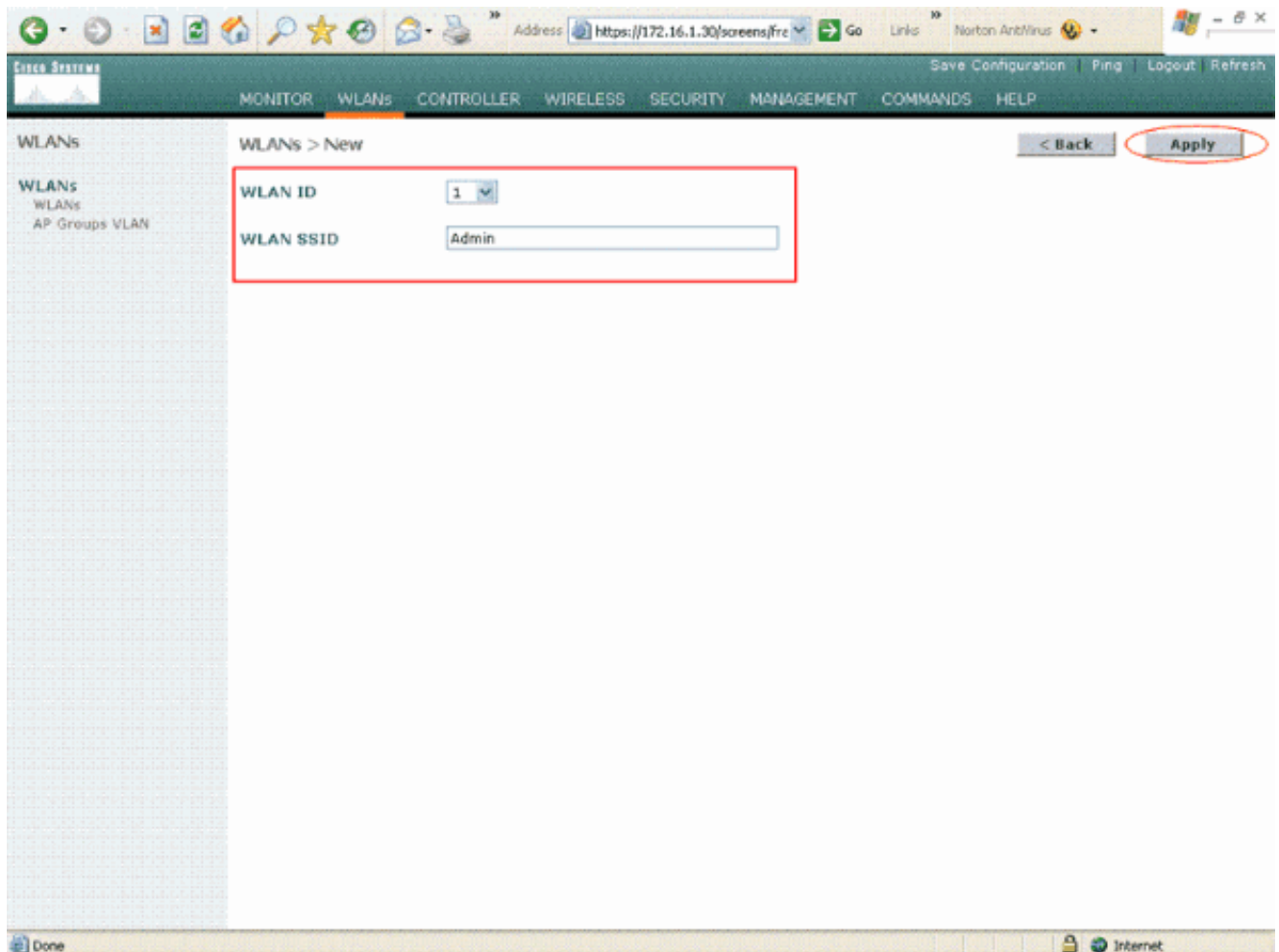


Haga clic **nuevo** para definir los parámetros del servidor de RADIUS. Estos parámetros incluyen la dirección IP, el secreto compartido, el número del puerto, y el estado del servidor del servidor de RADIUS. Las casillas de verificación del usuario de la red y de la Administración determinan si la autenticación basada en RADIUS solicita la Administración y los usuarios de la red. Este ejemplo utiliza el Cisco Secure ACS como el servidor de RADIUS con la dirección IP 172.16.1.60.

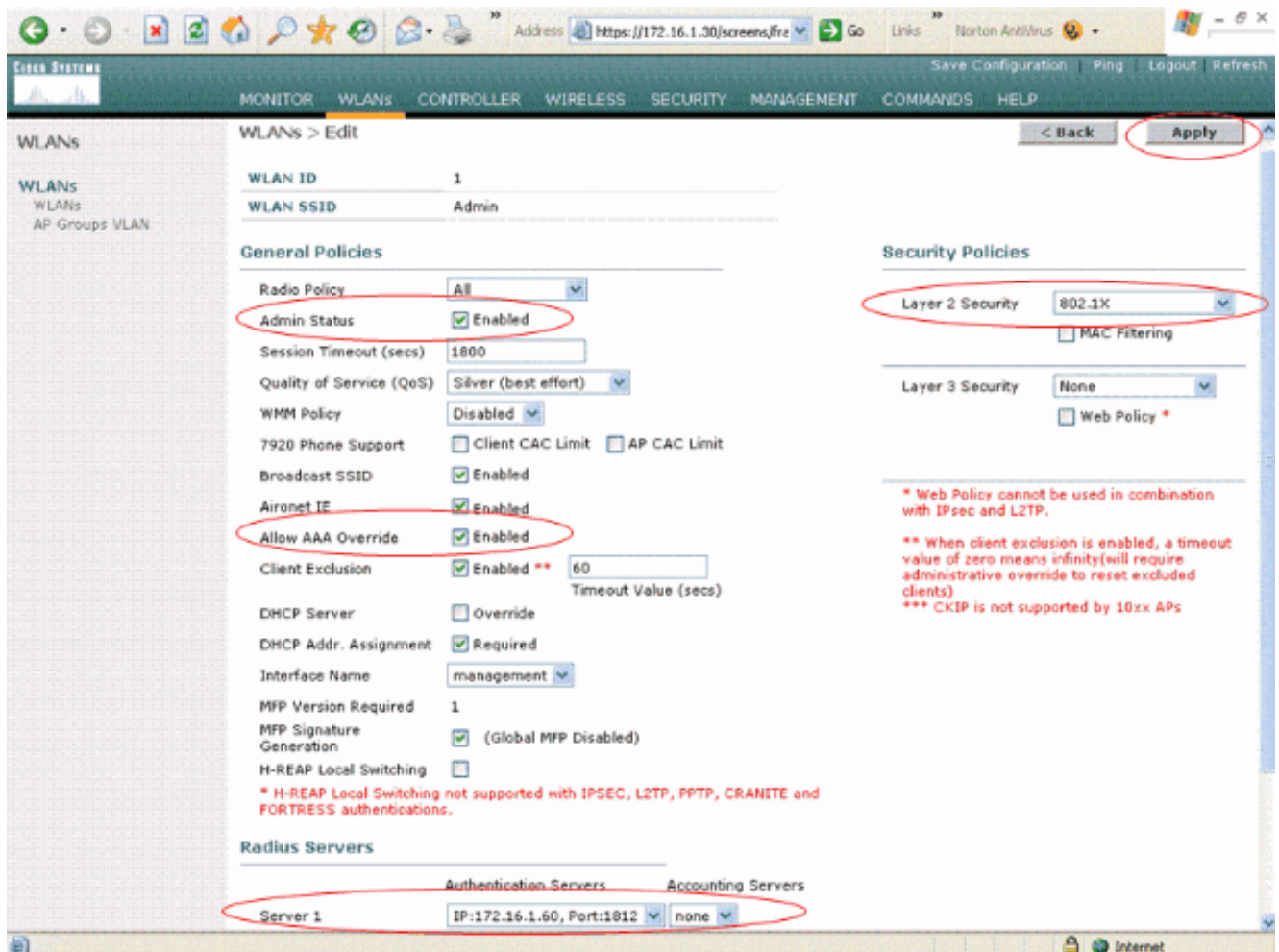


Haga clic en Apply (Aplicar).

2. Configure la una red inalámbrica (WLAN) para el departamento de administración con SSID **Admin** y la otra red inalámbrica (WLAN) para el Departamento de ventas con las **ventas** SSID. Para hacerlo, complete estos pasos:Haga clic los **WLAN del** regulador GUI para crear una red inalámbrica (WLAN). La ventana del WLAN aparece. Esta ventana enumera los WLAN configurados en el regulador.Tecleo **nuevo** para configurar una nueva red inalámbrica (WLAN).Este ejemplo crea una red inalámbrica (WLAN) nombrada **Admin** para el departamento de administración y el ID DE WLAN es 1. tecleos **se aplica**.



En la red inalámbrica (WLAN) > edite la ventana, definen los parámetros específicos a la red inalámbrica (WLAN): Del menú desplegable de la Seguridad de la capa 2, seleccione el **802.1x**. Por abandono, la opción de seguridad de la capa 2 es 802.1x. Esto habilita la autenticación 802.1x/EAP para la red inalámbrica (WLAN). Bajo políticas generales, marque el cuadro de la **invalidación AAA**. Cuando se habilita la invalidación AAA, y un cliente tiene parámetros de autenticación de la red inalámbrica (WLAN) AAA que están en conflicto y del regulador, la autenticación de cliente es realizada por el servidor de AAA. Seleccione al servidor de RADIUS apropiado del menú desplegable bajo los servidores de RADIUS. Los otros parámetros se pueden modificar basaron en el requisito de la red WLAN. Haga clic en Apply (Aplicar).



Semejantemente, para crear una red inalámbrica (WLAN) para el Departamento de ventas, relance los pasos b y C. Aquí está el screenshots.

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

[Cisco Secure ACS de la configuración](#)

En el servidor del Cisco Secure ACS usted necesita:

1. Configure el WLC como cliente AAA.
2. Cree la base de datos de usuarios y defina el NAR para la autenticación SSID-basada.
3. Habilite la autenticación EAP.

Complete estos pasos en el Cisco Secure ACS:













1. Para definir el regulador como cliente AAA en el servidor ACS, haga clic la **configuración de red del ACS GUI**. Bajo los clientes AAA haga clic en **agregar la entrada**.

The screenshot displays the Cisco Secure ACS Network Configuration interface. On the left is a navigation sidebar with icons for User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Feature Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'Network Configuration' and has a 'Select' dropdown menu. Below this, there are two main sections: 'AAA Clients' and 'AAA Servers'. The 'AAA Clients' section shows a table with columns 'AAA Client Hostname', 'AAA Client IP Address', and 'Authenticate Using', with the text 'None Defined' below it. The 'AAA Servers' section shows a table with columns 'AAA Server Name', 'AAA Server IP Address', and 'AAA Server Type', with one entry: 'tsweb-laptop' with IP '127.0.0.1' and type 'CiscoSecure ACS'. Both sections have 'Add Entry' and 'Search' buttons. At the bottom, there is a 'Back to Help' button.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		


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

2. Cuando aparece la página de la configuración de red, defina el nombre del WLC, de la dirección IP, del secreto compartido y del método de autenticación (Airespace RADIUS Cisco).

-  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. Haga clic la **configuración de usuario del ACS GUI**, ingrese el nombre de usuario, y el tecleo **agrega/edita**. En este ejemplo el usuario es A1.
4. Cuando aparece la página de la configuración de usuario, defina todos los parámetros específicos al usuario. En este ejemplo se configuran el nombre de usuario, la contraseña y la información del usuario suplementaria porque usted necesita estos parámetros para la autenticación LEAP.

- 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: 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. Navegue hacia abajo la página de la configuración de usuario, hasta que usted vea la sección de las restricciones del acceso a la red. Bajo interfaz de usuario de la restricción de acceso DNIS/CLI, el **Permitted Calling/Point of Access Locations** selecto y define estos parámetros: **Cliente AAA** — Dirección IP del WLC (172.16.1.30 en nuestro ejemplo) **Puerto** — ***CLI** — ***DNIS** — ***ssidname**
6. El atributo DNIS define el SSID que se permite al usuario acceder. El WLC envía el SSID en el atributo DNIS al servidor de RADIUS. Si el usuario necesita acceder solamente el Admin nombrado WLAN, ingrese el ***Admin** para el campo DNIS. Esto se asegura de que el usuario tenga acceso solamente a la red inalámbrica (WLAN) nombrada Admin. El teclado **ingresa**. **Nota:** El SSID se debe preceder siempre con *. Es obligatorio.

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. Haga clic en Submit (Enviar).

8. Semejantemente, cree a un usuario para el usuario del Departamento de ventas. Aquí está el screenshots.



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

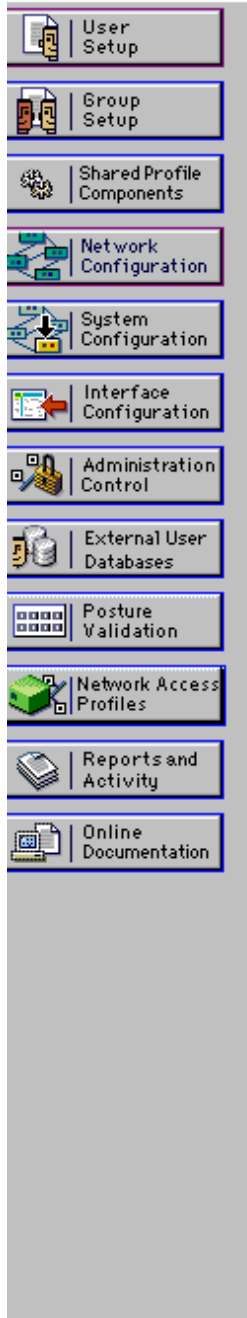
Separate (CHAP/MS-CHAP/ARAP)

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. Relance el mismo proceso para agregar a más usuarios a la base de datos. **Nota:** Por abandono agrupan a todos los usuarios bajo grupo predeterminado. Si usted quiere asignar a los usuarios específicos a diversos grupos, refiera a la [sección de administración del grupo de usuarios del guía del usuario para el servidor 3.2 del Cisco Secure ACS for Windows](#). **Nota:** Si usted no ve la sección de las restricciones del acceso a la red en la ventana de la configuración de usuario, puede ser que sea porque no se habilita. Para habilitar las restricciones del acceso a la red para los usuarios, elegir las **interfaces > avanzó las opciones del ACS GUI, las restricciones selectas del acceso a la red del nivel de usuario** y el tecleo **somete**. Esto habilita el NAR y aparece en la ventana de la configuración de usuario.



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. Para habilitar la autenticación EAP, la **configuración del sistema del teclado** y la **autenticación global ponen** para asegurarse de que configuran al servidor de autenticación para realizar el método de autenticación EAP deseado. Bajo el EAP los ajustes de la configuración seleccionan el método EAP apropiado. Este ejemplo utiliza la autenticación LEAP. El teclado **some** cuando le hacen.

- 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

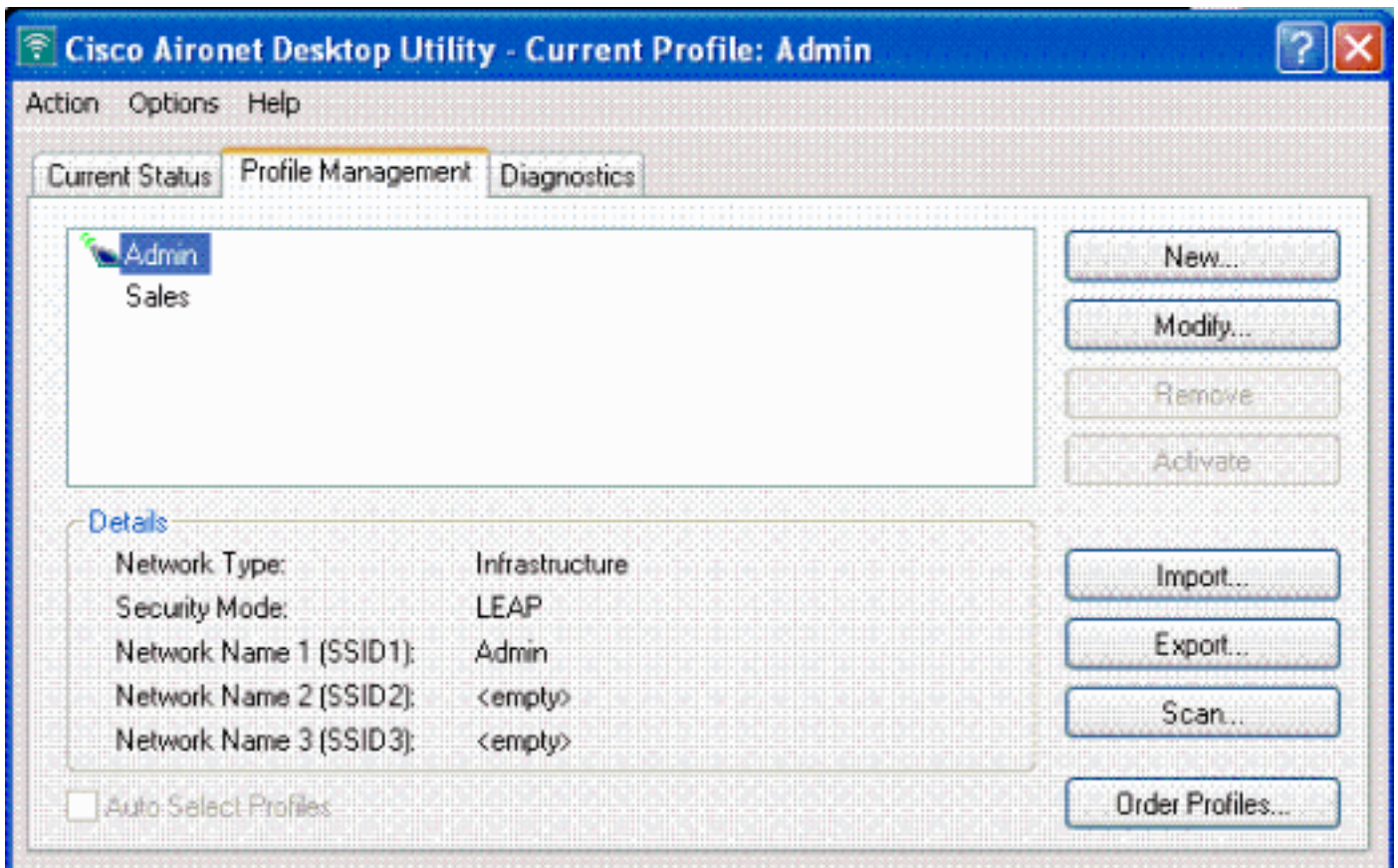
Cancel

[Configure al cliente de red inalámbrica y verifiquelo](#)

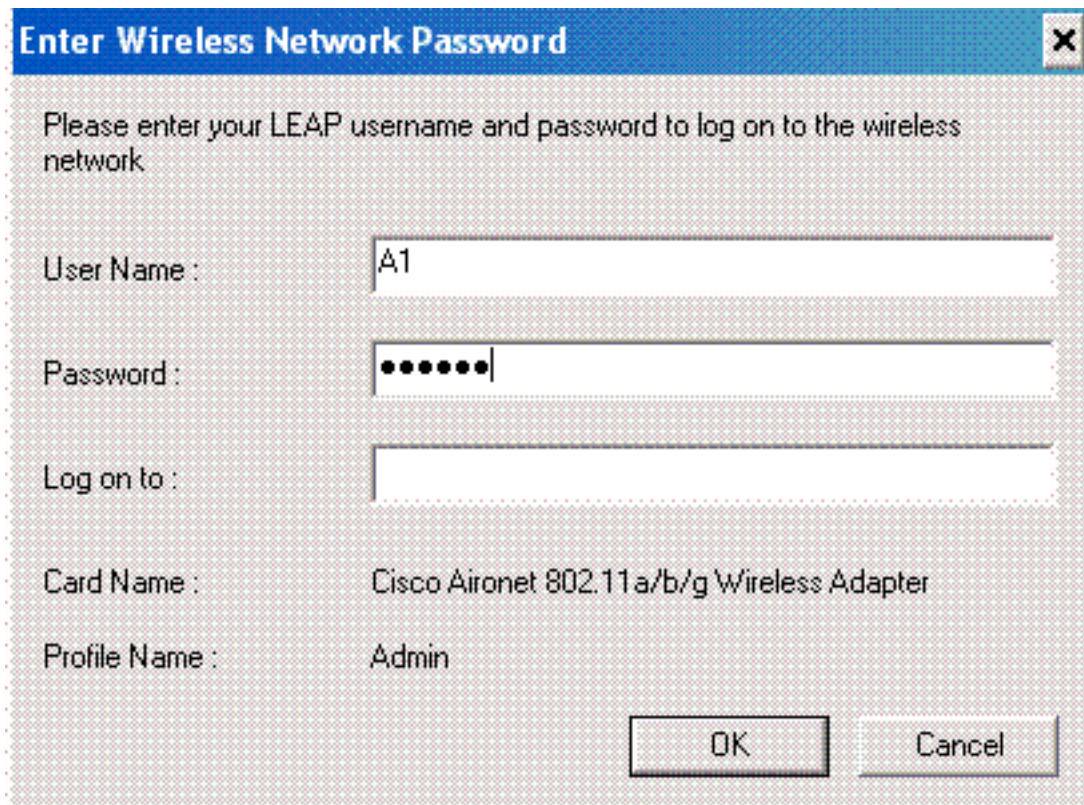
Use esta sección para confirmar que su configuración funciona correctamente. Intente asociar a un cliente de red inalámbrica al REVESTIMIENTO usando la autenticación LEAP para verificar si la configuración trabaja como se esperaba.

Nota: Este documento asume que el perfil del cliente está configurado para la autenticación LEAP. Refiérase [con la autenticación EAP](#) para la información sobre cómo configurar el adaptador de red inalámbrica de cliente del a/b/g del 802.11 para la autenticación LEAP.

Nota: Del ADU usted ve que usted ha configurado dos perfiles del cliente. Uno para los usuarios del departamento administrativos con SSID el **Admin** y el otro perfil para los usuarios del Departamento de ventas con las **ventas** SSID. Ambos perfiles se configuran para la autenticación LEAP.



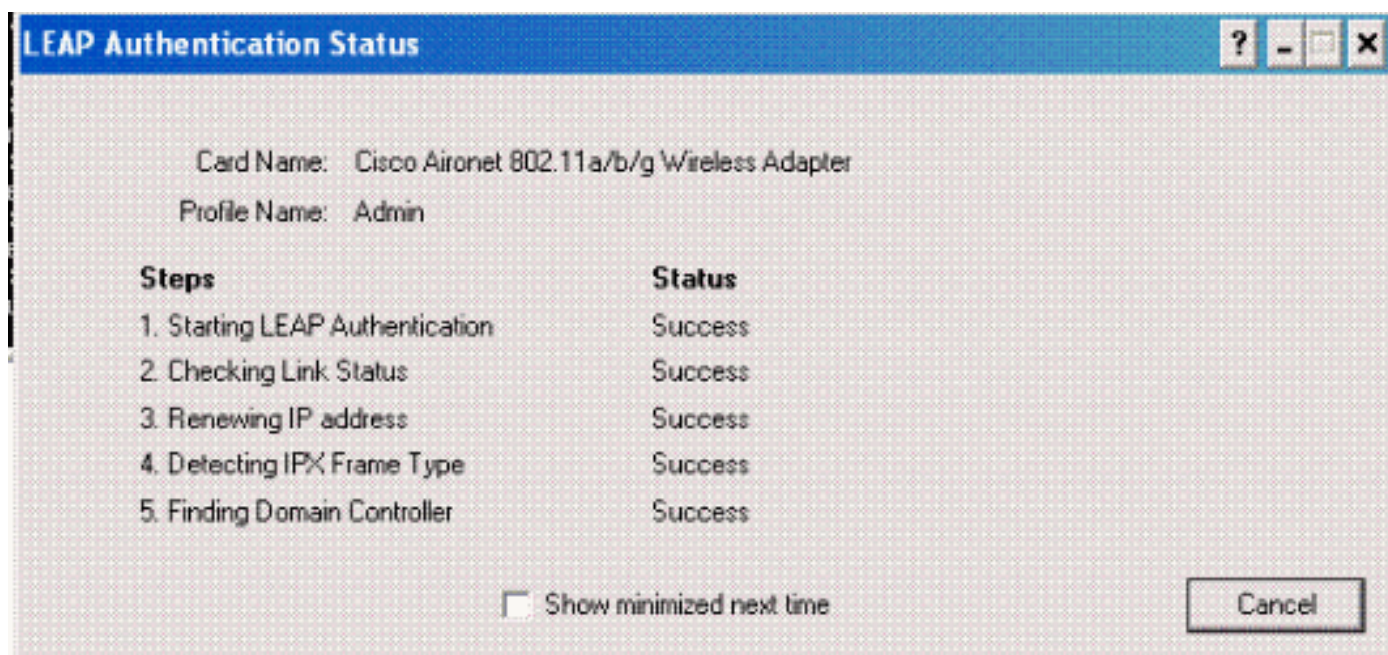
Cuando el perfil para el usuario de red inalámbrica del departamento de administración se activa, piden el usuario proporcionar el nombre de usuario/la contraseña para la autenticación LEAP. Aquí tiene un ejemplo:



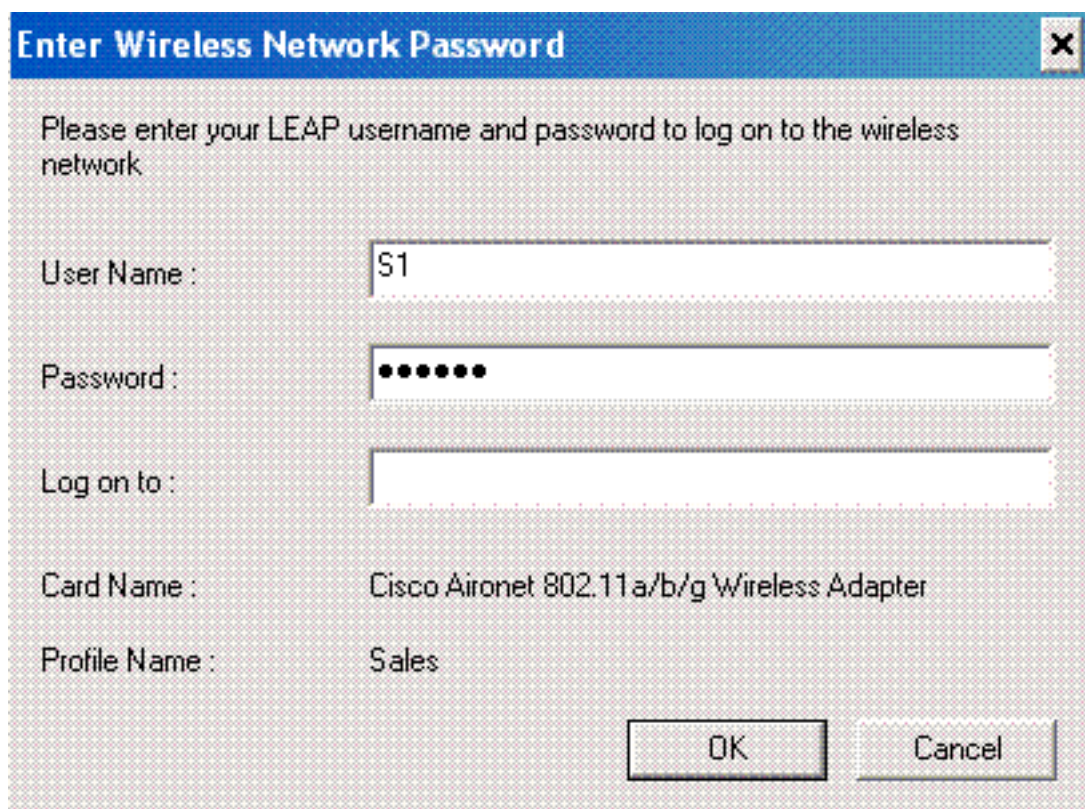
El REVESTIMIENTO y entonces el WLC pasa encendido los credenciales de usuario al servidor RADIUS externo (Cisco Secure ACS) para validar las credenciales. El WLC pasa encendido las credenciales incluyendo el atributo DNIS (nombre SSID) al servidor de RADIUS para la validación.

El servidor de RADIUS verifica los credenciales de usuario comparando los datos con la base de datos de usuarios (y los NAR) y proporciona el acceso al cliente de red inalámbrica siempre que los credenciales de usuario sean válidos.

Sobre la autenticación de RADIUS acertada el cliente de red inalámbrica se asocia al REVESTIMIENTO.



Semejantemente cuando un usuario del Departamento de ventas activa el perfil de las ventas, al servidor de RADIUS autentica al usuario basado en el nombre de usuario del SALTO/la contraseña y el SSID.



El informe pasajero de la autenticación sobre el servidor ACS muestra que el cliente ha pasado la autenticación de RADIUS (autenticación EAP y autenticación SSID). Aquí tiene un ejemplo:

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

Ahora, si el usuario de las ventas intenta acceder el **Admin** SSID, el servidor de RADIUS niega el acceso del usuario a la red inalámbrica (WLAN). Aquí tiene un ejemplo:



Esta manera que los usuarios pueden ser acceso restringido basó en el SSID. En un entorno para empresas, todos los usuarios que caen en un departamento específico pueden ser agrupados en un solos grupo y acceso a la red inalámbrica (WLAN) pueden ser proporcionados basaron en el SSID que utilizan como se explica en este documento.

Troubleshooting

Comandos para resolución de problemas

La herramienta [Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un comando debug.

- haga el debug del permiso aaa del dot1x — Habilita el debug de las interacciones del 802.1x AAA.

- **permiso del paquete del dot1x del debug** — Habilita el debug de todos los paquetes del dot1x.
- **el debug aaa todo habilita** — Configura el debug de todos los mensajes AAA.

Usted puede también utilizar el informe pasajero de la autenticación y el informe de la autenticación fallida sobre el servidor del Cisco Secure ACS para resolver problemas la configuración. Estos informes están bajo los **informes** y la **ventana de actividad** en el ACS GUI.

[Información Relacionada](#)

- [Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN \(WLC\)](#)
- [Ejemplo de Configuración de la Autenticación Web del Controlador LAN Inalámbrico](#)
- [Ejemplo de Configuración de VLANs de Grupo de AP con Controladores de LAN Inalámbrica](#)
- [Página de Soporte de Red Inalámbrica](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)