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

Contenido

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 LAN de la Tecnología inalámbrica (WLC) y el Punto de acceso ligero (REVESTIMIENTO) para la operación básica
- Conocimiento básico en cómo configurar el Cisco Secure Access Control Server (ACS)
- Conocimiento de los métodos ligeros del protocolo (LWAPP) y de la seguridad de red inalámbrica del Punto de acceso

Componentes Utilizados

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

- Cisco 2000 Series WLC que funciona con los firmwares 4.0
- REVESTIMIENTO de las Cisco 1000 Series
- Cisco asegura la versión 3.2 del servidor ACS
- Adaptador de red inalámbrica de cliente de Cisco 802.11a/b/g que funciona con los firmwares 2.6
- Versión 2.6 de Cisco utilidad Aironet Desktop (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 TécnicosCisco 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). Cisco asegura al servidor ACS se utiliza para autenticar a los usuarios. La autenticación sucede en dos etapas en Cisco ACS seguro:

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

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

Cisco ACS seguro utiliza la característica NAR para restringir el acceso del usuario basado en el SSID. Un NAR es una definición, que usted hace en Cisco ACS seguro, de las condiciones adicionales que deben ser cumplidas antes de que un usuario pueda tener acceso a la red. Cisco ACS seguro aplica estas condiciones usando la información de los atributos enviados por sus clientes AAA. Aunque haya varias maneras que usted puede poner 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 pone un NAR, usted puede elegir si el filtro actúa positivamente o negativamente. Es decir, en el NAR usted especifica si permitir o negar el acceso a la red, 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 Libro Blanco de las restricciones del acceso a la red para más información.

Cisco ACS seguro utiliza dos tipos de filtros NAR:

1. **filtros IP-basados** — el NAR IP-basado filtra el acceso del límite basado sobre los IP Addresses del cliente del usuario final y del cliente AAA. Refiérase sobre los filtros IP-basados NAR para más información sobre este tipo de filtro NAR.
2. **filtros No-IP-basados** — el NAR No-IP-basado filtra el acceso del límite basado sobre la comparación de cadenas simple de un valor enviado del cliente AAA. El valor puede ser la línea de llamada el número identificación (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 No-IP-basados NAR para más información sobre este tipo de filtro NAR.

Este documento utiliza los filtros no-IP-basados para hacer la autenticación SSID-basada. Un filtro no-IP-basado NAR (es decir, un filtro DNIS/CLI-based NAR) es una lista de llamada permitida o negada/punta de las ubicaciones del acceso que usted puede utilizar en la restricción de un cliente AAA cuando usted no tiene una conexión IP-basada establecida. La característica no-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 las restricciones del por-usuario SSID.

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

- **Cliente AAA** — El NAS-IP-direccionamiento (se utiliza el atributo 4) o, si no existe el NAS-IP-direccionamiento, el NAS-identificador (atributo de RADIUS 32).
- **Puerto** — El NAS-puerto (se utiliza el atributo 5) o, si no existe el NAS-puerto, la NAS-puerto-identificación (atributo 87).
- **CLI** — Se utiliza La llamar-estación-identificación (atributo 31).
- **DNIS** — Se utiliza La llamar-estación-identificación (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 las restricciones del por-usuario SSID. En el caso del WLC, los campos NAR tienen estos valores:

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

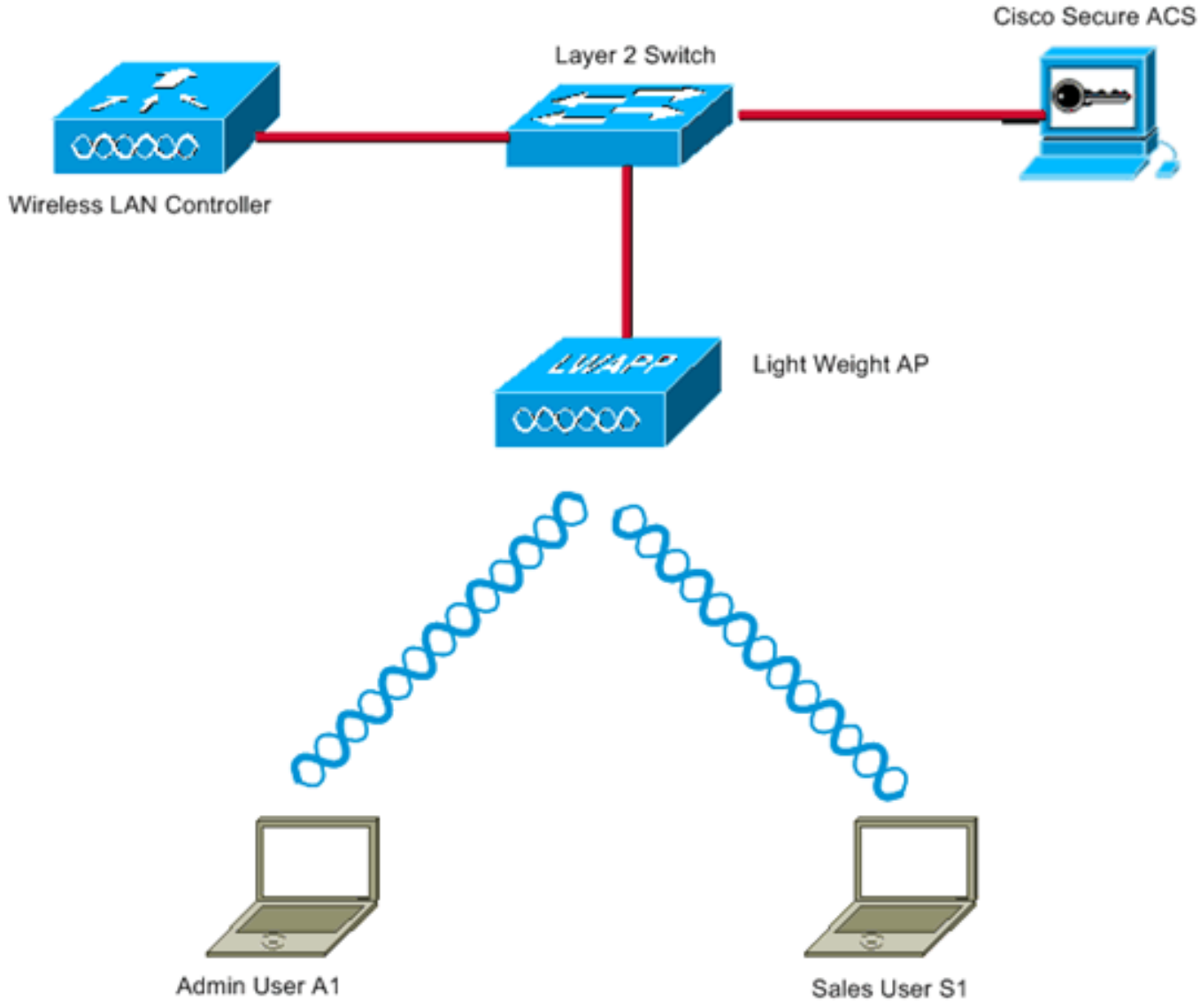
El recordatorio de este documento proporciona a un ejemplo de la configuración en cómo lograr esto.

Configuración de la red

En esta disposición del ejemplo, WLC se registra al REVESTIMIENTO. Se utilizan dos redes inalámbricas (WLAN). Una red inalámbrica (WLAN) está para los usuarios del departamento Admin y la otra red inalámbrica (WLAN) está para los usuarios del Departamento de ventas. El cliente de red inalámbrica A1 (usuario Admin) y S1 (usuario de las ventas) conecta con la red

inalámbrica. Usted necesita configurar el WLC y el servidor de RADIUS de una manera tal que el usuario A1 Admin pueda tener acceso solamente a la red inalámbrica (WLAN) **Admin** y sea acceso restringido a las **ventas** y al usuario S1 de la red inalámbrica (WLAN) de las ventas debe poder tener acceso a 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 a WLC y no sabe configurar el WLC para la operación básica, refiere al registro ligero AP (REVESTIMIENTO) a un regulador LAN de la Tecnología inalámbrica (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

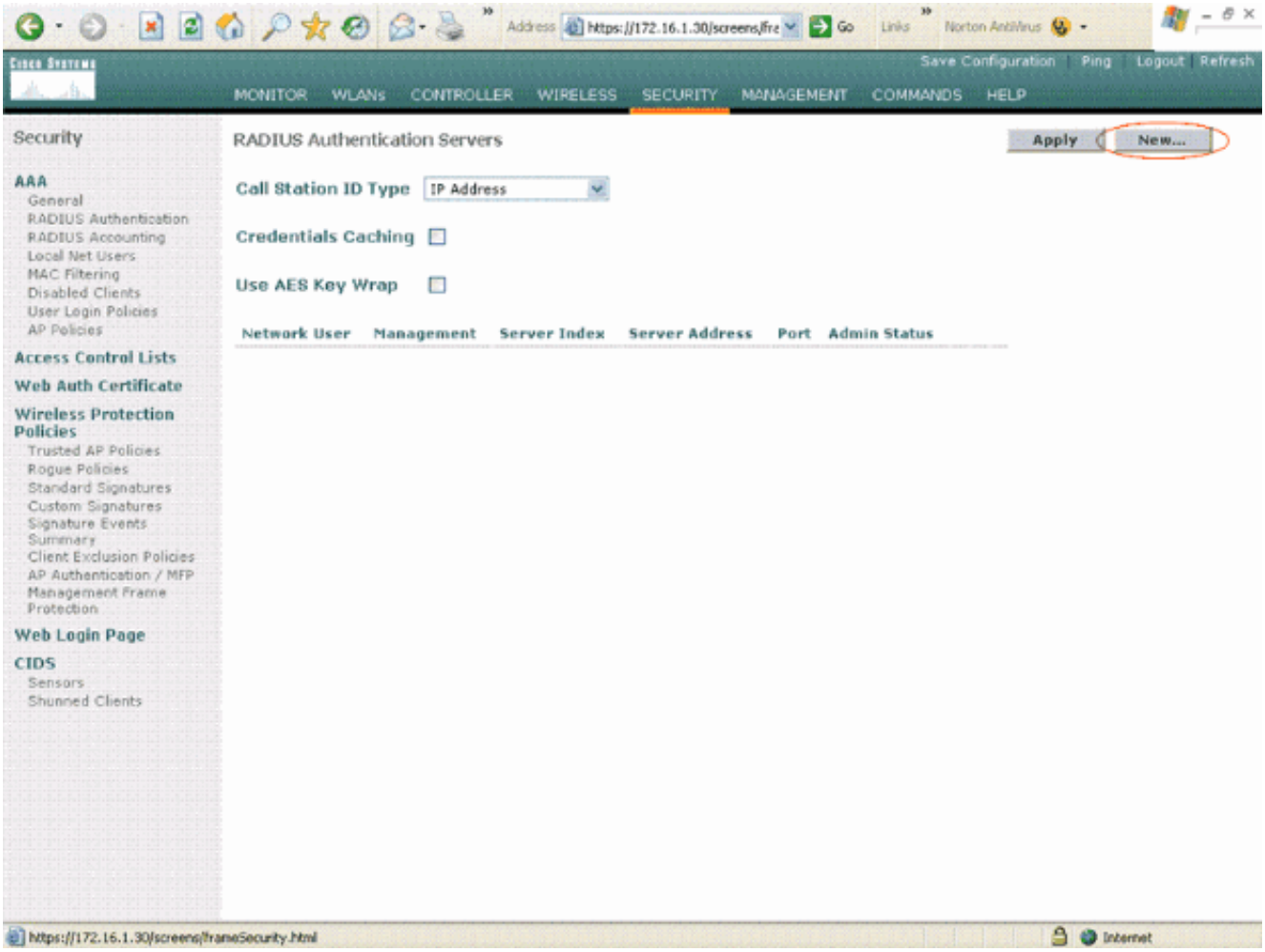
Para configurar los dispositivos para esta disposición, usted necesita:

1. Configure el WLC para las dos redes inalámbricas (WLAN) y servidores de RADIUS.
2. Configure Cisco ACS seguro.
3. Configure a los clientes de red inalámbrica y verifiqúelos.

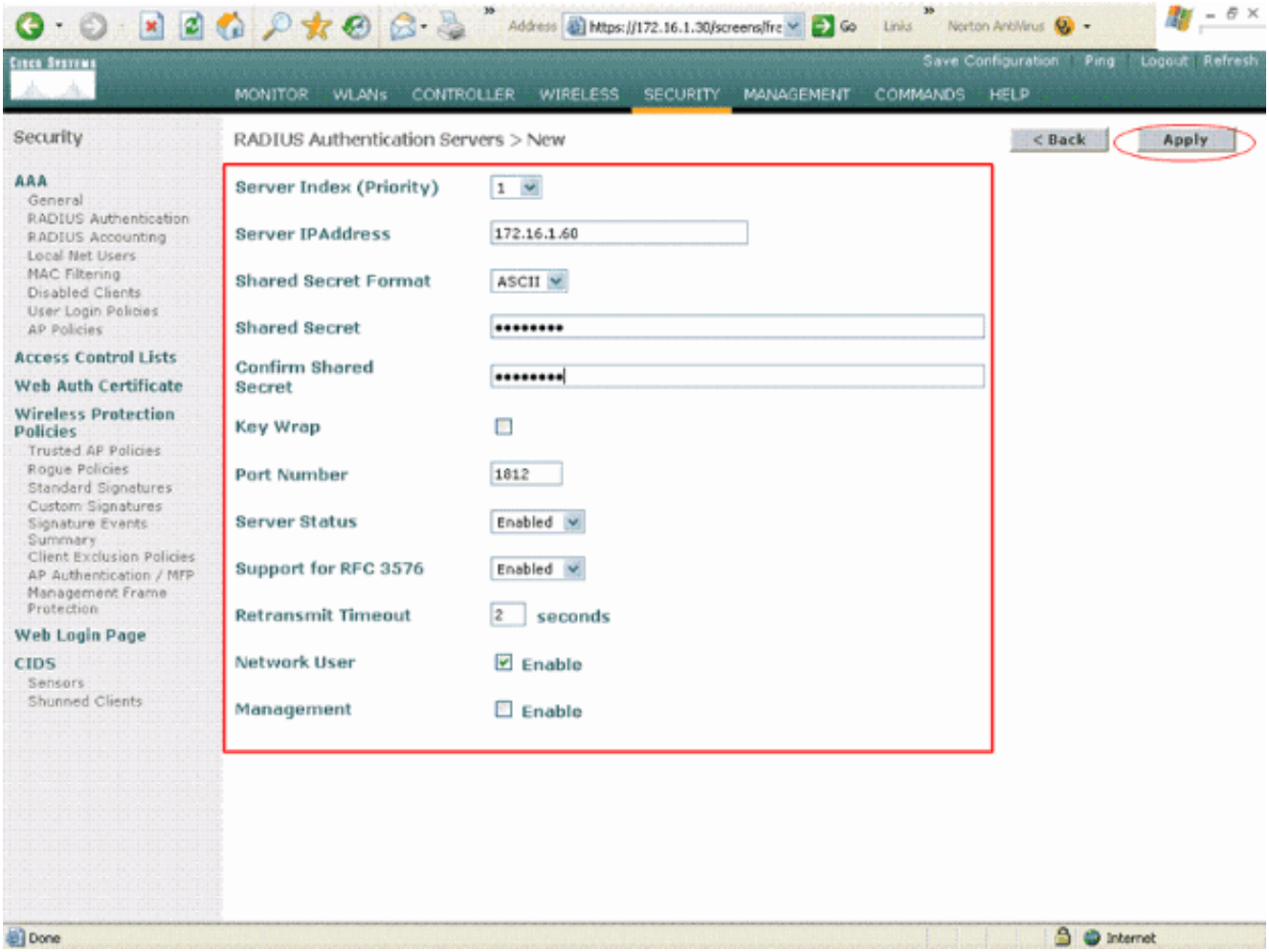
Configure el WLC

Complete estos pasos para configurar el WLC para esta disposición:

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

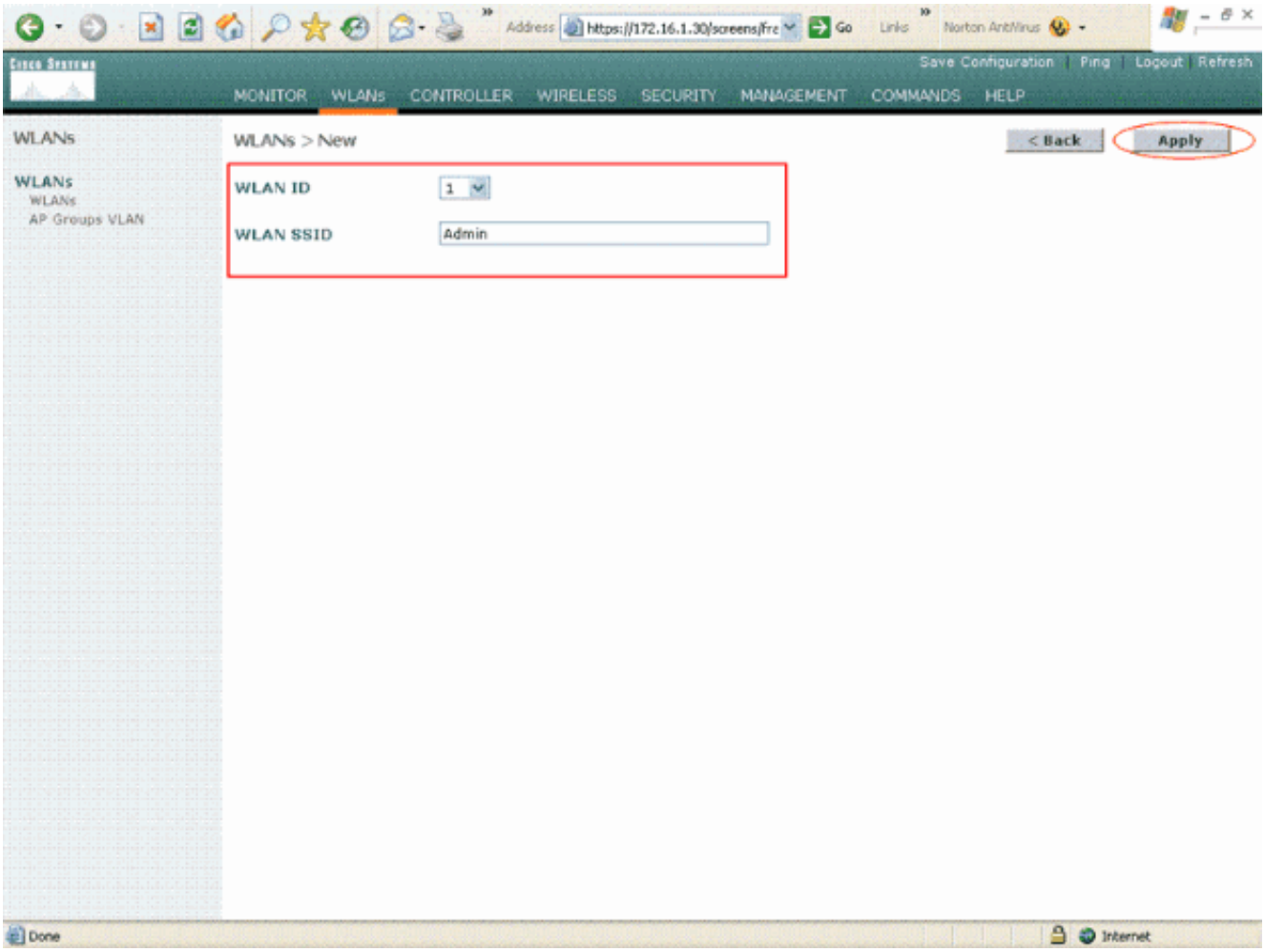


Haga clic **nuevo** para definir los parámetros del servidor de RADIUS.Estos parámetros incluyen la dirección IP, el secreto compartido, el número del puerto, y el estado del servidor del servidor de RADIUS. Las casillas de verificación del usuario de la red y de la Administración determinan si la autenticación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

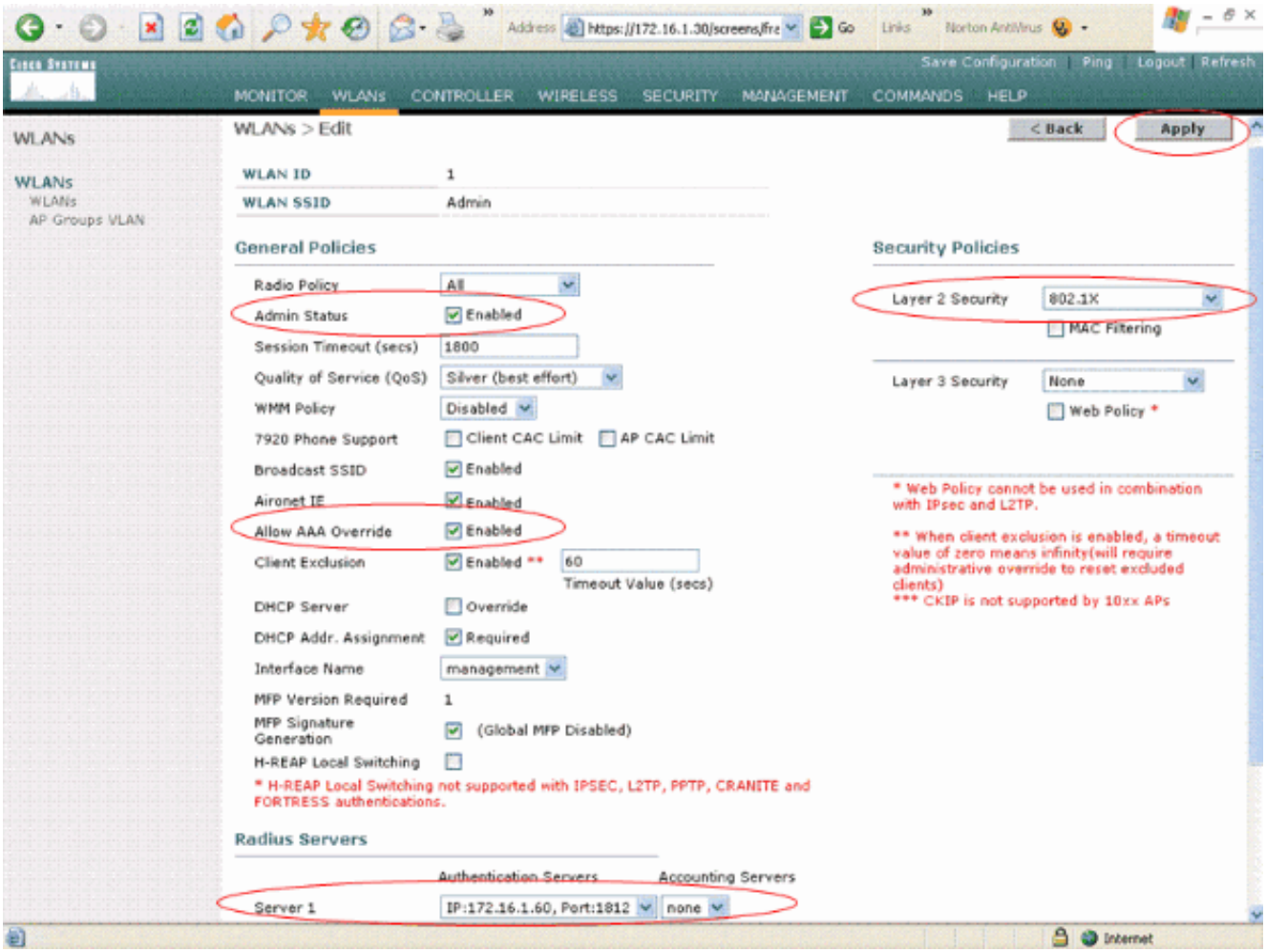


Haga clic en Apply (Aplicar).

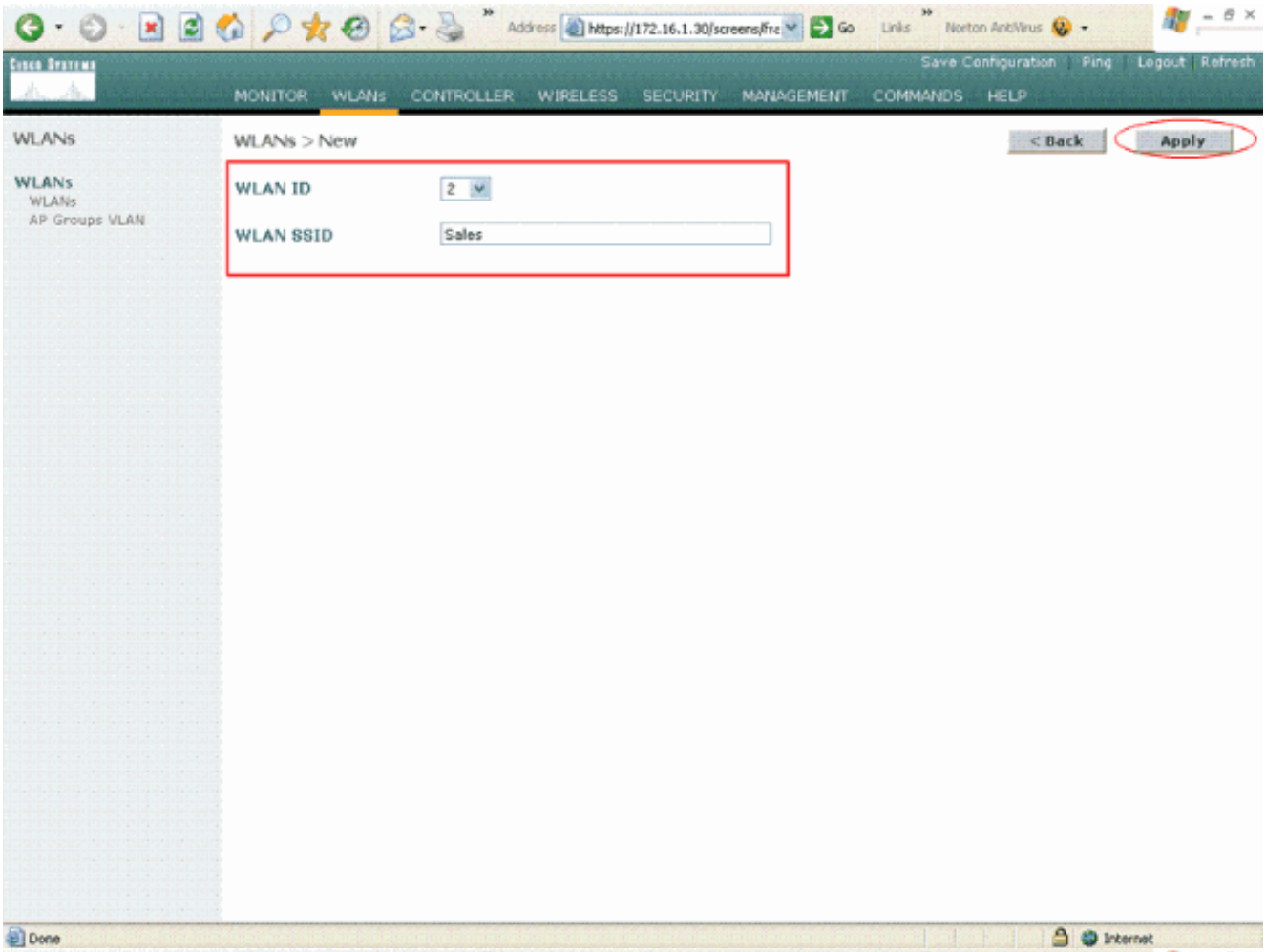
2. Configure la una red inalámbrica (WLAN) para el departamento Admin con SSID **Admin** y la otra red inalámbrica (WLAN) para el Departamento de ventas con las **ventas** SSID. Para hacerlo, complete estos pasos:Haga clic las **redes inalámbricas (WLAN) del** GUI del regulador para crear una red inalámbrica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

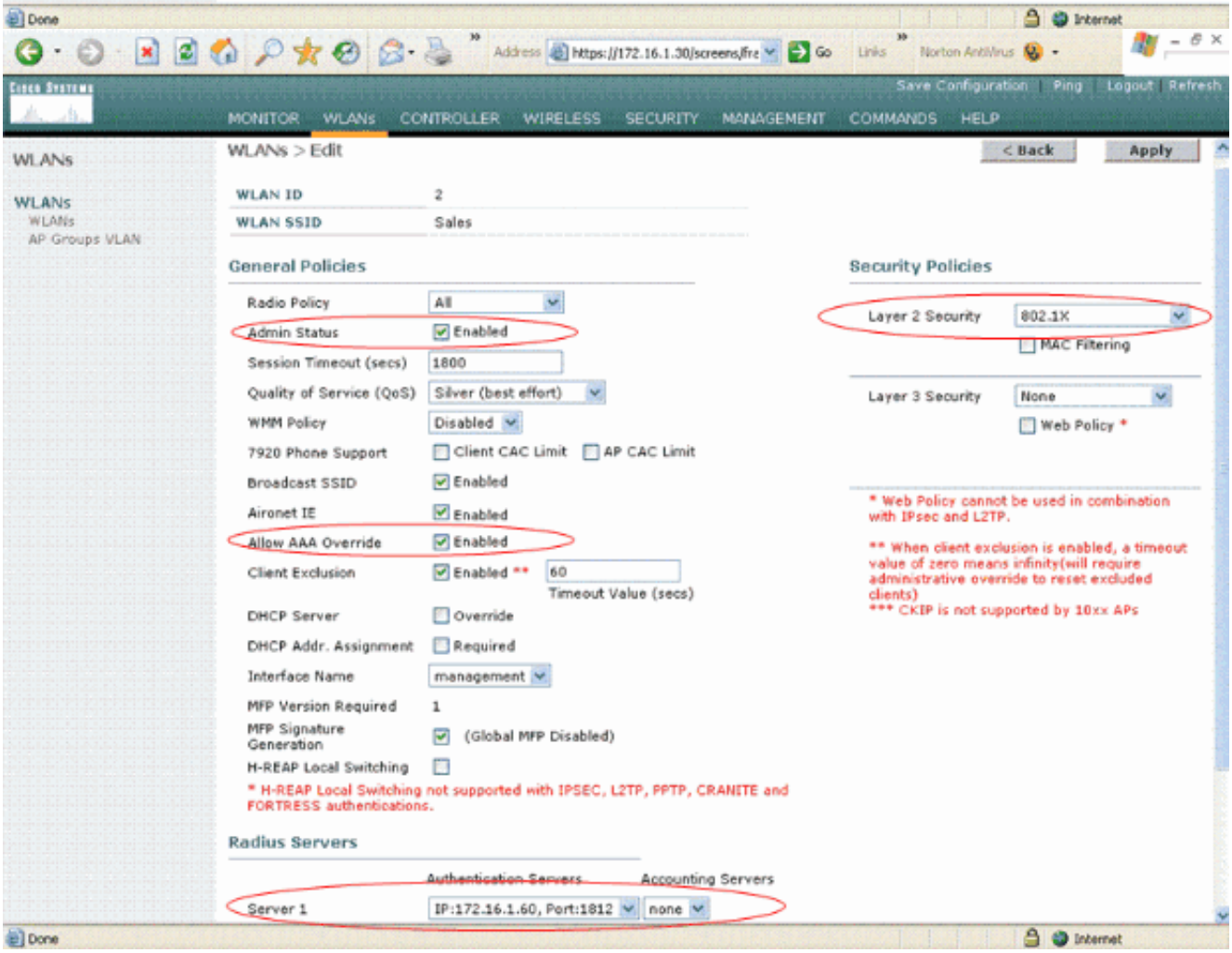


En la **red inalámbrica (WLAN) > corrija la** ventana, definen los parámetros específicos a la red inalámbrica (WLAN):Del menú desplegable de la Seguridad de la capa 2, seleccione el **802.1x**. Por abandono, la opción de seguridad de la capa 2 es 802.1x. Esto activa la autenticación 802.1x/EAP para la red inalámbrica (WLAN).Bajo políticas generales, controle el cuadro de la **invalidación AAA**. Cuando se activa 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 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 de la red inalámbrica (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 están las capturas de pantalla.


Address https://172.16.1.30/screens/fra
Go
Links
Norton AntiVirus
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
WLANs > New
< Back
Apply
WLAN ID
2
WLAN SSID
Sales


Done
Internet
Address https://172.16.1.30/screens/fra
Go
Links
Norton AntiVirus
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
WLANs > Edit
< Back
Apply
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

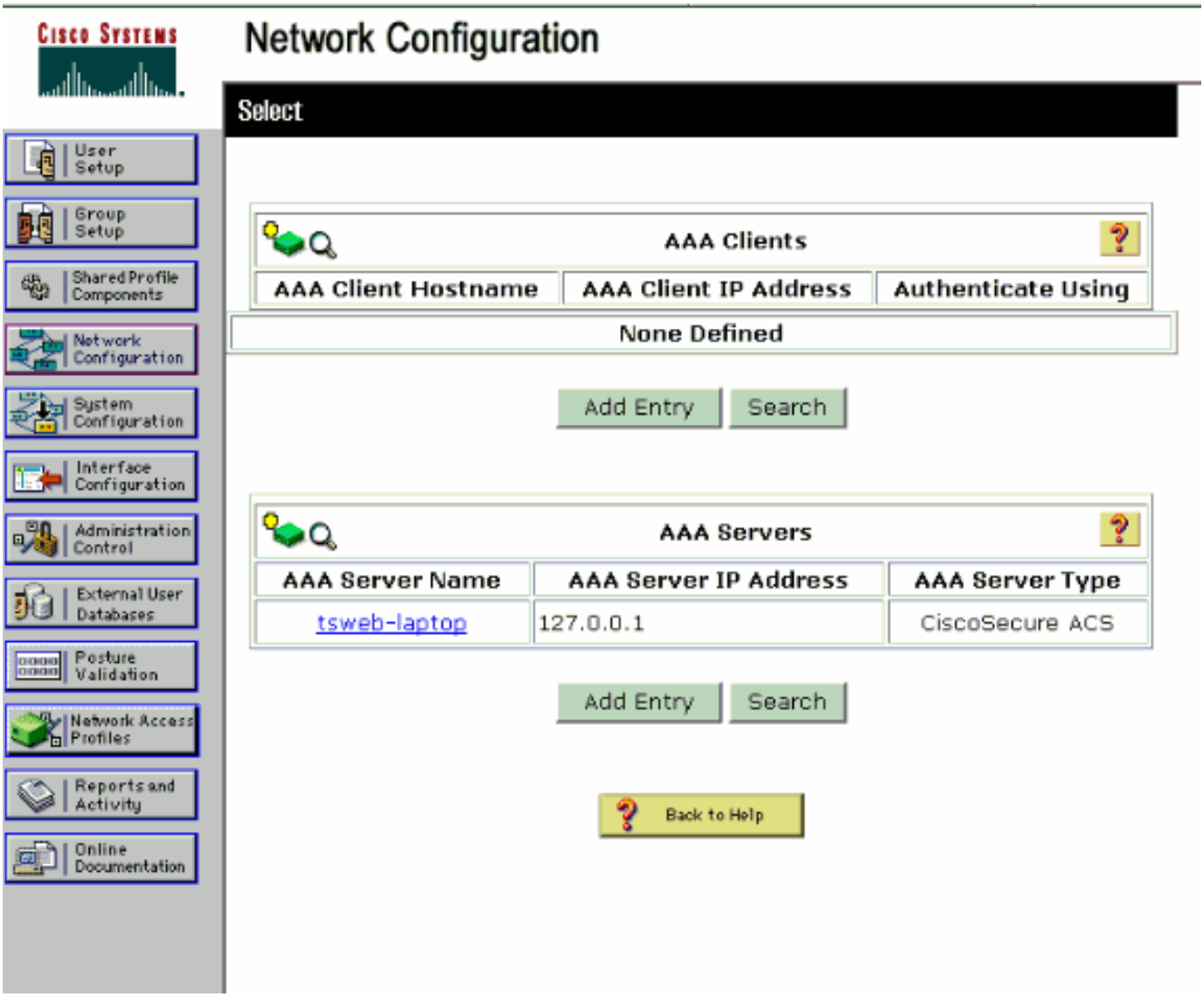
Configure Cisco ACS seguro

En Cisco asegure al servidor ACS que usted necesita:

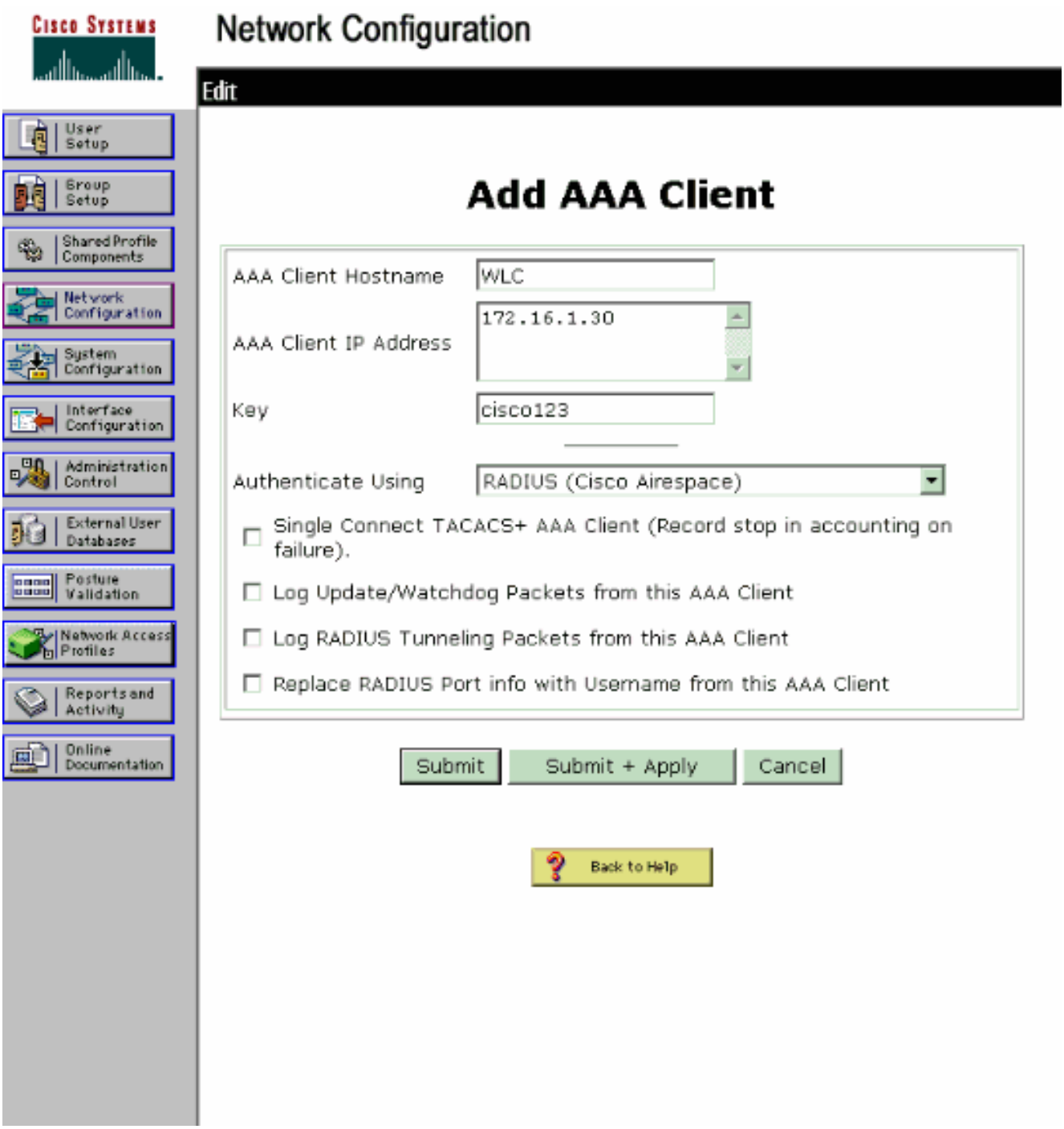
1. Configure el WLC como cliente AAA.
2. Cree la base de datos de usuarios y defina el NAR para la autenticación SSID-basada.
3. Active la autenticación EAP.

Complete estos pasos en Cisco ACS seguro:

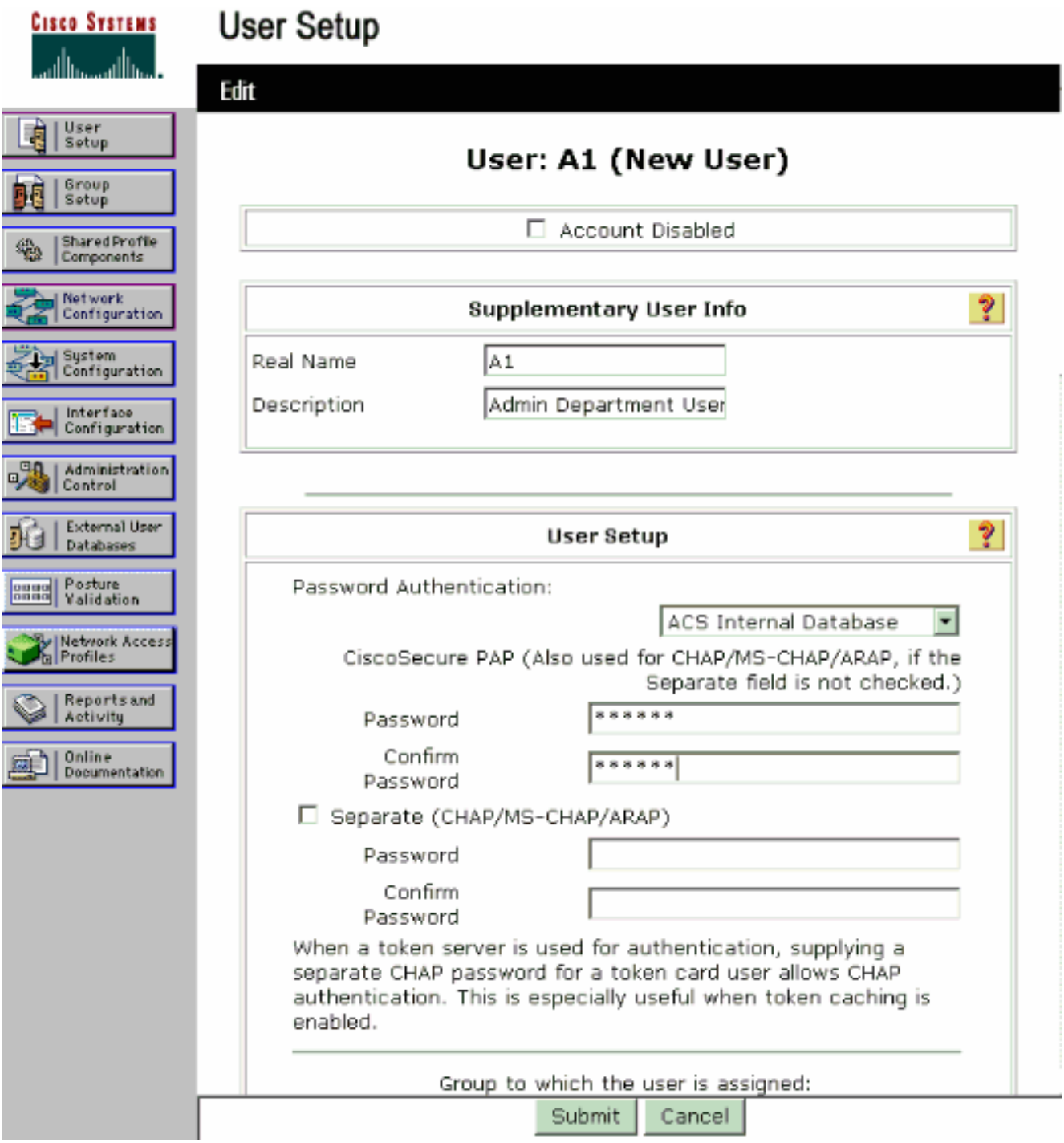
1. Para definir el regulador como cliente AAA en el servidor ACS, haga clic la **configuración de red del** GUI ACS. Bajo los clientes AAA haga clic en **agregan la entrada**.



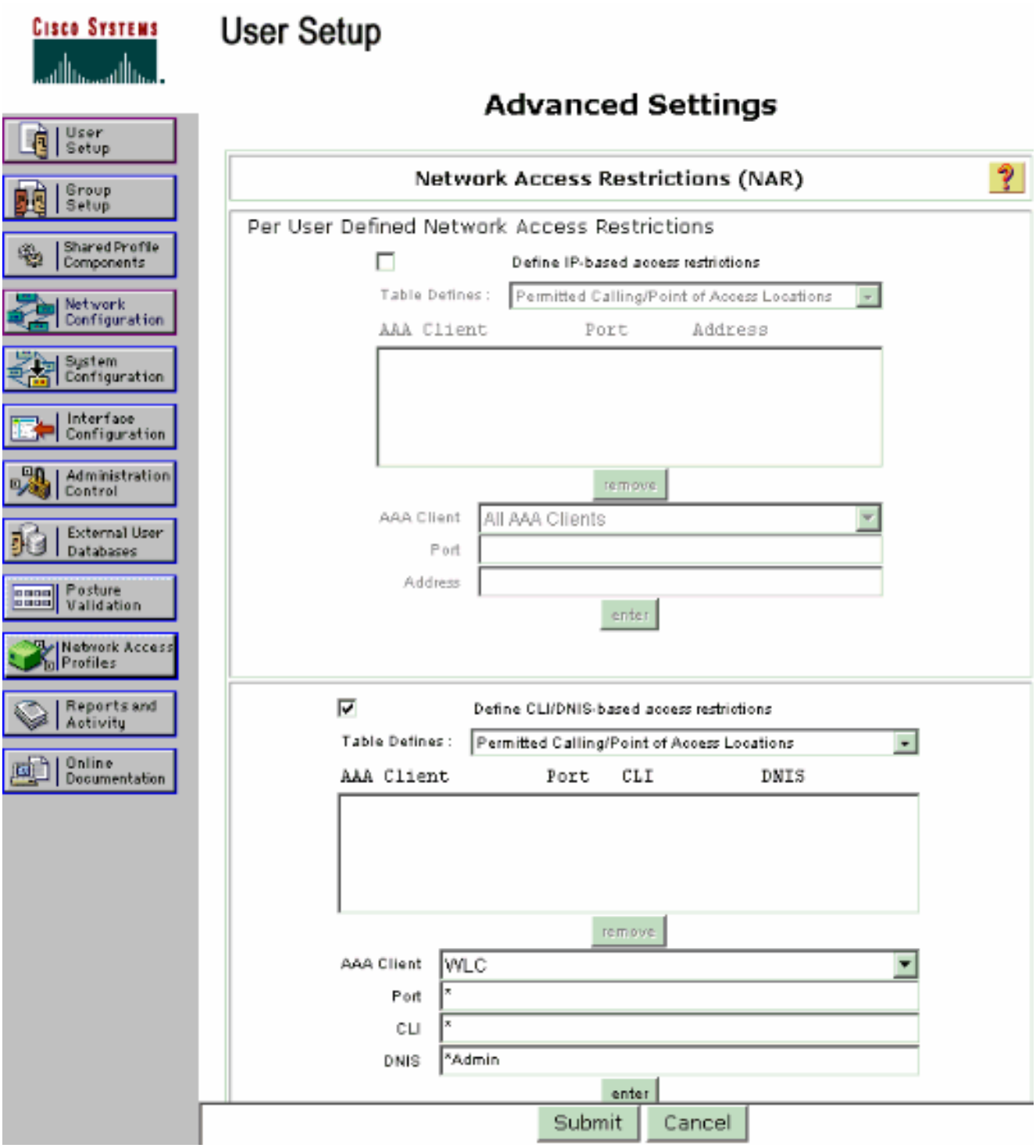
2. Cuando aparece la página de la configuración de red, defina el nombre del WLC, de la dirección IP, del secreto compartido y del método de autenticación (RADIUS Cisco Airespace).



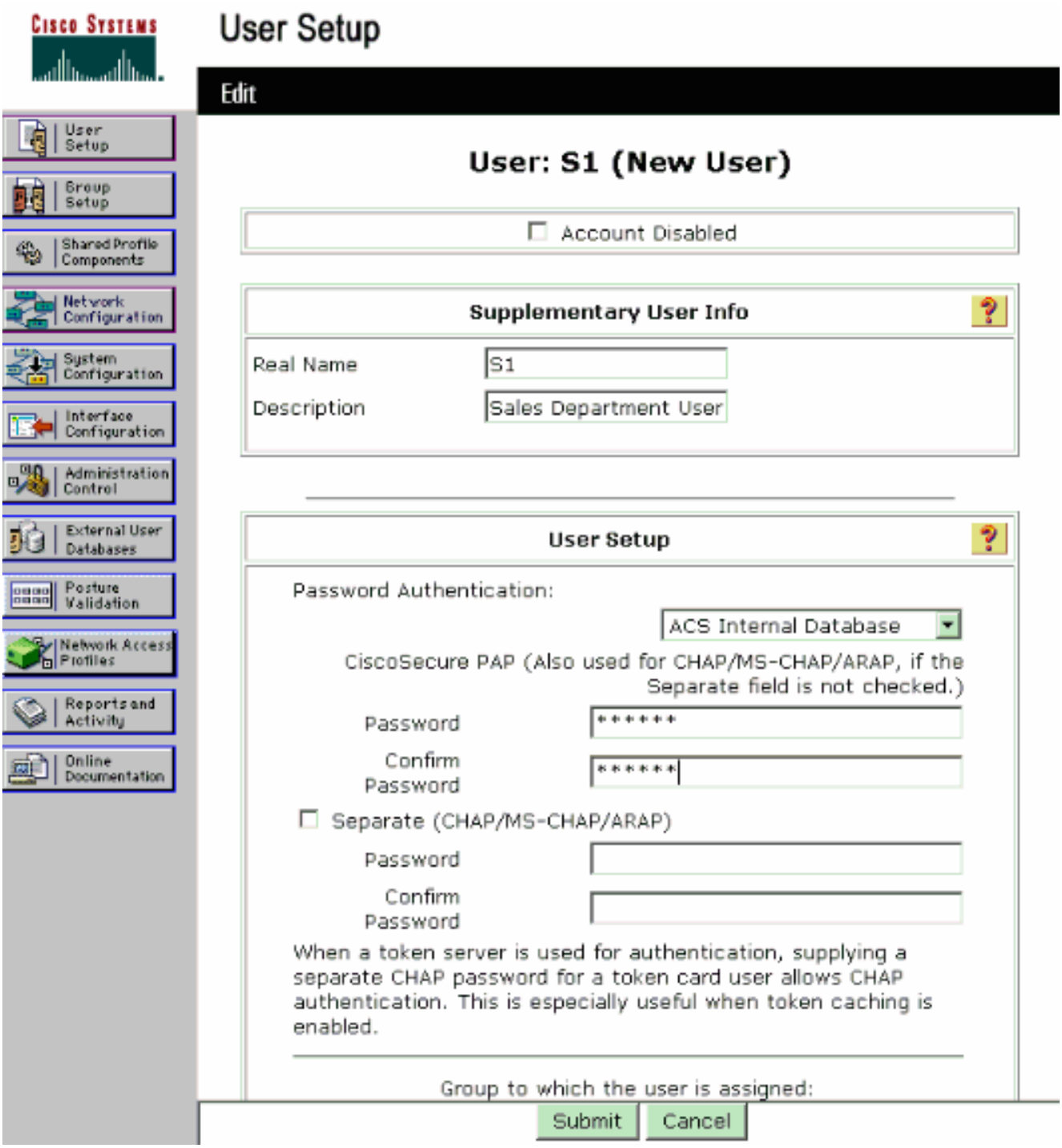
3. Haga clic la **configuración de usuario del** GUI ACS, ingrese el username, y el tecleo **agrega/corrige**. En este ejemplo el usuario es A1.
4. Cuando aparece la página de la configuración de usuario, defina todos los parámetros específicos al usuario. En este ejemplo se configuran el username, la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

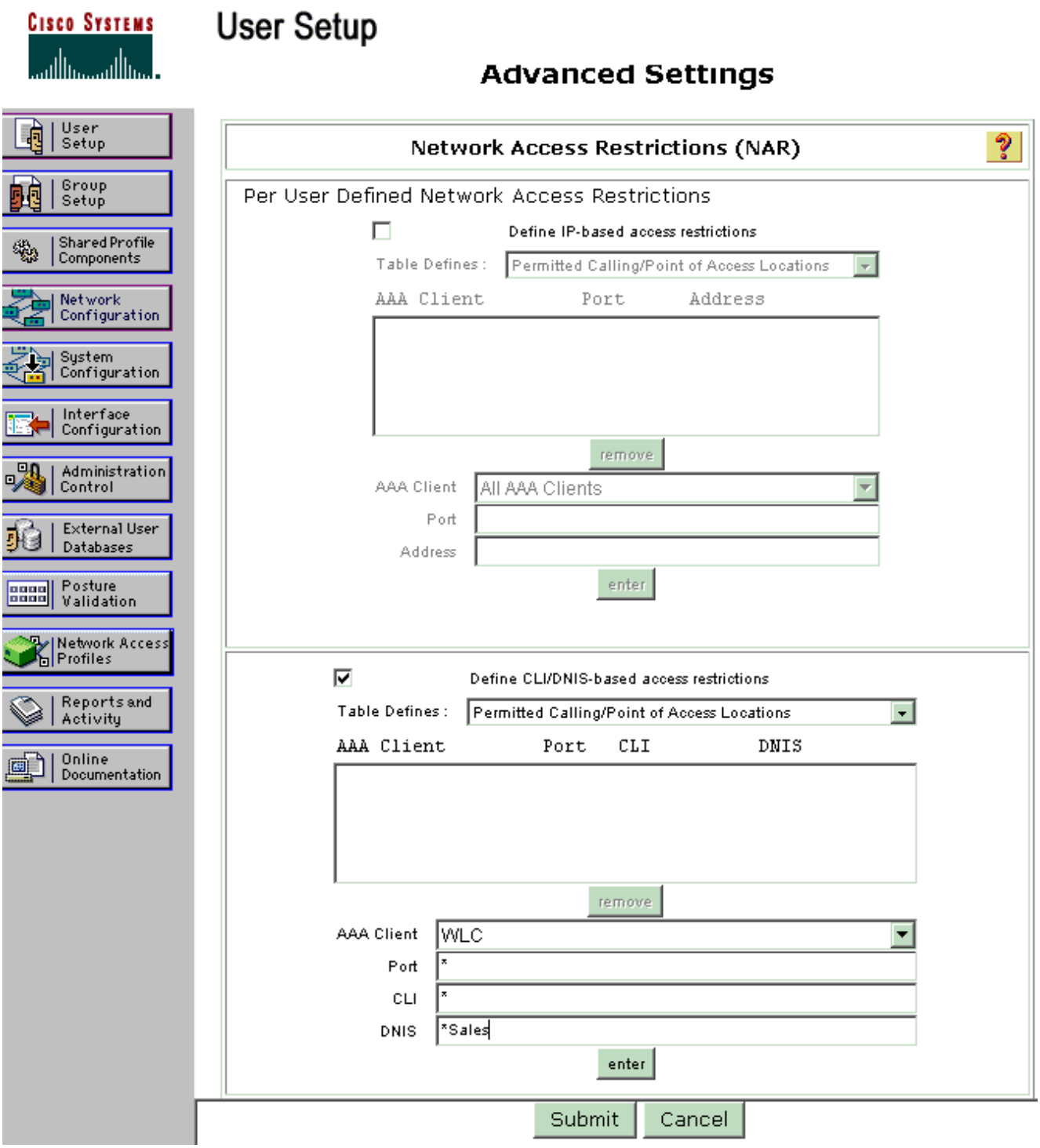


5. Enrolle abajo la página de la configuración de usuario, hasta que usted vea la sección de las restricciones del acceso a la red. Bajo interfaz de usuario de la restricción de acceso DNIS/CLI, seleccione la **punta de llamada permitida de las ubicaciones del acceso** y defina estos parámetros:**Cliente AAA** — Dirección IP WLC (172.16.1.30 en nuestro ejemplo)**Puerto** — ***CLI** — ***DNIS** — *ssidname
6. El atributo DNIS define el SSID a que se permite al usuario tener acceso. El WLC envía el SSID en el atributo DNIS al servidor de RADIUS.Si el usuario necesita tener acceso solamente al 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 tecleo **ingresa**.**Nota:** El SSID se debe preceder siempre con ***. Es obligatorio.

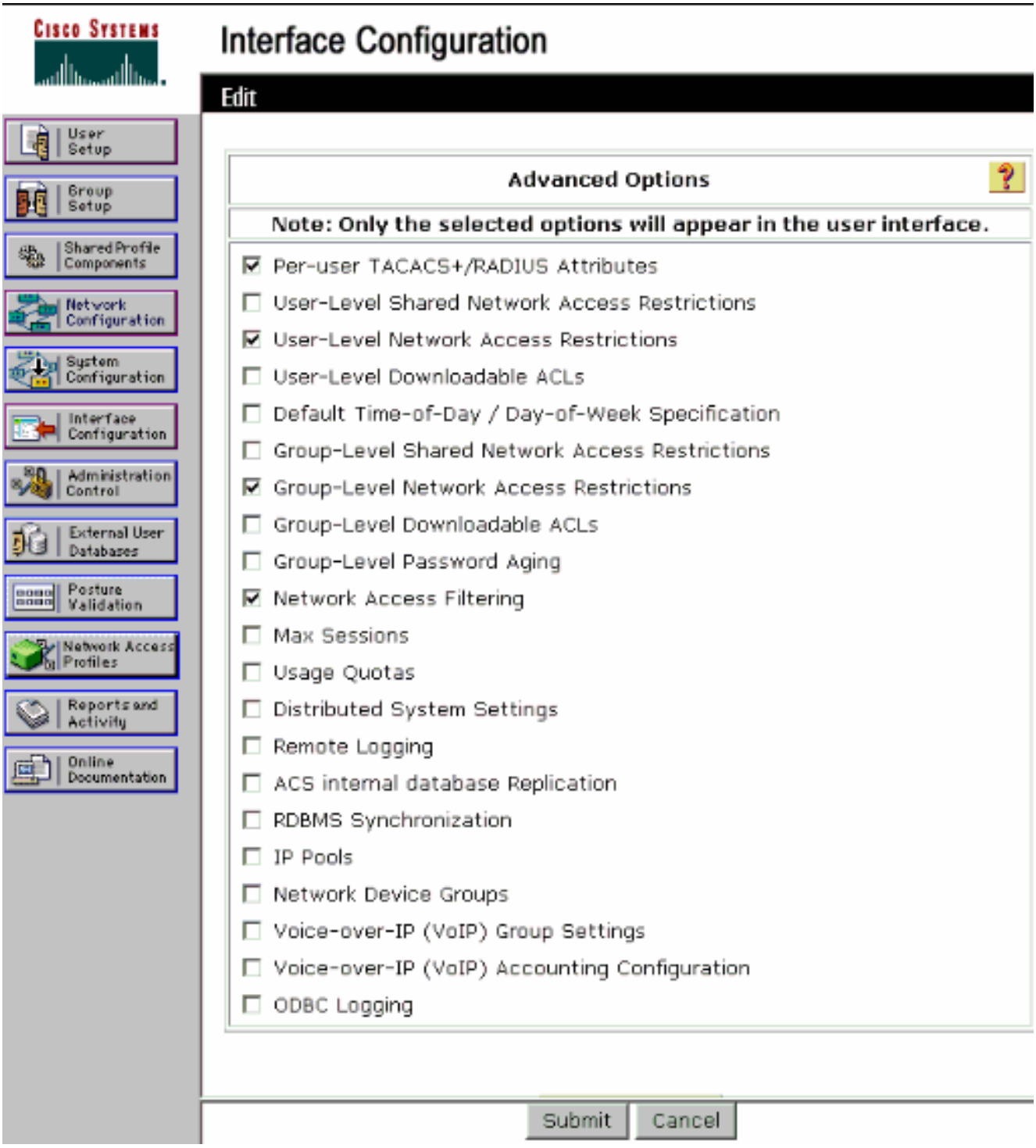


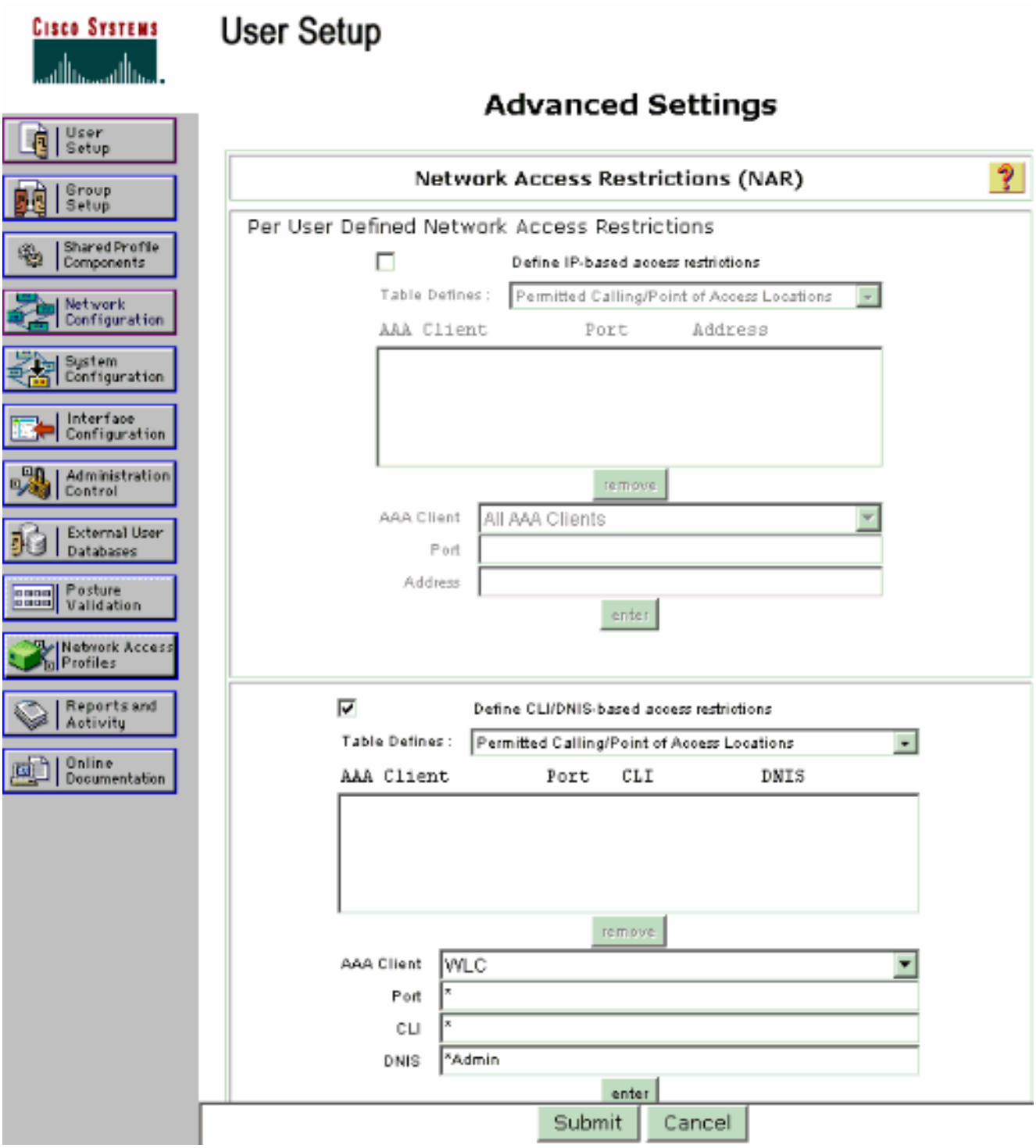
7. Haga clic en Submit (Enviar).
8. Semejantemente, cree a un usuario para el usuario del Departamento de ventas. Aquí están las capturas de
pantalla.


Cisco Systems
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
S1
Description
Sales Department User
User Setup
Password Authentication:
ACS Internal Database
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:
Submit
Cancel

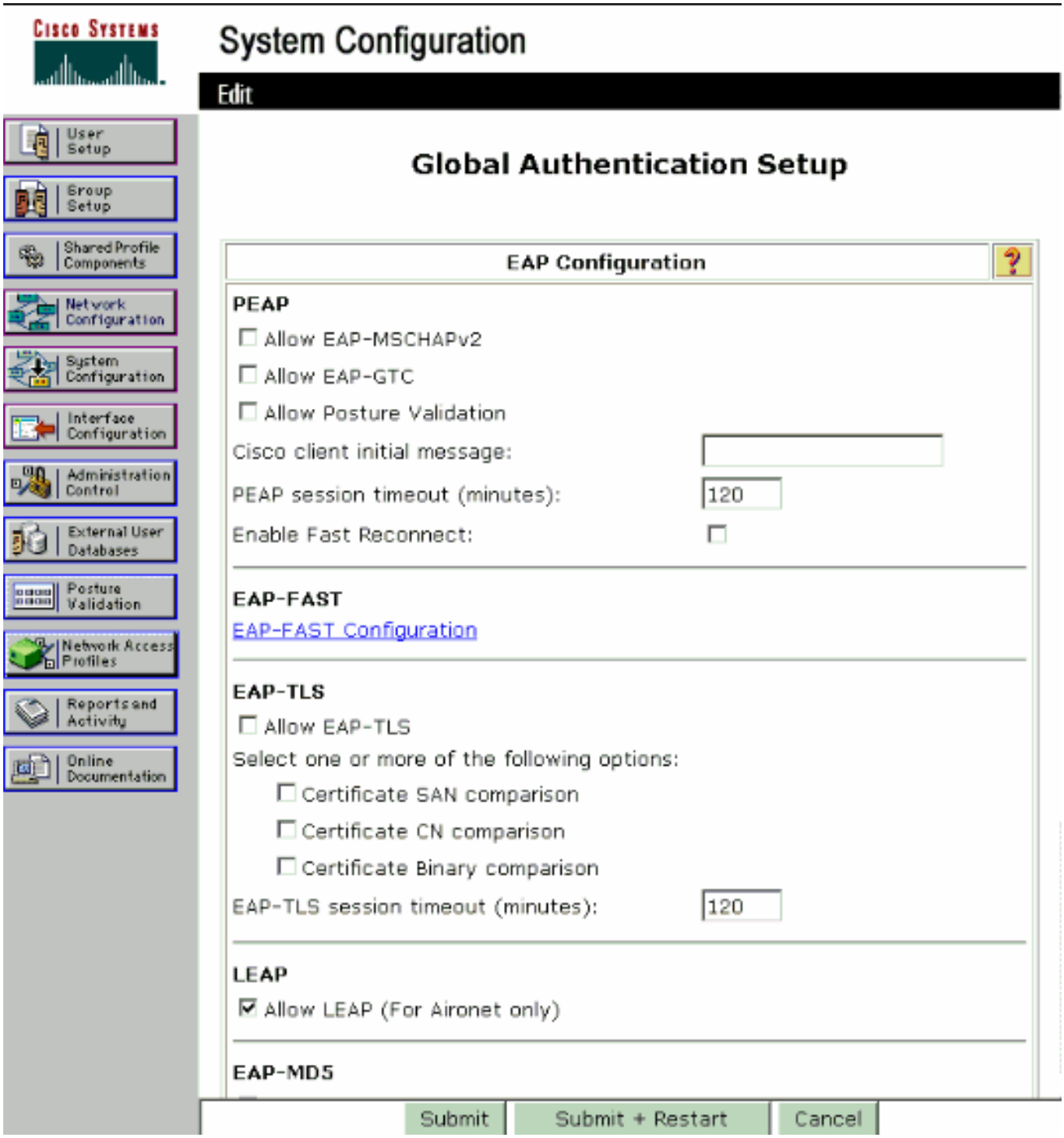


9. Relance el mismo proceso para agregar a más usuarios a la base de datos.**Nota:** Por abandono agrupan a todos los usuarios bajo grupo predeterminado. Si usted quiere asignar a los usuarios específicos a diversos grupos, refiera a la sección de administración del grupo de usuarios de la guía de usuario para Cisco ACS seguro para el Servidor Windows 3.2.**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 activa. Para activar las restricciones del acceso a la red para los usuarios, elegir los **interfaces > avanzó las opciones del** GUI ACS, las **restricciones** selectas del **acceso a la red del nivel de usuario** y el tecleo **somete**. Esto activa el NAR y aparece en la ventana de la configuración de usuario.


Cisco Systems
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



10. Para activar la autenticación EAP, la **configuración del sistema del** tecleo y la **autenticación global ponen** para asegurarse de que el servidor de la autenticación está configurado para realizar el método de autenticación deseado EAP.Bajo EAP las configuraciones seleccionan el método EAP apropiado. Este ejemplo utiliza la autenticación LEAP. El tecleo **somete** cuando le
hacen.

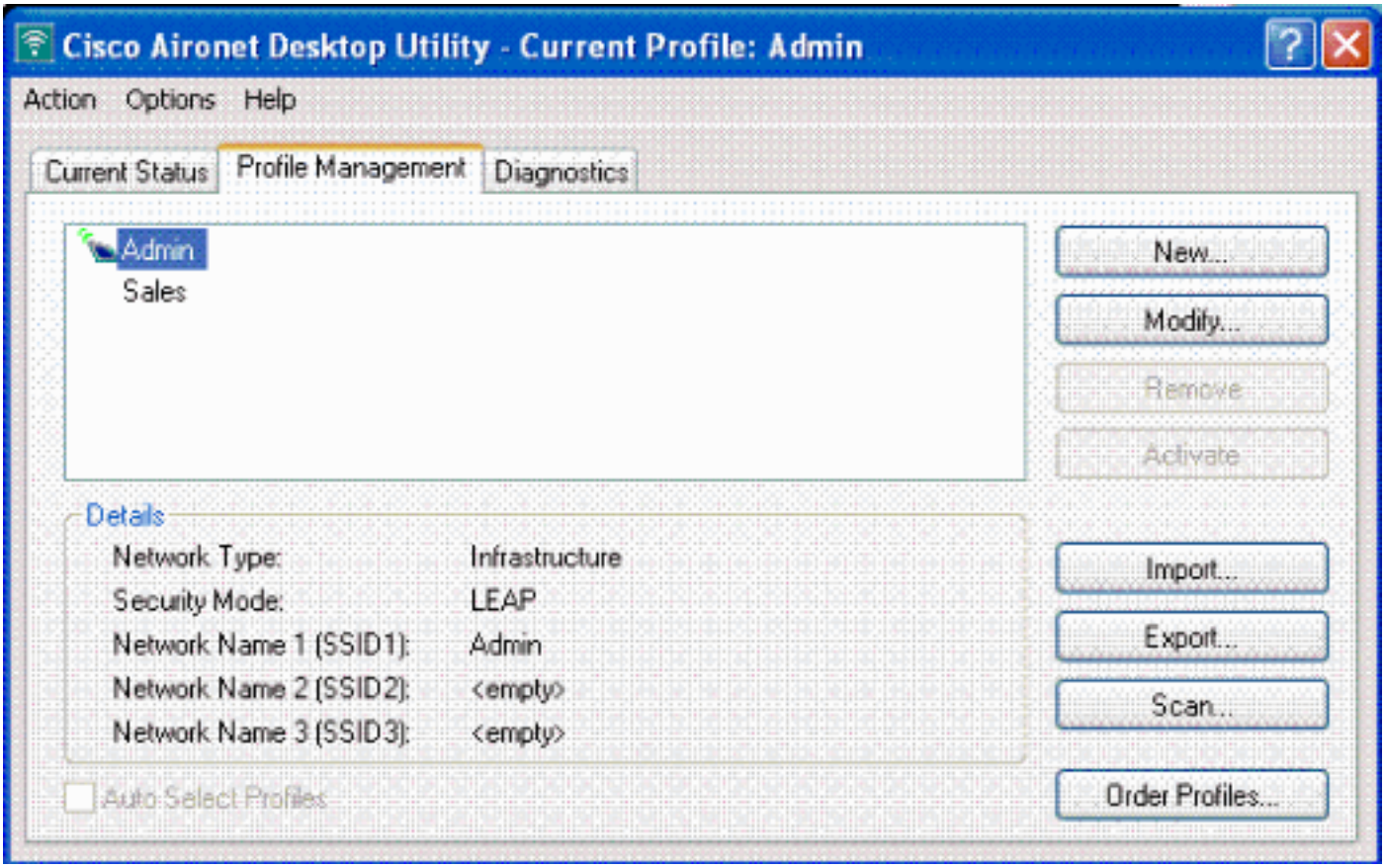


Configure al cliente de red inalámbrica y verifiqúelo

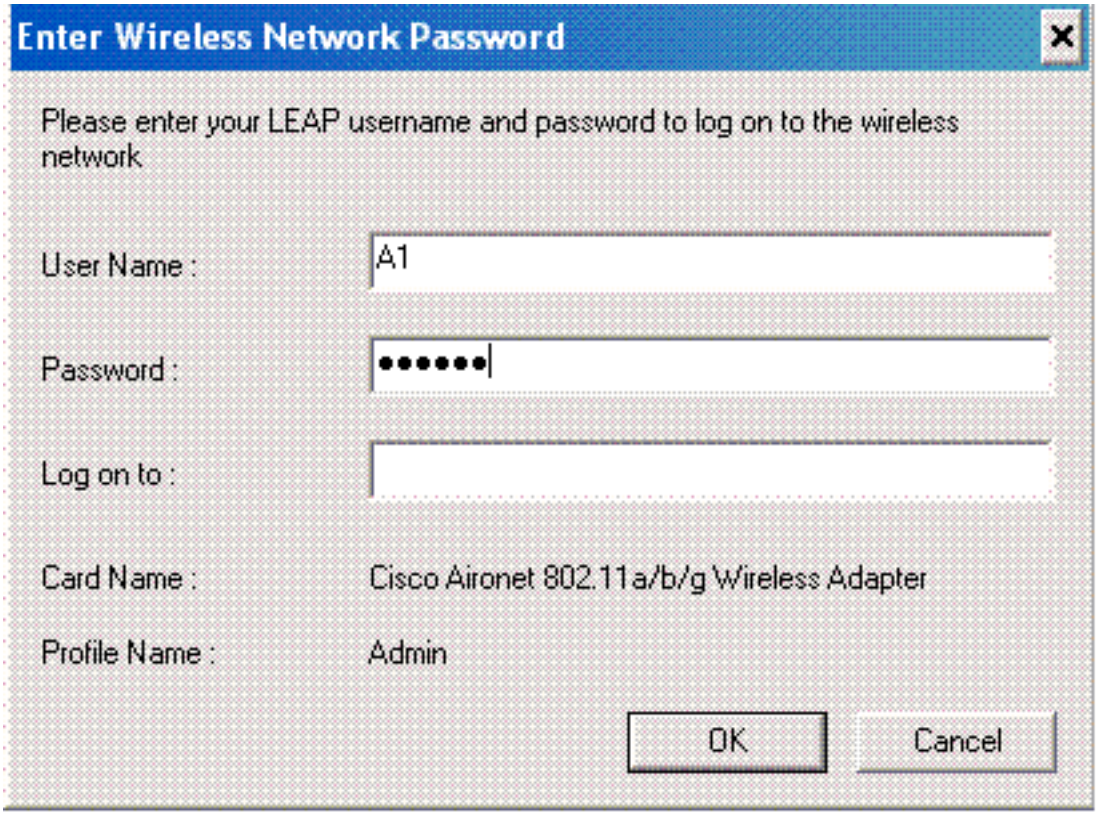
Use esta sección para confirmar que su configuración funciona correctamente. Intente asociar a un cliente de red inalámbrica al REVESTIMIENTO usando la autenticación LEAP para verificar si la configuración trabaja como se esperaba.

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

Nota: Del ADU usted ve que usted ha configurado dos perfiles del cliente. Uno para los usuarios del departamento Admin 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.



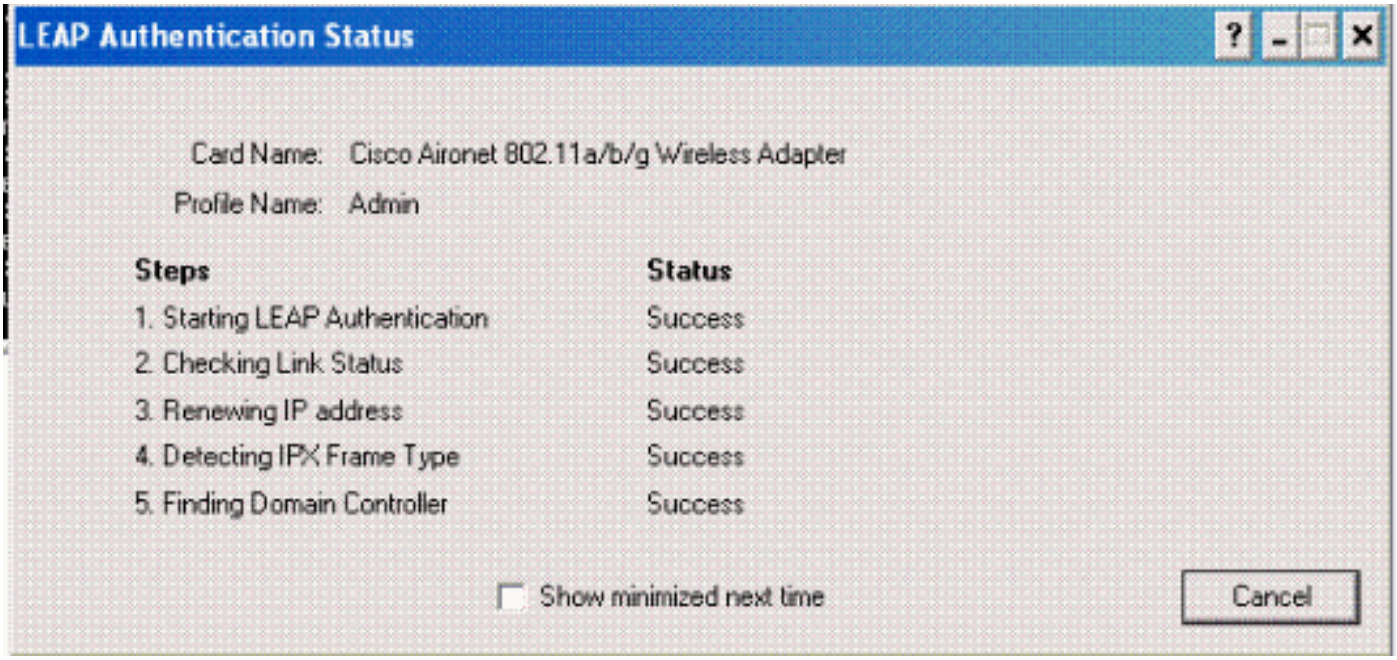
Cuando el perfil para el usuario de red inalámbrica del departamento Admin se activa, piden el usuario proporcionar al username/a la contraseña para la autenticación LEAP. Aquí tiene un ejemplo:



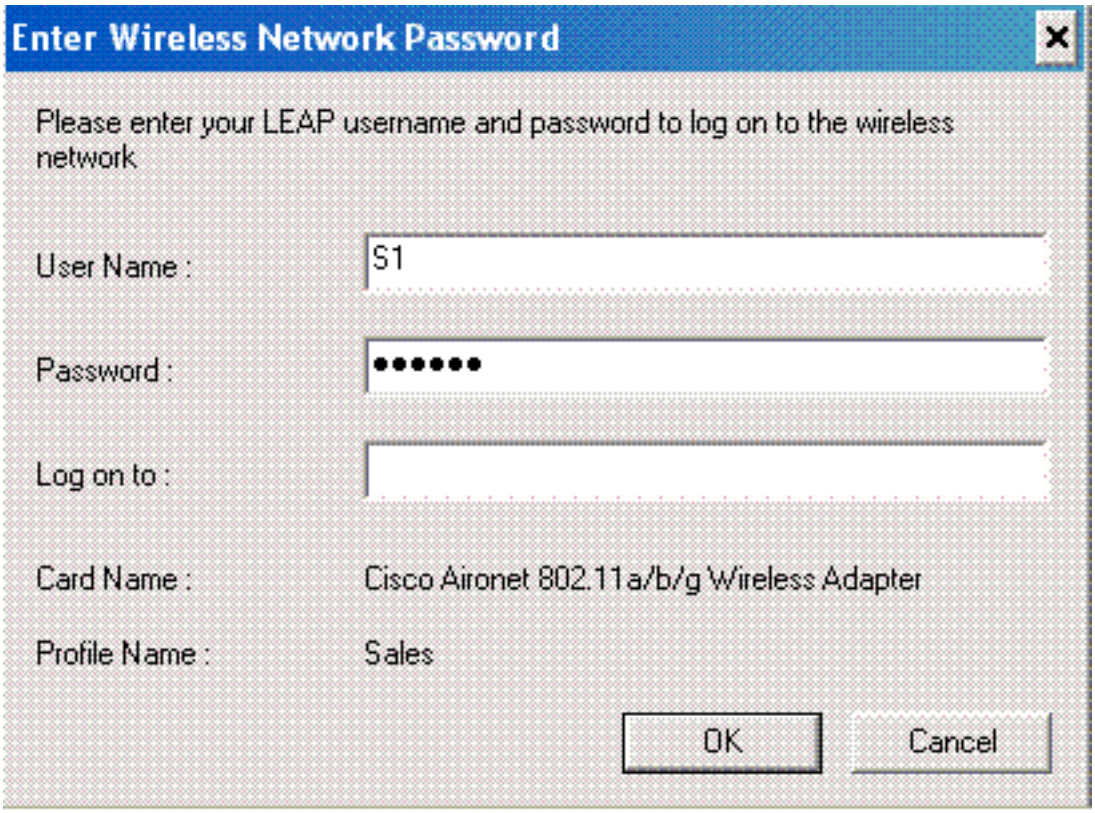
El REVESTIMIENTO y entonces el WLC pasa encendido los credenciales de usuario al servidor de RADIUS externo (Cisco ACS seguro) para validar las credenciales. El WLC pasa encendido las credenciales incluyendo el atributo DNIS (nombre SSID) al servidor de RADIUS para la validación.

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

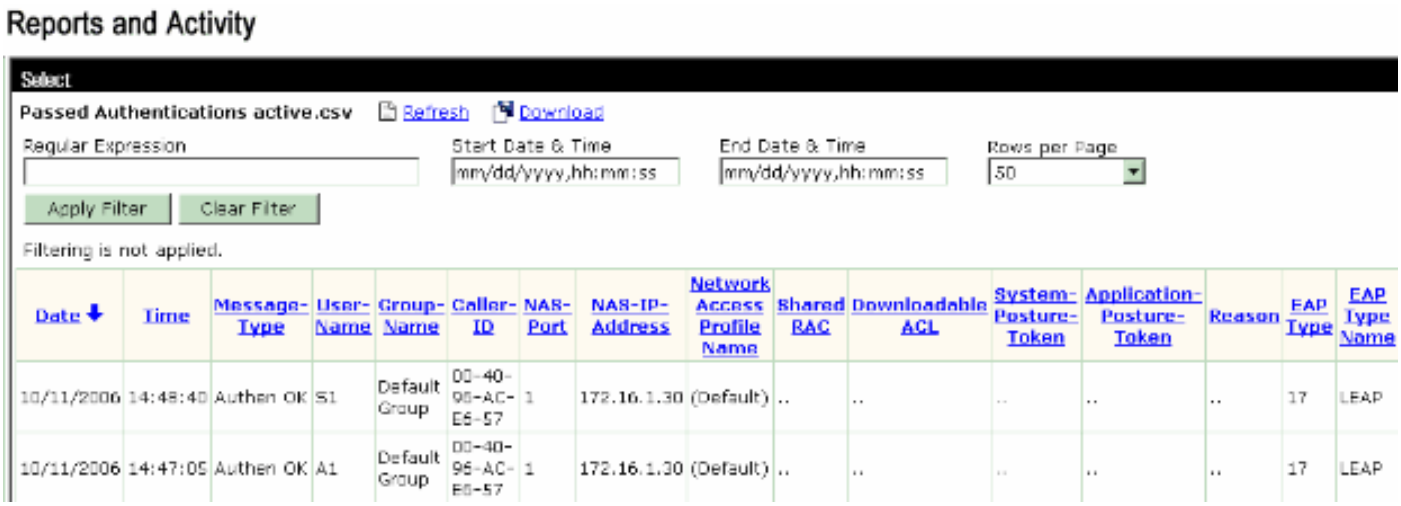
Sobre la autenticación de RADIUS acertada el cliente de red inalámbrica se asocia al REVESTIMIENTO.



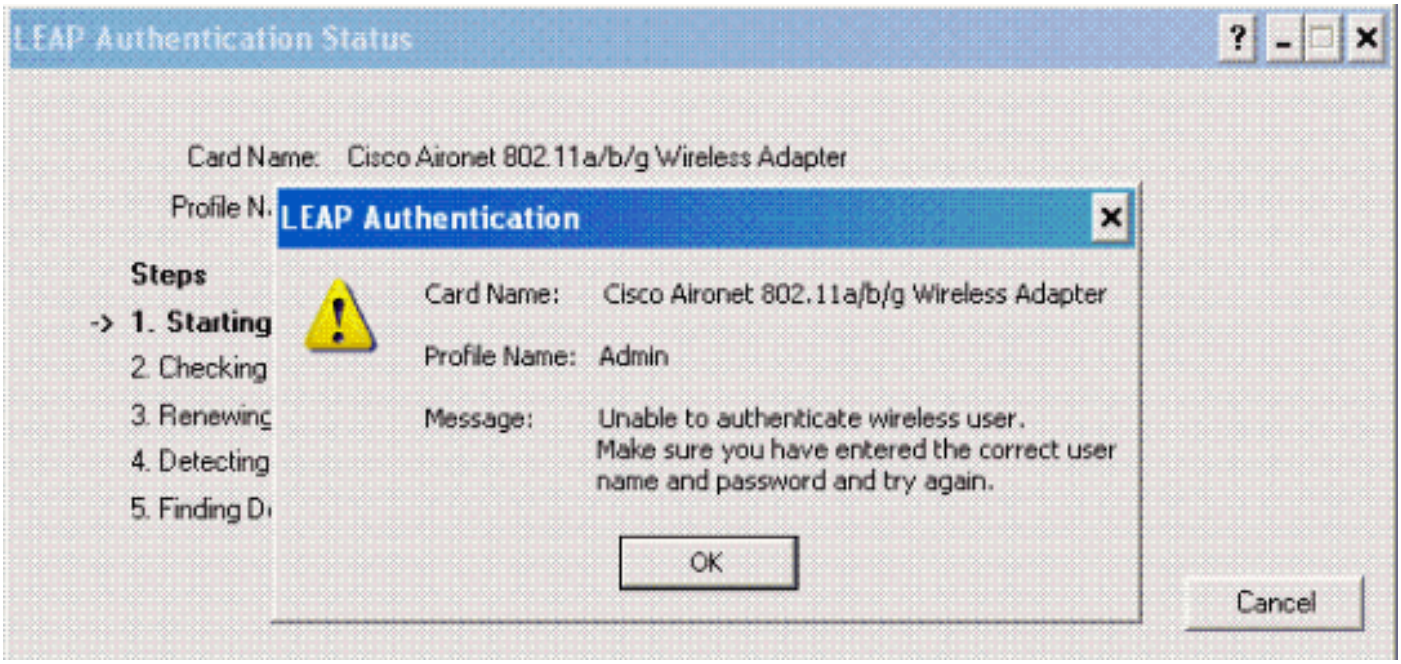
Semejantemente cuando un usuario del Departamento de ventas activa el perfil de las ventas, al servidor de RADIUS autentica al usuario basado en el username del SALTO/la contraseña y el SSID.



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:



Ahora, si el usuario de las ventas intenta tener acceso al **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 de la empresa, 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 el OIT para ver un análisis de la **salida del comando show**.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **ponga a punto el permiso dot1x aaa** — Activa la depuración de las interacciones AAA del 802.1x.

- **permiso del paquete de la depuración dot1x** — Activa la depuración de todos los paquetes dot1x.
- **la depuración aaa todo activa** — Configura la depuración de todos los mensajes AAA.

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

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