Configuración de los servicios de dominio inalámbrico

Contenido

Introducción

Este documento introduce el concepto de Servicios de dominio inalámbrico (WDS). El documento también describe cómo configurar un punto de acceso (AP) o el Wireless LAN Services Module (WLSM) como WDS y al menos otro como un AP de infraestructura. El procedimiento que se describe en este documento ayuda en la configuración de un WDS que sea funcional y permita a los clientes asociarse ya sea al AP de WDS o a un AP de infraestructura. Este documento pretende establecer una base a partir de la cual puede configurar Fast Secure Roaming o introducir un Wireless LAN Solutions Engine (WLSE) en la red, para que pueda utilizar las funciones.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conozca a fondo las redes LAN inalámbricas y los problemas de seguridad inalámbrica.
- Conozca los métodos de seguridad actuales del protocolo de autenticación extensible (EAP).

Componentes Utilizados

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

- AP con Cisco IOS® Software
- Versión 12.3(2)JA2 o posterior del software del IOS de Cisco
- Módulo de servicios LAN inalámbricos Catalyst serie 6500

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos utilizados en este documento comenzaron con una configuración despejada (predeterminada) y una dirección IP en la interfaz BVI1, de modo que se pueda acceder a la unidad desde la GUI del software Cisco IOS o desde la interfaz de línea de comandos (CLI). Si trabaja en una red activa, asegúrese de comprender el impacto potencial de cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Servicios de dominio inalámbrico

WDS es una nueva función para AP en Cisco IOS Software y la base de Catalyst 6500 Series WLSM. WDS es una función central que permite otras funciones como estas:

- Roaming seguro rápido
- interacción WLSE
- Administración de radios

Debe establecer relaciones entre los AP que participan en WDS y WLSM, antes de que otras funciones basadas en WDS funcionen. Uno de los propósitos de WDS es eliminar de la necesidad que tiene el servidor de autenticación de validar las credenciales de usuario y reducir el tiempo requerido para las autenticaciones de los clientes.

Para utilizar WDS, debe designar un AP o el WLSM como el WDS. Un AP WDS debe utilizar un nombre de usuario y una contraseña WDS para establecer una relación con un servidor de autenticación. El servidor de autenticación puede ser un servidor RADIUS externo o la función de servidor RADIUS local en el AP WDS. El WLSM debe tener una relación con el servidor de autenticación, aunque WLSM no necesita autenticarse con el servidor.

Otros AP, llamados AP de infraestructura, se comunican con el WDS. Antes de que se produzca el registro, los AP de infraestructura deben autenticarse en el WDS. Un grupo de servidores de infraestructura en WDS define esta autenticación de infraestructura.

Uno o más grupos de servidores cliente en WDS definen la autenticación de cliente.

Cuando un cliente intenta asociarse a un AP de infraestructura, el AP de infraestructura pasa las credenciales del usuario al WDS para la validación. Si WDS ve las credenciales por primera vez, WDS se dirige al servidor de autenticación para validar las credenciales. El WDS luego almacena en memoria caché las credenciales, para eliminar la necesidad de volver al servidor de autenticación cuando el mismo usuario intenta la autenticación de nuevo. Algunos ejemplos de

reautenticación son:

- Reorientación
- Roaming
- Cuando el usuario inicia el dispositivo cliente

Cualquier protocolo de autenticación EAP basado en RADIUS se puede tunelizar a través de WDS como estos:

- EAP ligero (LEAP)
- EAP protegido (PEAP)
- EAP-seguridad de la capa de transporte (EAP-TLS)
- EAP-autenticación flexible mediante tunelación segura (EAP-FAST)

La autenticación de dirección MAC también puede tunelizarse a un servidor de autenticación externo o a una lista local a un AP WDS. El WLSM no admite la autenticación de direcciones MAC.

El WDS y los AP de infraestructura se comunican a través de un protocolo de multidifusión denominado protocolo de control de contexto de WLAN (WLCCP). Estos mensajes de multidifusión no se pueden rutear, por lo que un WDS y los AP de infraestructura asociados deben estar en la misma subred IP y en el mismo segmento LAN. Entre WDS y WLSE, WLCCP utiliza TCP y protocolo de datagramas de usuario (UDP) en el puerto 2887. Cuando WDS y WLSE están en subredes diferentes, un protocolo como la traducción de direcciones de red (NAT) no puede traducir los paquetes.

Un AP configurado como dispositivo WDS soporta hasta 60 AP participantes. Un router de servicios integrados (ISR) configurado como dispositivos WDS admite hasta 100 puntos de acceso participantes. Además, un switch equipado con WLSM admite hasta 600 puntos de acceso participantes y hasta 240 grupos de movilidad. Un solo AP admite hasta 16 grupos de movilidad.

Nota: Cisco recomienda que los AP de infraestructura ejecuten la misma versión del IOS que el dispositivo WDS. Si utiliza una versión anterior del IOS, los AP podrían no autenticarse en el dispositivo WDS. Además, Cisco recomienda utilizar la última versión del IOS. Puede encontrar la última versión de IOS en la página Descargas inalámbricas.

Función del dispositivo WDS

El dispositivo WDS realiza varias tareas en su LAN inalámbrica:

- Anuncia su capacidad WDS y participa en la elección del mejor dispositivo WDS para su LAN inalámbrica. Cuando configura su LAN inalámbrica para WDS, configura un dispositivo como candidato principal de WDS y uno o más dispositivos adicionales como candidatos de WDS de respaldo. Si el dispositivo WDS principal se desactiva, uno de los dispositivos WDS de respaldo toma su lugar.
- Autentica todos los AP en la subred y establece un canal de comunicación seguro con cada uno de ellos.
- Recopila datos de radio de los AP en la subred, agrega los datos y los reenvía al dispositivo WLSE de la red.
- Actúa como una transferencia para todos los dispositivos cliente 802.1x autenticados asociados a los AP participantes.

- Registra todos los dispositivos cliente en la subred que utilizan claves dinámicas, establece claves de sesión para ellos y almacena en caché sus credenciales de seguridad. Cuando un cliente se traslada a otro AP, el dispositivo WDS reenvía las credenciales de seguridad del cliente al nuevo AP.

Función de los puntos de acceso mediante el dispositivo WDS

Los AP de su LAN inalámbrica interactúan con el dispositivo WDS en estas actividades:

- Descubra y realice un seguimiento del dispositivo WDS actual y transmita los anuncios WDS a la LAN inalámbrica.
- Autentique con el dispositivo WDS y establezca un canal de comunicación seguro para el dispositivo WDS.
- Registre los dispositivos cliente asociados con el dispositivo WDS.
- Informe los datos de radio al dispositivo WDS.

Configuración

WDS presenta la configuración de forma ordenada y modular. Cada concepto se basa en el concepto que precede. El WDS omite otros elementos de configuración como contraseñas, acceso remoto y ajustes de radio para mayor claridad y se centra en el asunto principal.

Esta sección presenta la información necesaria para configurar las funciones descritas en este documento.

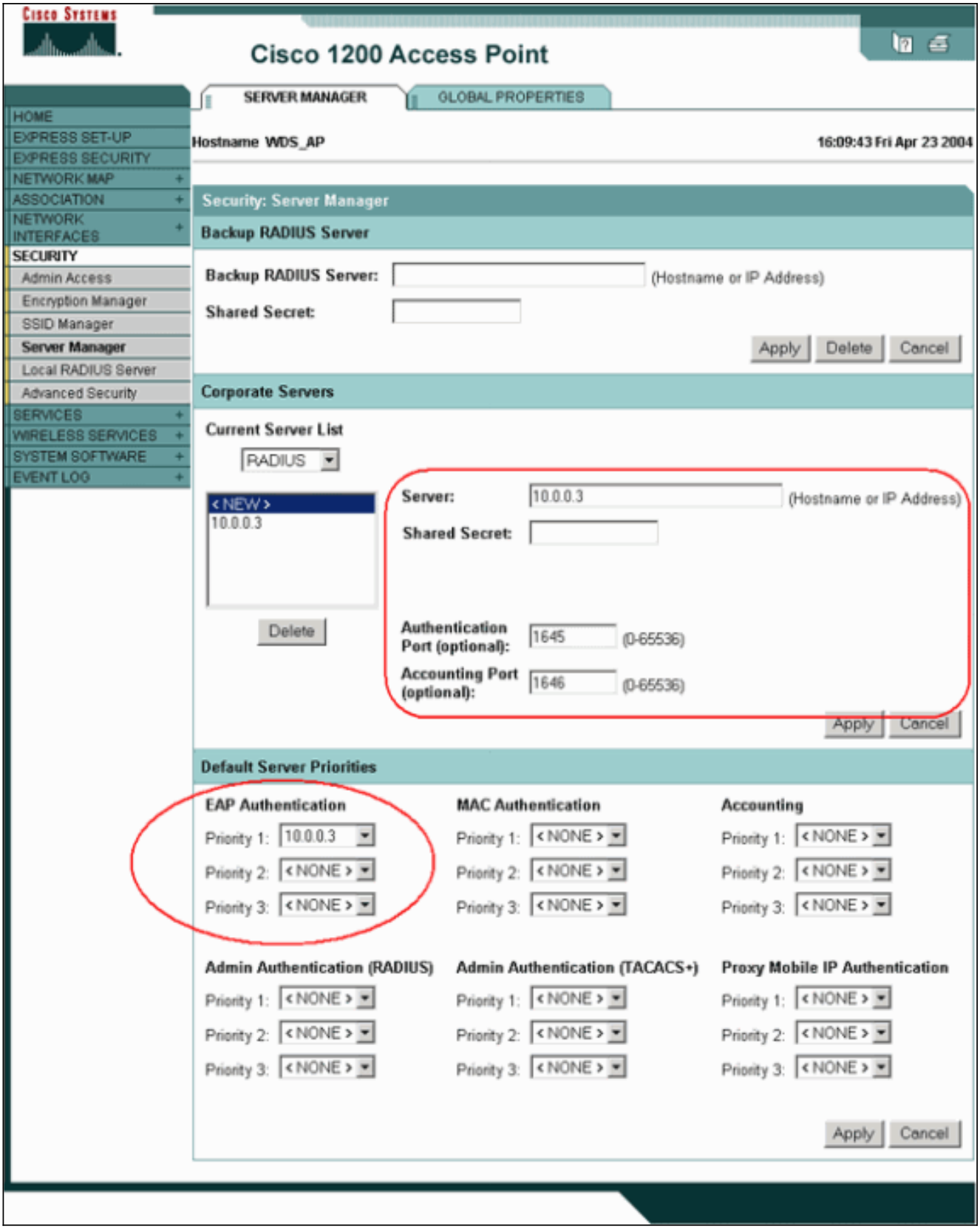
Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Designar un AP como WDS

El primer paso es designar un AP como el WDS. El AP WDS es el único que se comunica con el servidor de autenticación.

Complete estos pasos para designar un AP como WDS:

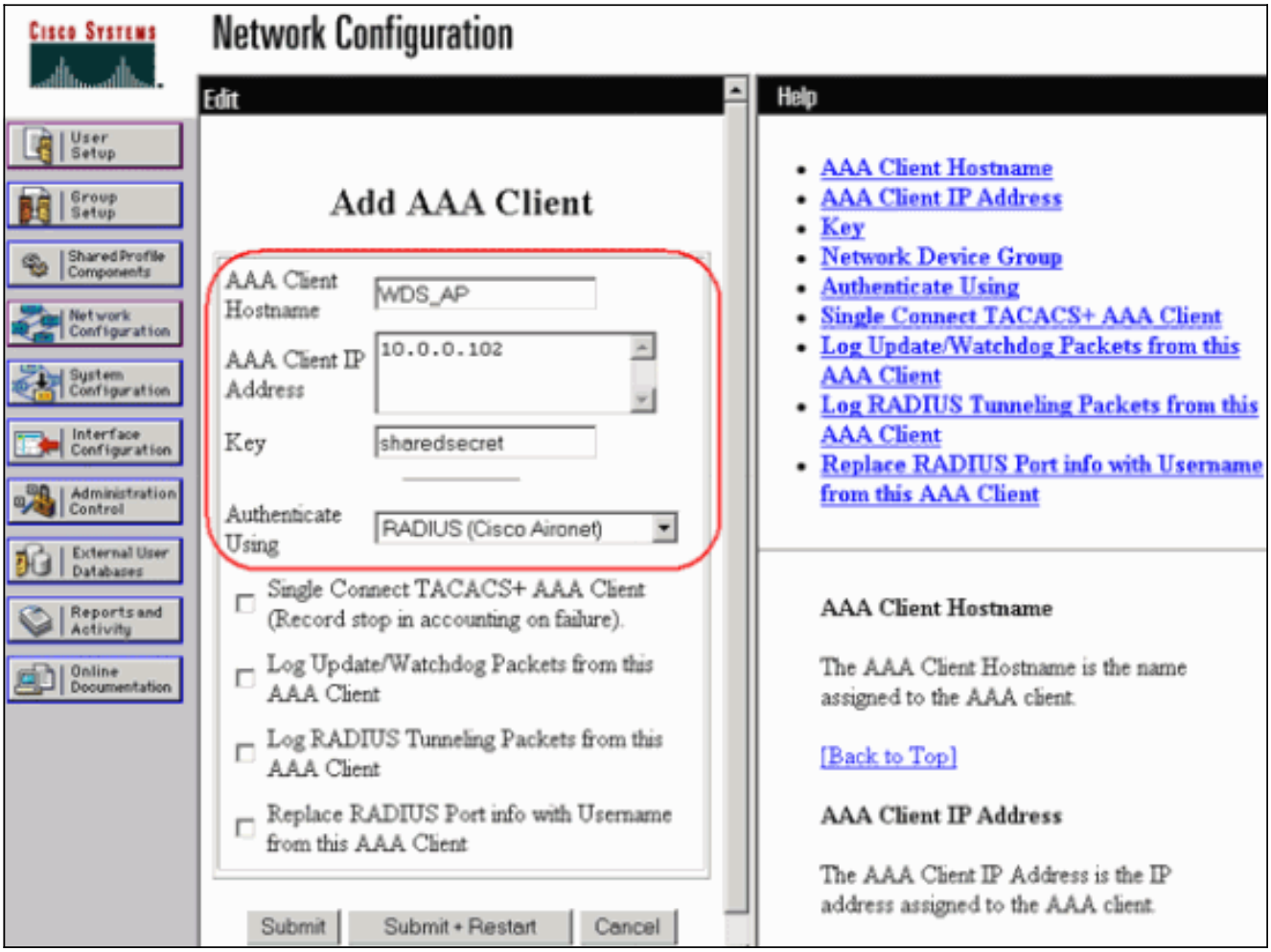
1. Para configurar el servidor de autenticación en el WDS AP, elija **Security > Server Manager** para ir a la pestaña Server Manager:En Servidores corporativos, escriba la dirección IP del servidor de autenticación en el campo Servidor.Especifique el secreto compartido y los puertos.En Prioridades de servidor predeterminadas, establezca el campo Prioridad 1 en esa dirección IP del servidor bajo el tipo de autenticación apropiado.



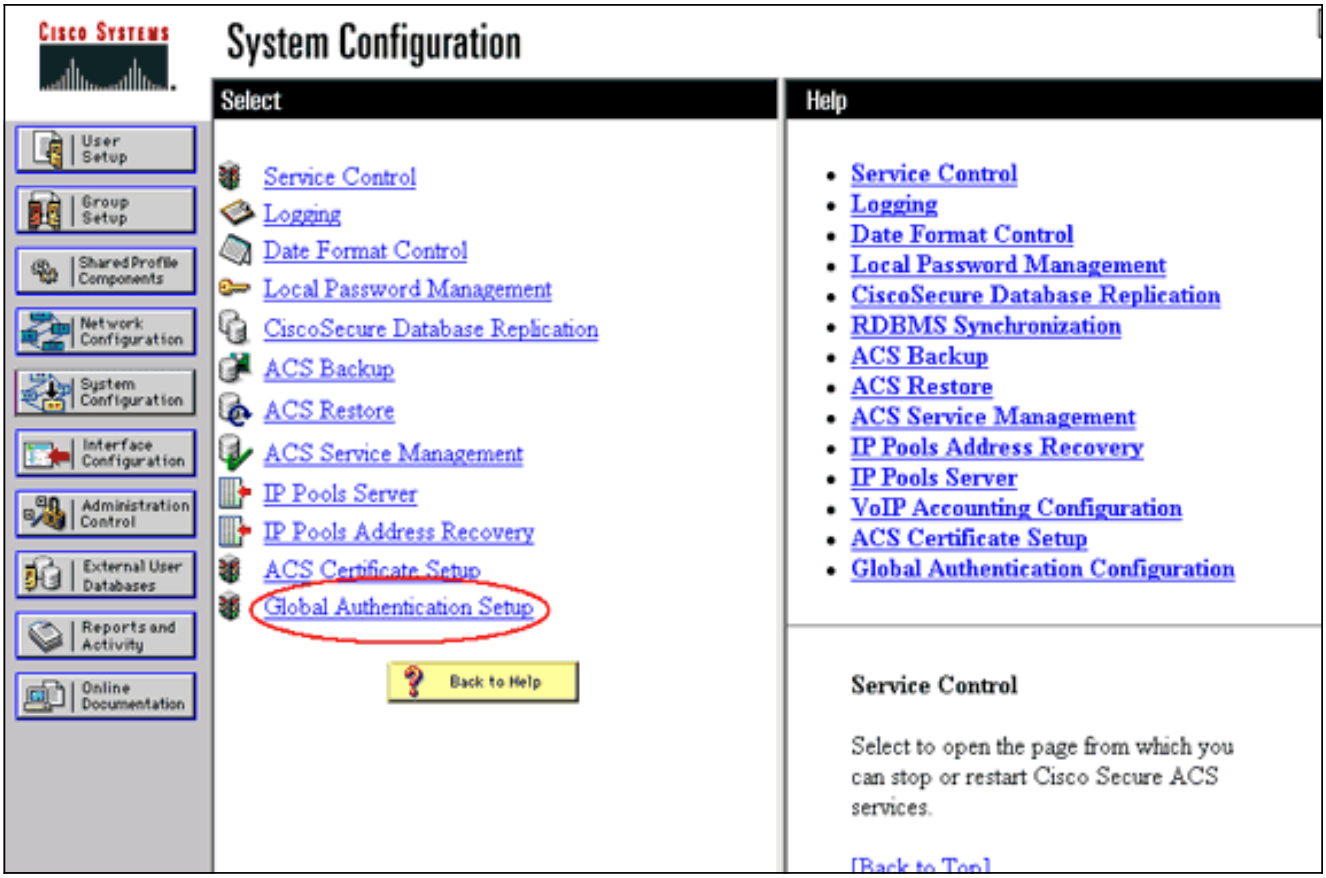
Alternativamente, ejecute estos comandos desde la CLI:

2. El siguiente paso es configurar el WDS AP en el servidor de autenticación como cliente de autenticación, autorización y contabilidad (AAA). Para esto, debe agregar el AP WDS como un cliente AAA. Complete estos pasos:**Nota:** Este documento utiliza el servidor Cisco Secure ACS como servidor de autenticación.En Cisco Secure Access Control Server (ACS), esto ocurre en la página Network Configuration donde define estos atributos para el WDS AP:NombreDirección IPSecreto compartidoMétodo de autentificaciónRADIUS Cisco AironetGrupo de trabajo en ingeniería de Internet [IETF] RADIUSHaga clic en **Enviar**.Para otros servidores de autenticación no ACS, consulte la documentación del

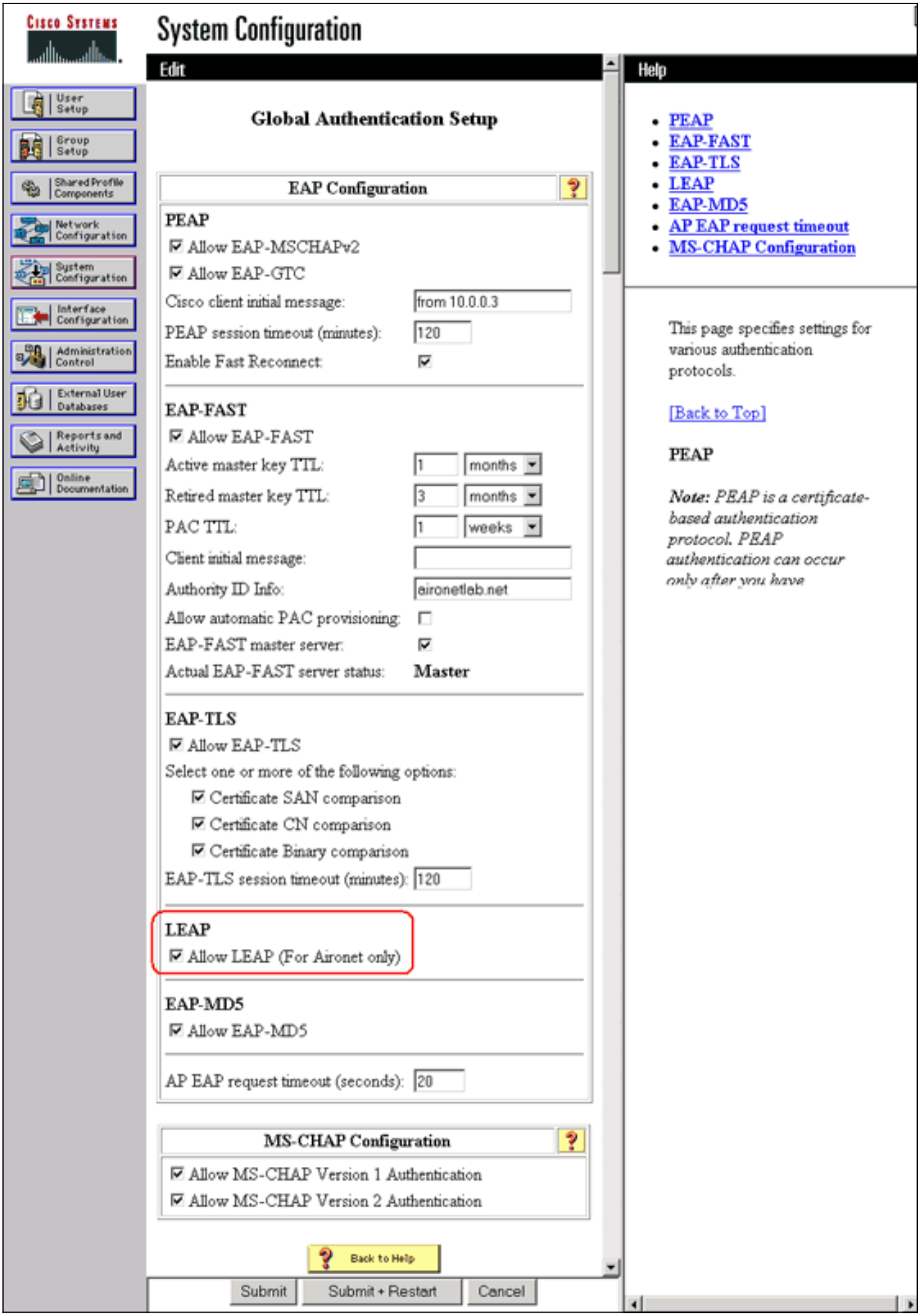
fabricante.



Además, en Cisco Secure ACS, asegúrese de configurar ACS para realizar la autenticación LEAP en la página Configuración del sistema - Configuración de autenticación global. Primero, haga clic en **Configuración del sistema** y luego haga clic en **Configuración de autenticación global**.

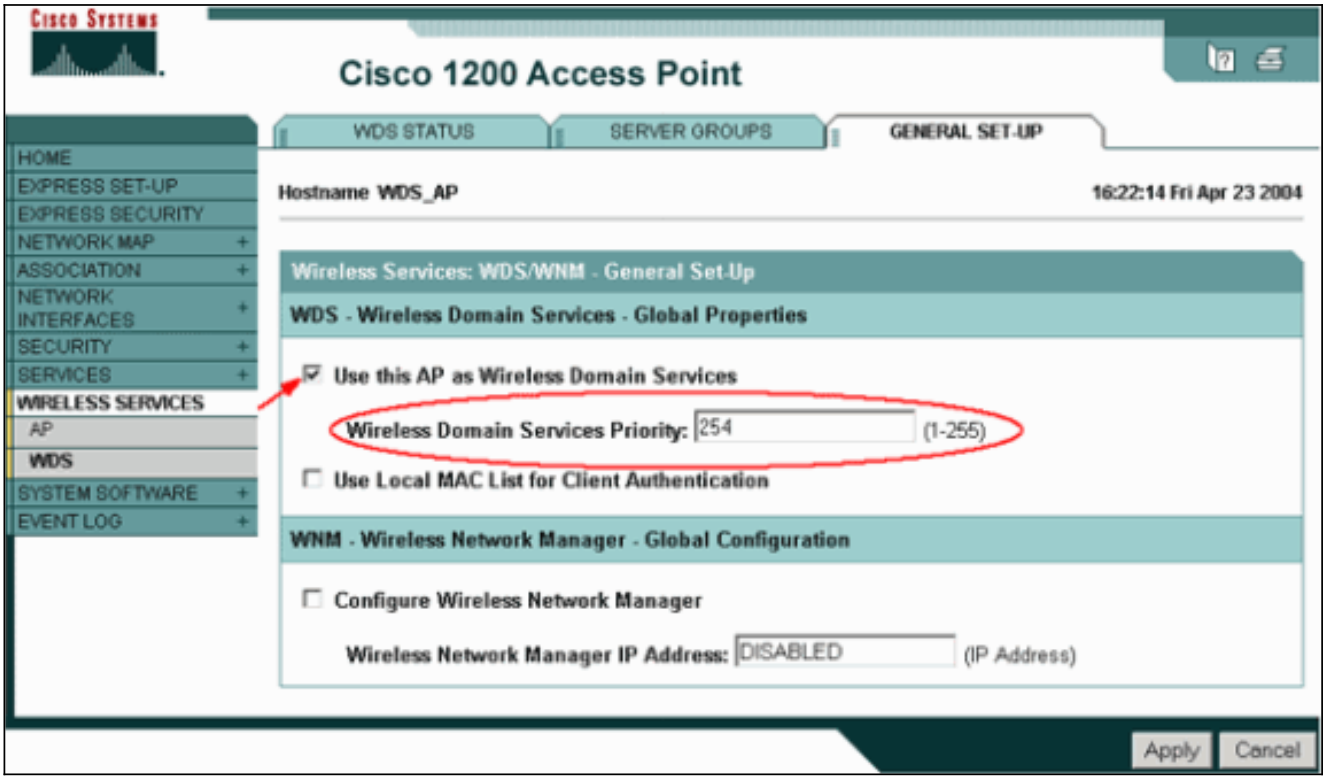


Desplácese hacia abajo en la página hasta la configuración LEAP. Cuando usted examina la caja, ACS autentica
LEAP.



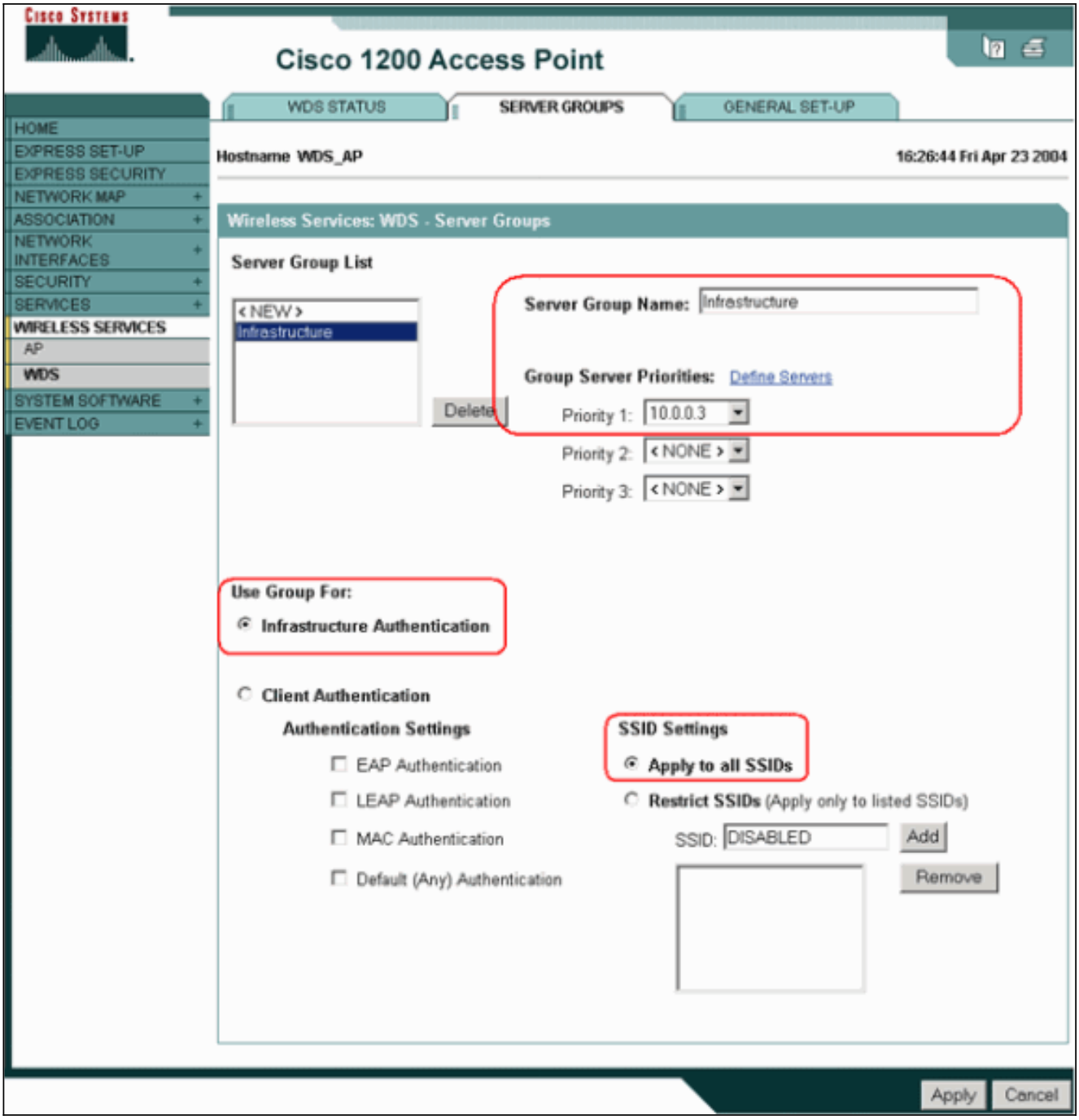
3. Para configurar los parámetros WDS en el WDS AP, elija **Wireless Services > WDS** en el WDS AP y haga clic en la **ficha General Set-Up**. Siga estos pasos:Bajo WDS-Wireless Domain Services - Global Properties , verifique **Use this AP as Wireless Domain**

Services.Establezca el valor para el campo Wireless Domain Services Priority en un valor aproximado de **254**, porque éste es el primero. Puede configurar uno o más AP o switches como candidatos para proporcionar WDS. El dispositivo con la prioridad más alta proporciona
WDS.



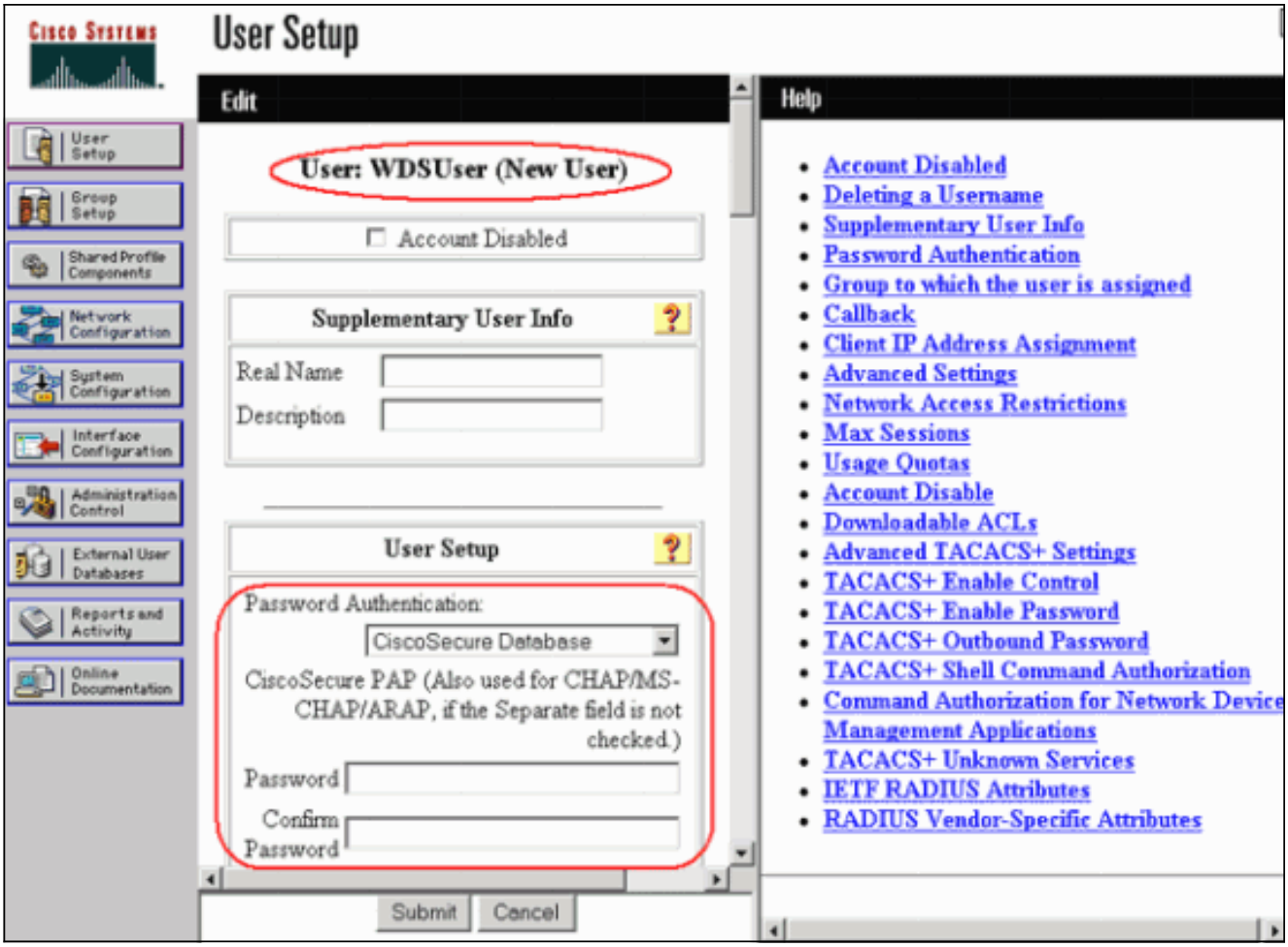
Alternativamente, ejecute estos comandos desde la CLI:

4. Elija **Wireless Services > WDS** y vaya a la **ficha Server Groups**:Defina un nombre de grupo de servidores que autentique los otros APs, un grupo de infraestructura.Establezca Prioridad 1 para el servidor de autenticación configurado previamente.Haga clic en **Usar grupo para:** Botón de opción **Autenticación de infraestructura**.Aplique los parámetros a los identificadores de conjunto de servicios (SSID)
pertinentes.



Alternativamente, ejecute estos comandos desde la CLI:

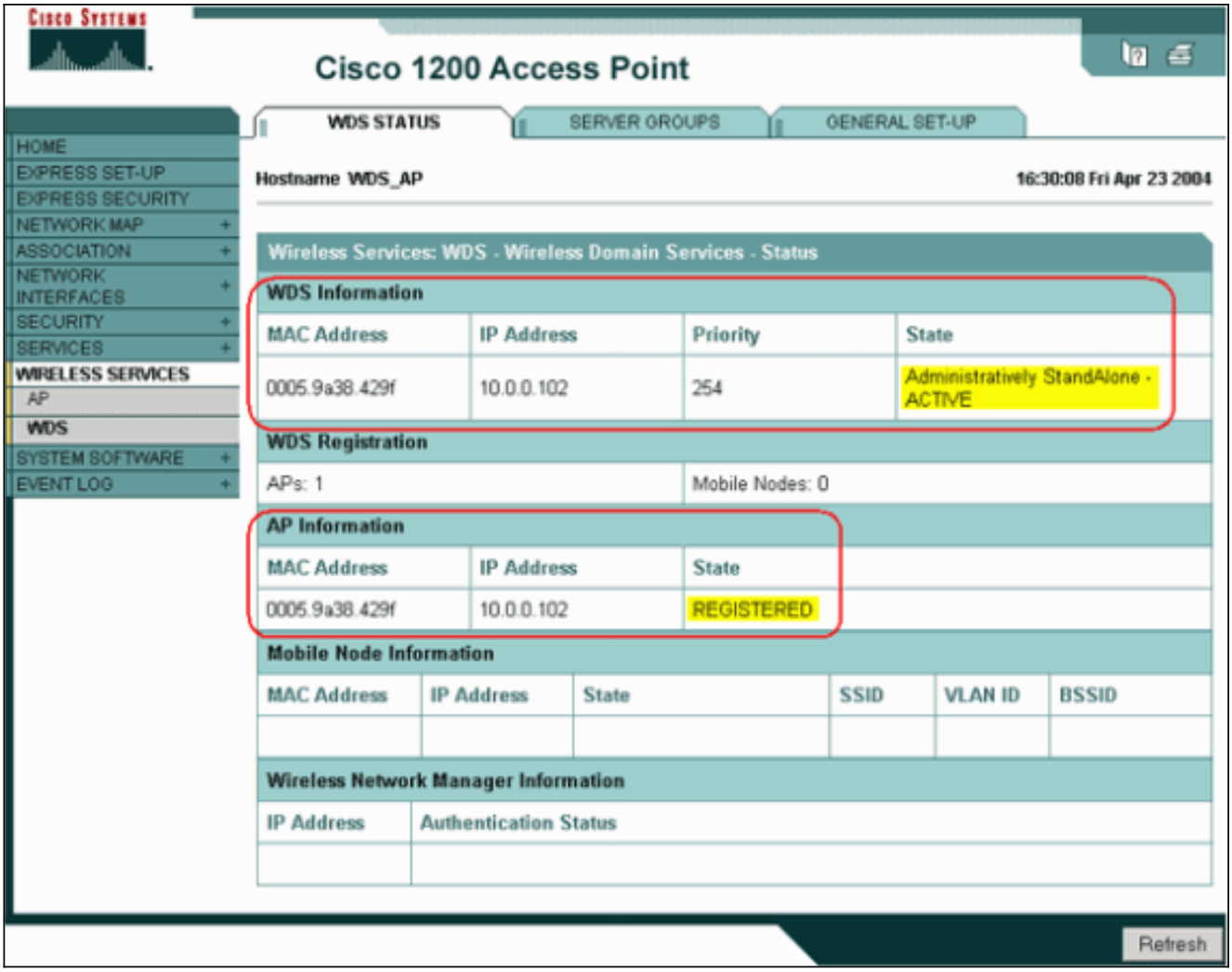
5. Configure el nombre de usuario y la contraseña de WDS como usuario en su servidor de autenticación.En Cisco Secure ACS, esto ocurre en la página User Setup, donde define el nombre de usuario y la contraseña de WDS. Para otros servidores de autenticación no ACS, consulte la documentación del fabricante.**Nota:** No coloque al usuario WDS en un grupo al que se le asignan muchos derechos y privilegios: WDS sólo requiere autenticación limitada.



6. Elija **Wireless Services > AP** y haga clic en **Enable** para la opción Participar en la infraestructura SWAN. A continuación, escriba el nombre de usuario y la contraseña de WDS.Debe definir un nombre de usuario y una contraseña de WDS en el servidor de autenticación para todos los dispositivos que sean designados miembros del WDS.

Alternativamente, ejecute estos comandos desde la CLI:

7. Elija **Wireless Services > WDS**. En la pestaña WDS AP WDS Status , verifique si el WDS AP aparece en el área WDS Information, en el estado ACTIVE. El AP también debe aparecer en el área de información AP, con el estado REGISTRADO.Si el AP no aparece REGISTRADO o ACTIVE, verifique el servidor de autenticación para ver si hay errores o intentos fallidos de autenticación.Cuando el AP se registra adecuadamente, agregue un AP de infraestructura para utilizar los servicios del
WDS.



Alternativamente, ejecute estos comandos desde la CLI:**Nota:** No puede probar las asociaciones de clientes porque la autenticación de cliente todavía no tiene provisiones.

Designar un WLSM como WDS

Esta sección explica cómo configurar un WLSM como WDS. WDS es el único dispositivo que se comunica con el servidor de autenticación.

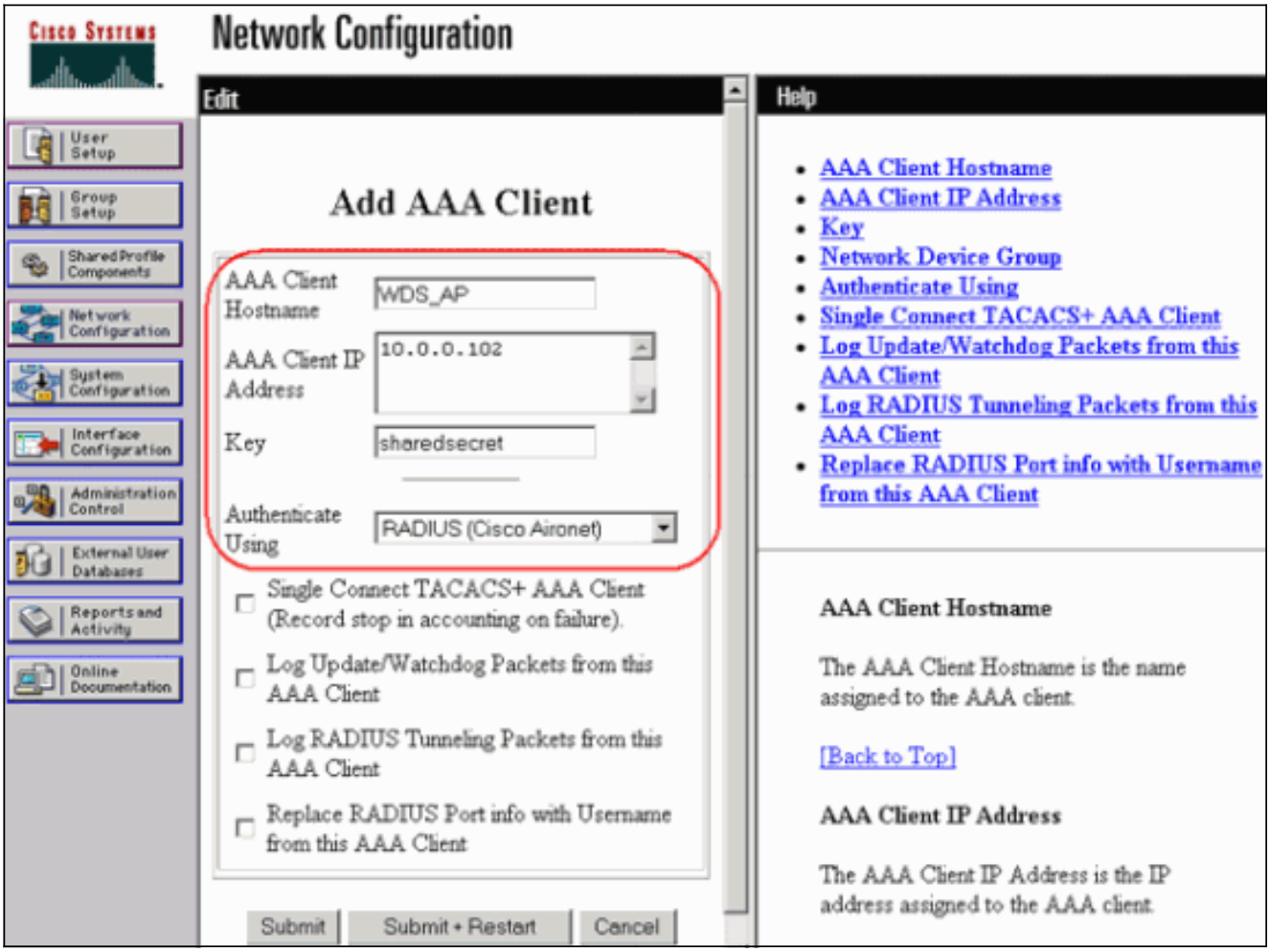
Nota: Ejecute estos comandos en el indicador de comandos `enable` del WLSM, no del Supervisor Engine 720. Para llegar al símbolo del sistema de WLSM, ejecute estos comandos en un símbolo del sistema `enable` en Supervisor Engine 720:

```
c6506#session slot x proc 1
!--- In this command, x is the slot number where the
WLSM resides. The default escape character is Ctrl-^,
then x. You can also type 'exit' at the remote prompt to
end the session Trying 127.0.0.51 ... Open User Access
Verification Username: <username> Password: <password>
wlan>enable
Password: <enable password>
wlan#
```

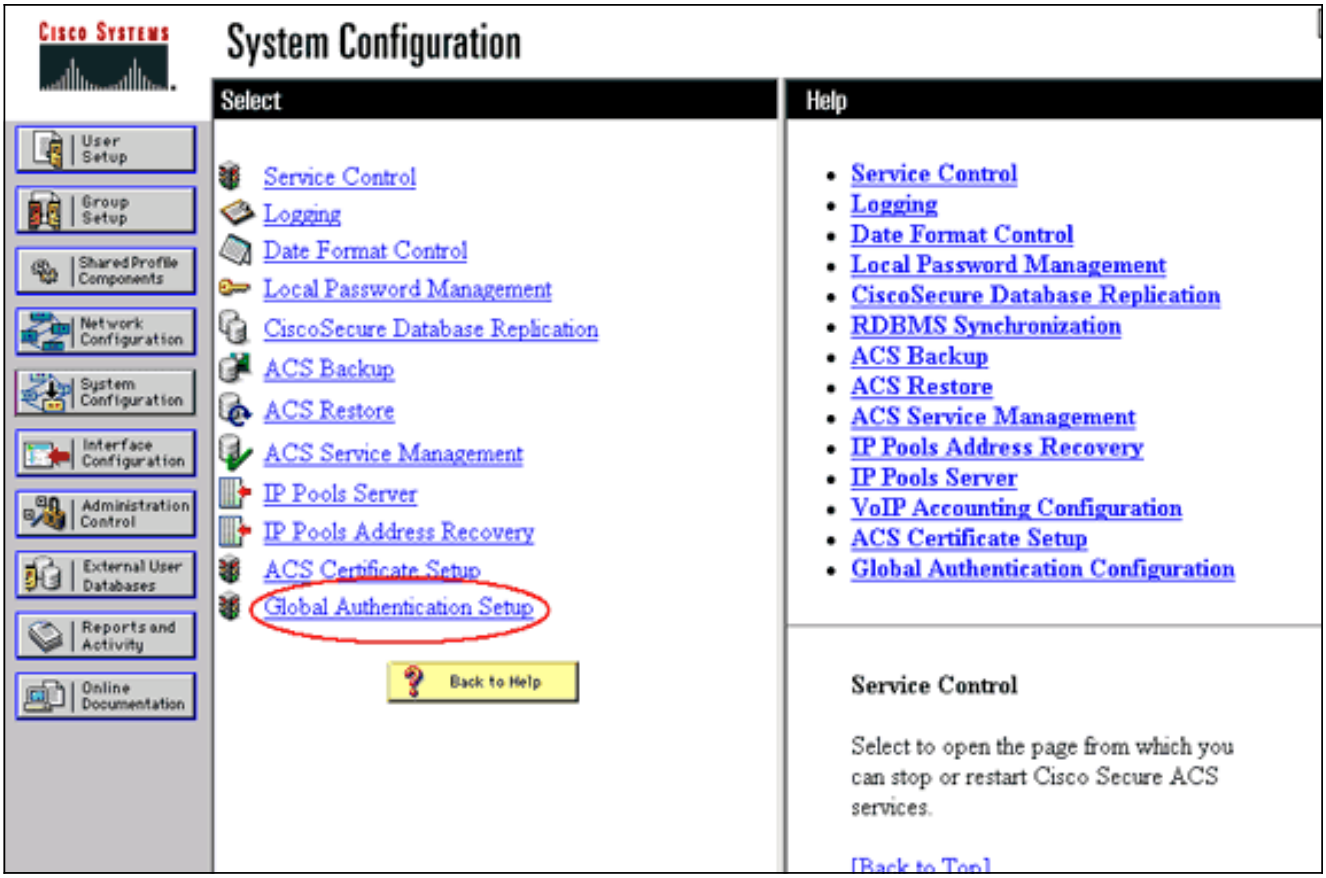
Nota: Para resolver problemas y mantener su WLSM más fácilmente, configure el acceso remoto Telnet al WLSM. Consulte Configuración de acceso remoto de Telnet.

Para designar un WLSM como WDS:

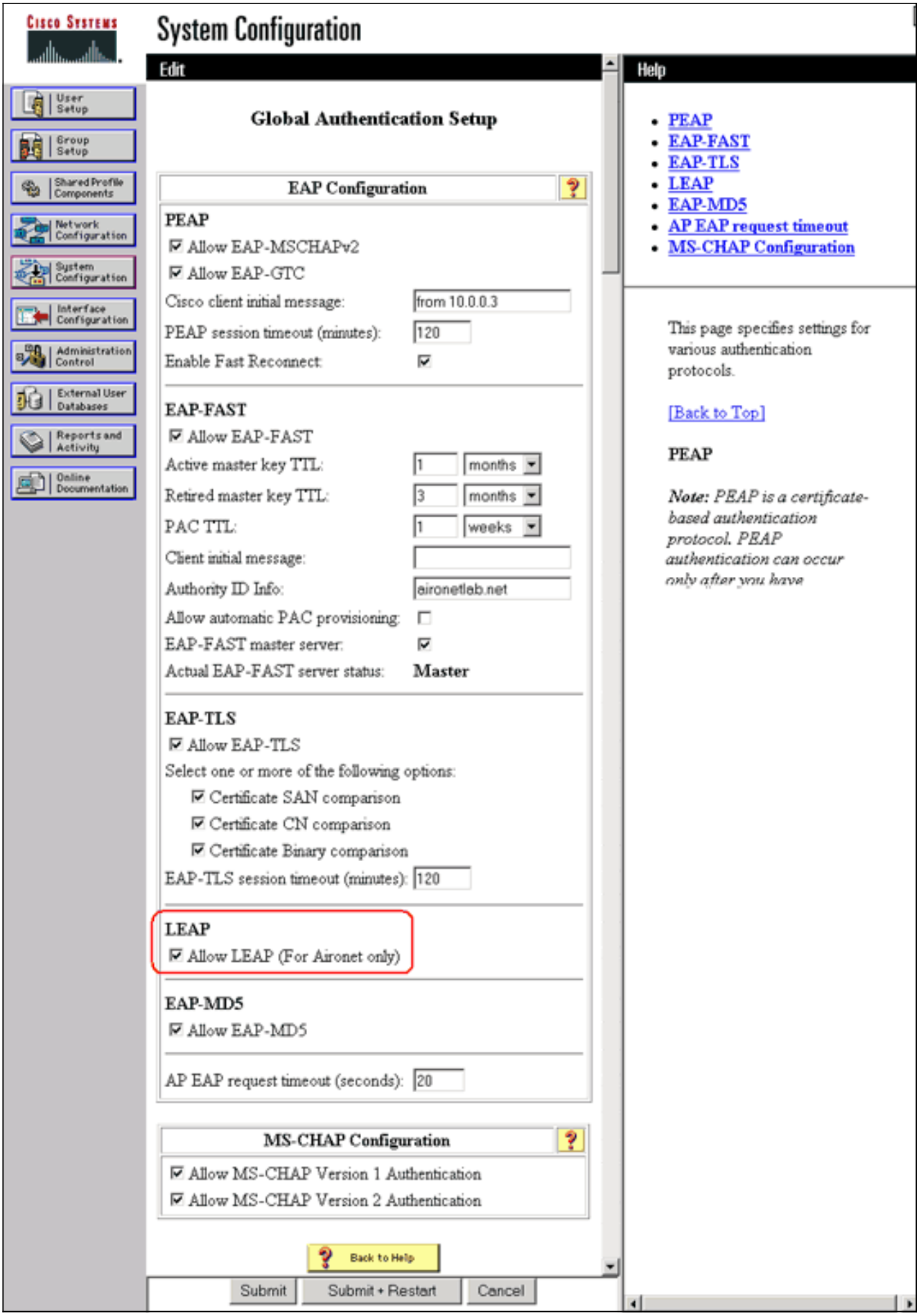
1. Desde la CLI del WLSM, ejecute estos comandos y establezca una relación con el servidor de autenticación:**Nota:** No hay control de prioridad en el WLSM. Si la red contiene varios módulos WLSM, WLSM utiliza configuración de redundancia para determinar el módulo primario.
2. Configure el WLSM en el servidor de autenticación como un cliente AAA.En Cisco Secure ACS, esto ocurre en la página Network Configuration donde define estos atributos para el WLSM:NombreDirección IPSecreto compartidoMétodo de autentificaciónRADIUS Cisco AironetIETF RADIUSPara otros servidores de autenticación no ACS, consulte la documentación del
fabricante.



Además, en Cisco Secure ACS, configure ACS para realizar la autenticación LEAP en la página Configuración del sistema - Configuración de autenticación global. Primero, haga clic en **Configuración del sistema** y luego haga clic en **Configuración de autenticación global**.



Desplácese hacia abajo en la página hasta la configuración LEAP. Cuando usted examina la caja, ACS autentica
LEAP.



3. En el WLSM, defina un método que autentique los otros APs (un grupo de servidores de infraestructura).
4. En WLSM, defina un método que autentique los dispositivos del cliente (un grupo de

servidores de clientes) y los tipos de EAP que dichos clientes utilizan.**Nota:** Este paso elimina la necesidad del proceso Definir método de autenticación de cliente.

5. Defina una VLAN única entre el Supervisor Engine 720 y el WLSM para permitir que el WLSM se comunique con entidades externas como AP y servidores de autenticación. Esta VLAN no se utiliza en ningún otro lugar ni para ningún otro propósito en la red. Cree primero la VLAN en Supervisor Engine 720 y luego ejecute estos comandos:En Supervisor Engine 720:En WLSM:
6. Verifique la función del WLSM con estos comandos:En WLSM:En Supervisor Engine 720:

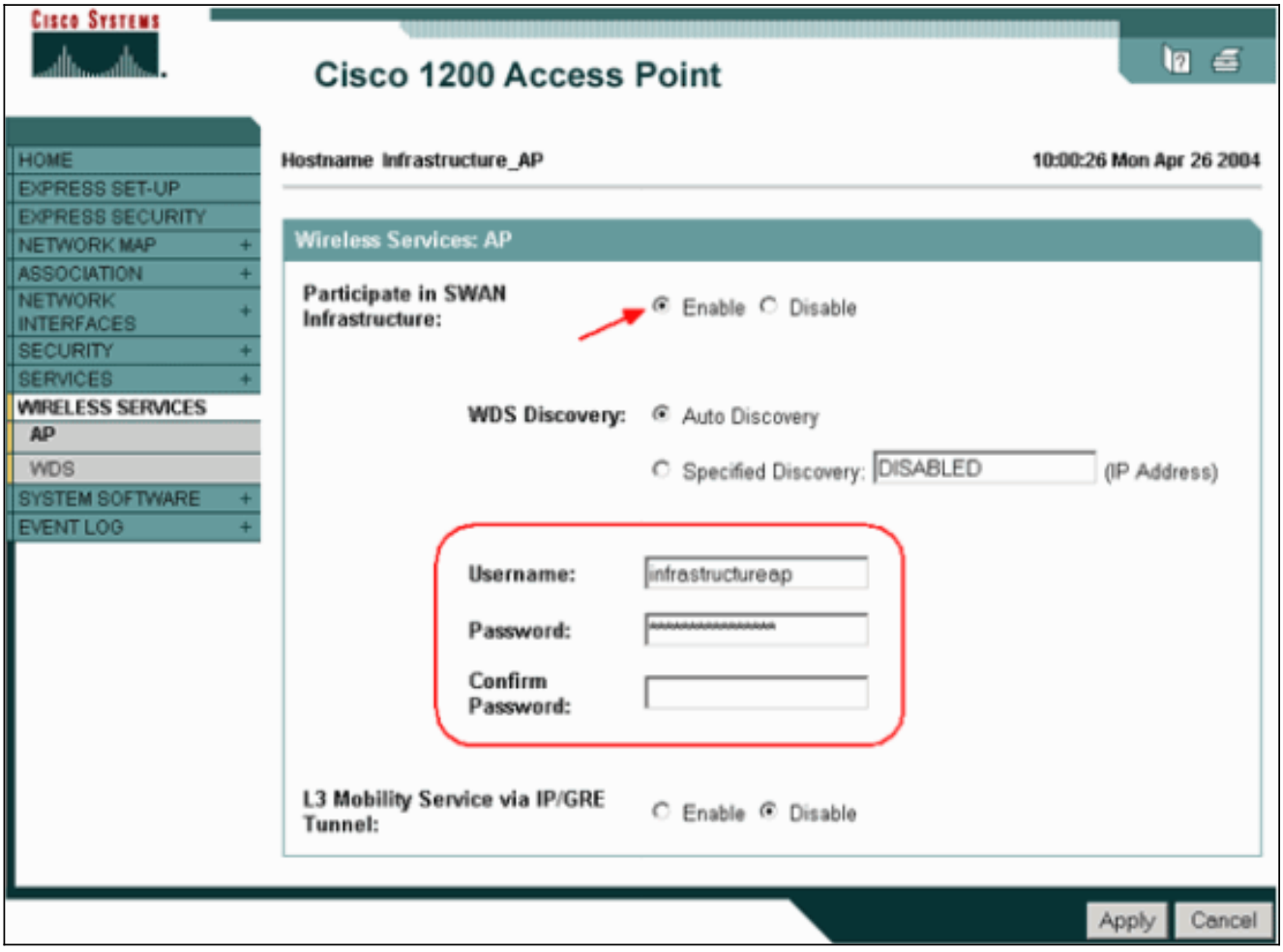
Designar un AP como dispositivo de infraestructura

A continuación, debe designar al menos un AP de infraestructura y relacionar el AP con el WDS. Los clientes se asocian a AP de infraestructura. Los AP de infraestructura solicitan al WDS AP o WLSM que realice la autenticación para ellos.

Complete estos pasos para agregar un AP de infraestructura que utilice los servicios de WDS:

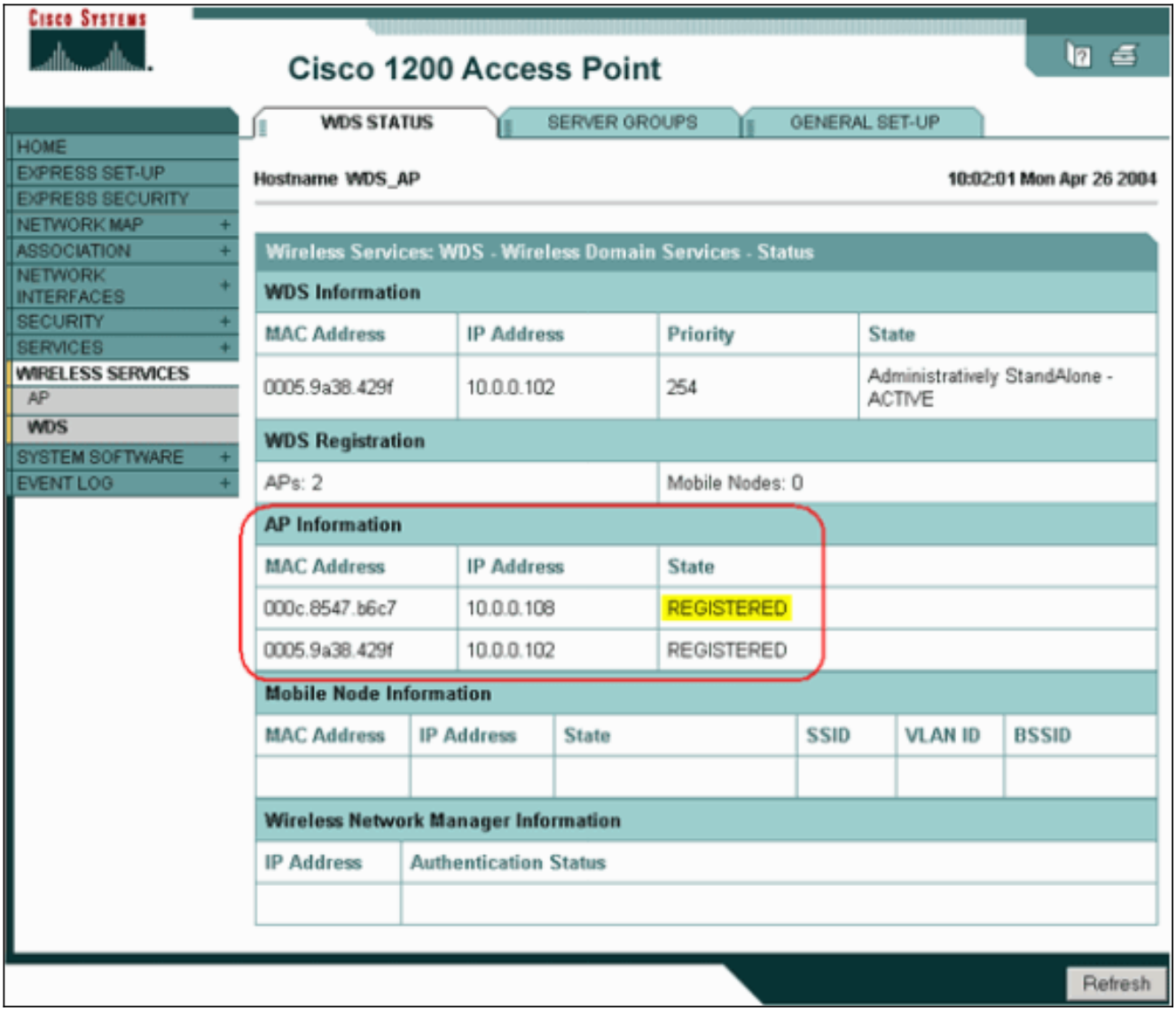
Nota: Esta configuración se aplica solamente a los AP de infraestructura y no al AP WDS.

1. Elija **Wireless Services > AP**. En el AP de infraestructura, seleccione **Enable** para la opción Wireless Services . A continuación, escriba el nombre de usuario y la contraseña de WDS.Debe definir un nombre de usuario y contraseña WDS en el servidor de autenticación para todos los dispositivos que serán miembros de WDS.



Alternativamente, ejecute estos comandos desde la CLI:

2. Elija **Wireless Services > WDS**. En la pestaña WDS AP WDS Status , el nuevo AP de infraestructura aparece en el área WDS Information , con State as ACTIVE , y en el área AP Information , con State as REGISTERED .Si el AP no aparece ACTIVE y/o REGISTERED, verifique el servidor de autenticación para ver si hay errores o intentos fallidos de autenticación.Después de que el AP aparezca ACTIVE y/o REGISTERED, agregue un método de autenticación de cliente al
WDS.



Alternativamente, ejecute este comando desde la CLI:Alternativamente, ejecute este comando desde el WLSM:Luego, ejecute este comando en el AP de infraestructura:**Nota:** No puede probar las asociaciones de clientes porque la autenticación de cliente todavía no tiene provisiones.

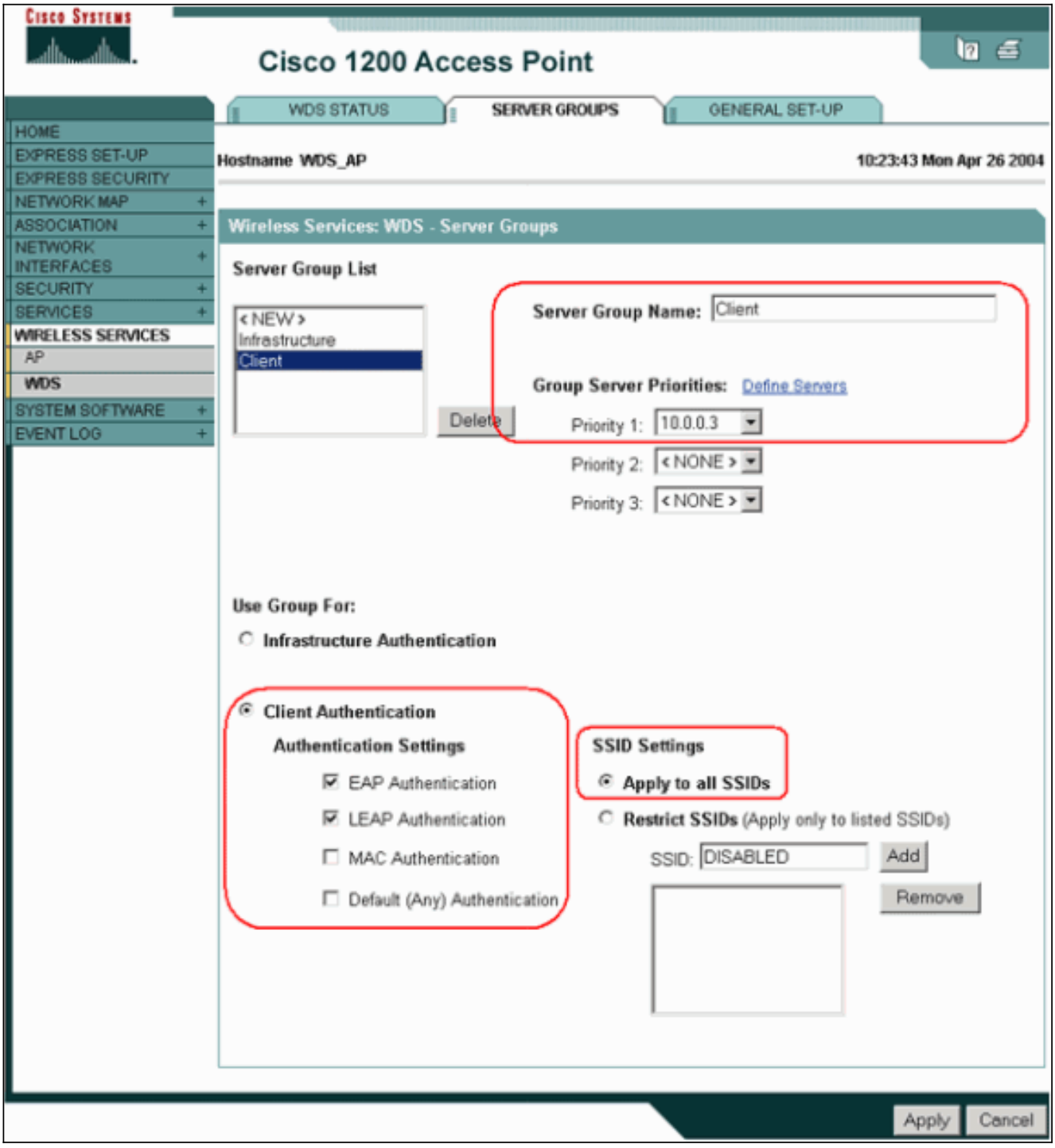
Definir método de autenticación de cliente

Finalmente, defina un método de autenticación de cliente.

Complete estos pasos para agregar un método de autenticación de cliente:

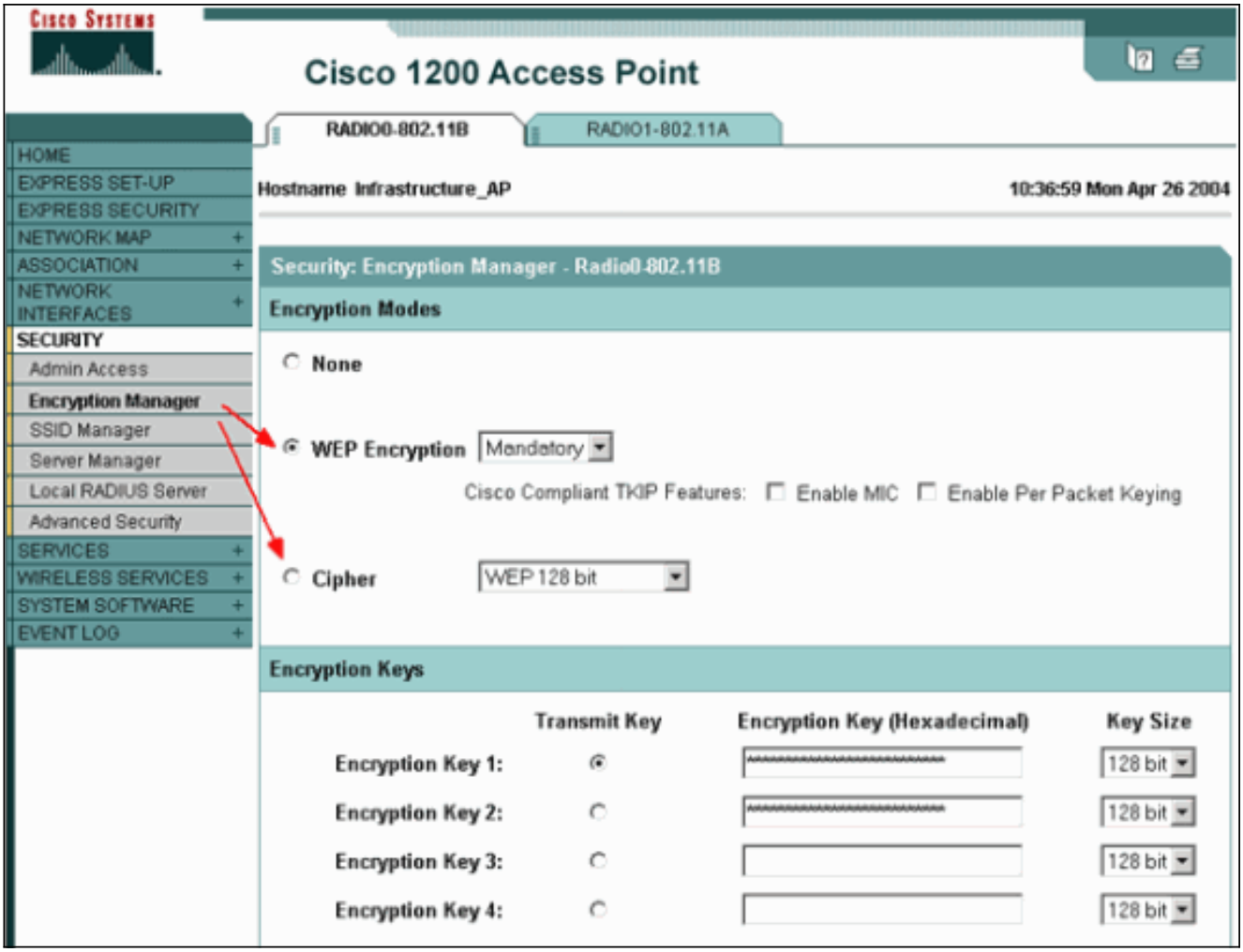
1. Elija **Wireless Services > WDS**. Realice estos pasos en la pestaña WDS AP Server Groups:Defina un grupo de servidores que autentique clientes (un grupo de clientes).Establezca Prioridad 1 para el servidor de autenticación configurado

previamente.Establezca el tipo de autenticación aplicable (LEAP, EAP, MAC, etc.).Aplique la configuración a los SSID
relevantes.

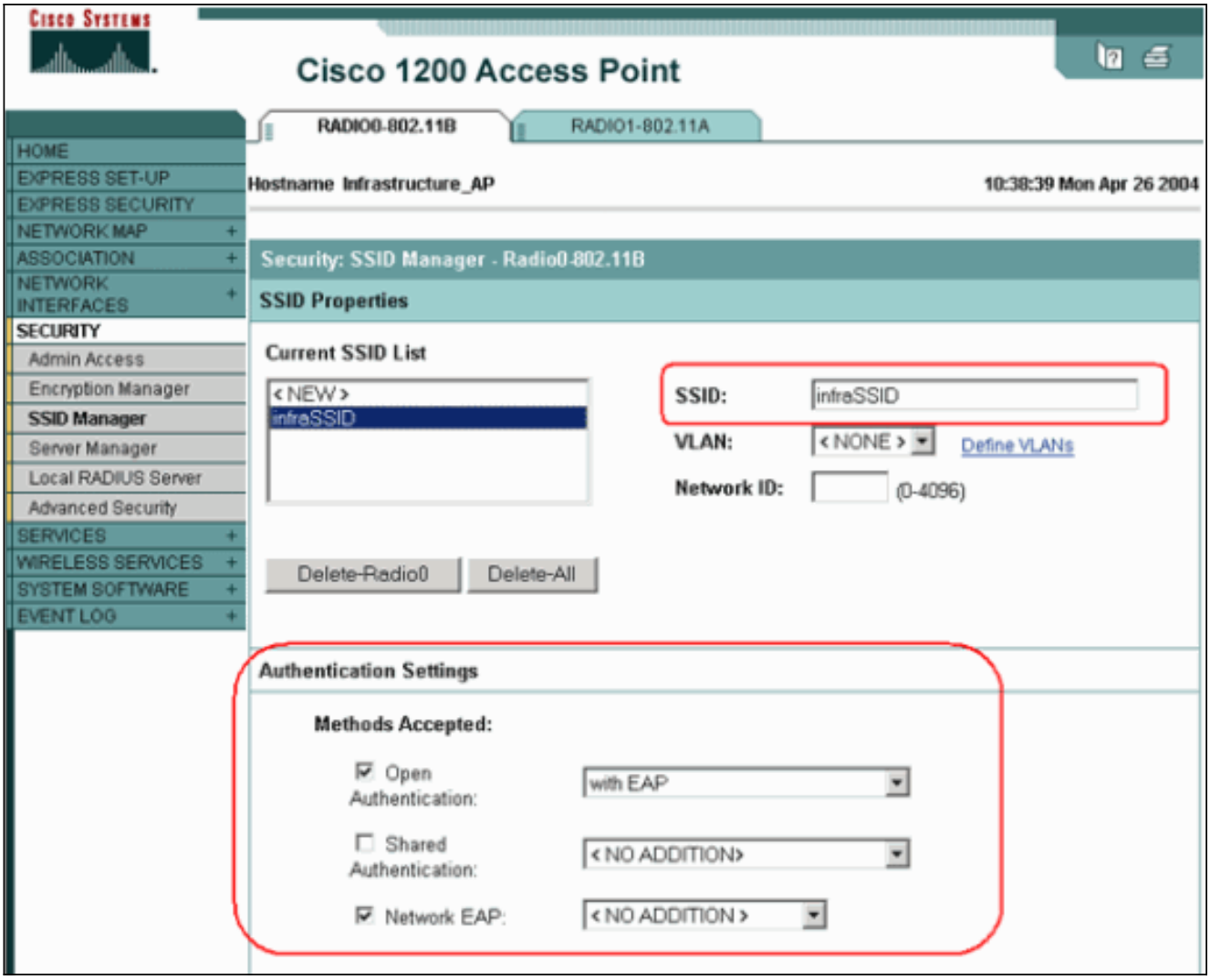


Alternativamente, ejecute estos comandos desde la CLI:**Nota:** El AP WDS de ejemplo está dedicado y no acepta asociaciones de clientes.**Nota:** No configure en los AP de infraestructura para los grupos de servidores porque los AP de infraestructura reenvían cualquier solicitud al WDS para ser procesados.

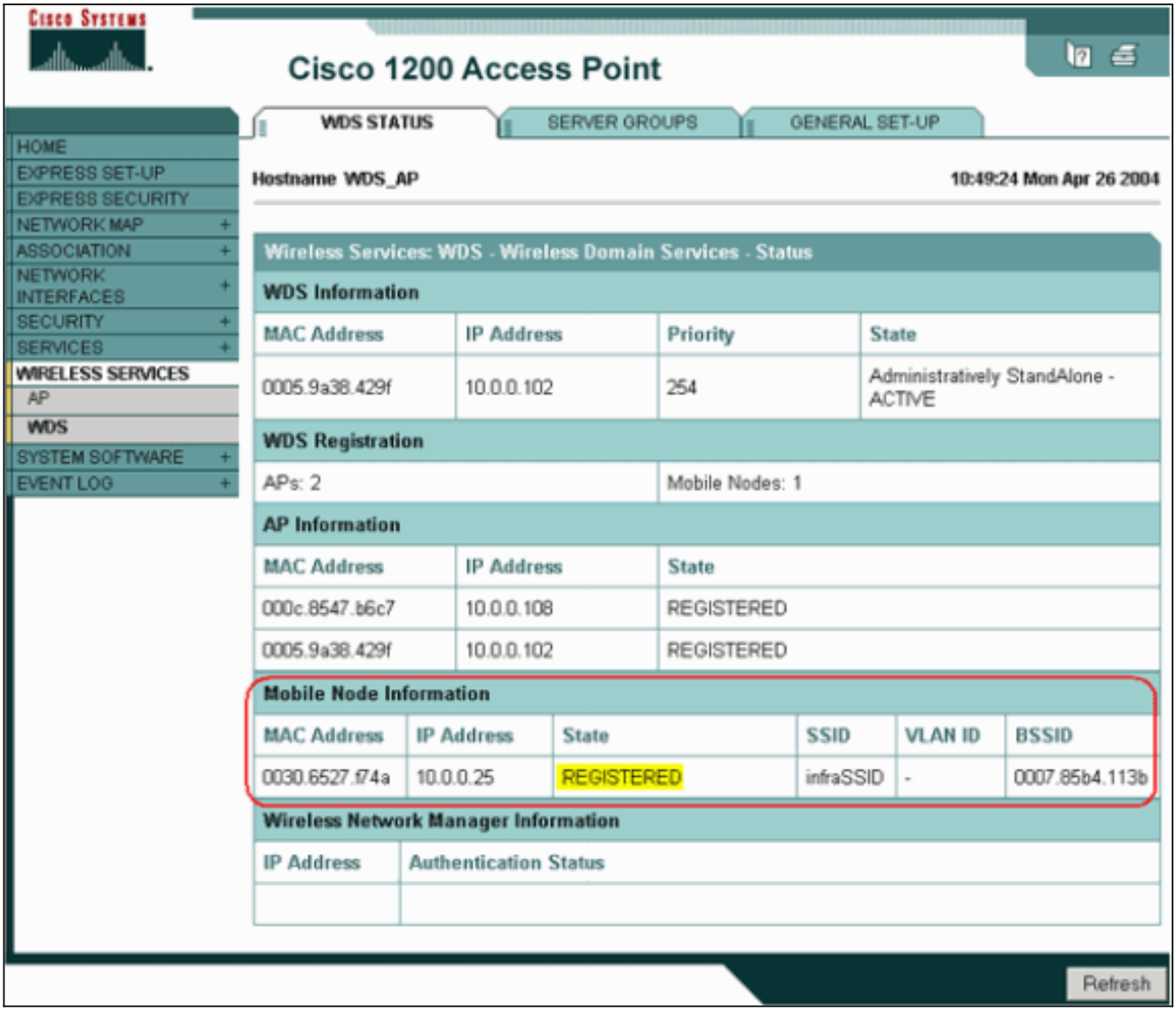
2. En los AP o AP de infraestructura:En el elemento de menú **Security > Encryption Manager, haga clic en WEP Encryption** o en **Cipher**, según lo requiera el protocolo de autenticación que
utilice.



En el elemento de menú **Security > SSID Manager**, seleccione los métodos de autenticación según lo requiera el protocolo de autenticación que utilice.



3. Ahora puede probar con éxito si los clientes se autentican en AP de infraestructura. El AP del WDS en la pestaña WDS Status (Estado de WDS) (en el elemento de menú **Wireless Services > WDS**) indica que el cliente aparece en el área Mobile Node Information (Información del nodo móvil) y tiene un estado REGISTRADO.Si el cliente no aparece, verifique que el servidor de autenticación tenga errores o intentos fallidos de autenticación por parte de los
clientes.



Alternativamente, ejecute estos comandos desde la CLI:**Nota:** Si necesita depurar la autenticación, asegúrese de depurar en el WDS AP, porque el WDS AP es el dispositivo que se comunica con el servidor de autenticación.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de la configuración. Esta lista muestra algunas de las preguntas comunes relacionadas con el comando WDS para aclarar más la utilidad de estos comandos:

- **Pregunta: En WDS AP, ¿cuáles son las configuraciones recomendadas para estos elementos?radius-server timeoutradius-server deadtimeTiempo de espera de fallo de la comprobación de integridad del mensaje (MIC) del protocolo de integridad de clave temporal (TKIP)Tiempo de espera del clienteEAP o intervalo de reautenticación MACTiempo de espera del cliente EAP (opcional)Respuesta:** Se sugiere que mantenga la configuración con la configuración predeterminada con respecto a estas configuraciones especiales y que sólo las

utilice cuando haya un problema con la temporización.Estos son los ajustes recomendados para el AP WDS:Inhabilite el **tiempo de espera del servidor radius**. Este es el número de segundos que un AP espera una respuesta a una solicitud RADIUS antes de que reenvíe la solicitud. El valor predeterminado es 5 segundos.Inhabilite **radius-server deadtime**. El RADIUS es omitido por solicitudes adicionales durante minutos a menos que todos los servidores estén marcados como muertos.El tiempo de espera de fallo de TKIP MIC se habilita de forma predeterminada en 60 segundos. Si activa el tiempo de espera, puede introducir el intervalo en segundos. Si el AP detecta dos fallas de MIC en 60 segundos, bloquea todos los clientes TKIP en esa interfaz durante el período de tiempo de espera especificado aquí.El tiempo de espera del cliente se debe inhabilitar de forma predeterminada. Si habilita el holdoff, ingrese el número de segundos que el AP debe esperar después de una falla de autenticación antes de que se procese una solicitud de autenticación subsiguiente.EAP o el intervalo de reautenticación MAC están desactivados de forma predeterminada. Si habilita la reautenticación, puede especificar el intervalo o aceptar el intervalo proporcionado por el servidor de autenticación. Si decide especificar el intervalo, introduzca el intervalo en segundos que espera el AP antes de obligar a un cliente autenticado a volver a autenticarse.El tiempo de espera del cliente EAP (opcional) es de 120 segundos de forma predeterminada. Introduzca la cantidad de tiempo que el AP debe esperar a que los clientes inalámbricos respondan a las solicitudes de autenticación EAP.

- **Pregunta: En cuanto al tiempo de espera de TKIP, leí que esto debería establecerse en 100 ms y no en 60 segundos. Asumo que está configurado en un segundo del navegador porque es el número más bajo que puede seleccionar?Respuesta:** No hay ninguna recomendación específica para establecerlo en 100 ms a menos que se informe de una falla donde la única solución es aumentar esta vez. Un segundo es la configuración más baja.
- **Pregunta: ¿Estos dos comandos ayudan a la autenticación del cliente de alguna manera y son necesarios en WDS o AP de infraestructura?radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multipleRespuesta:** Estos comandos no ayudan al proceso de autenticación y no son necesarios en el WDS o el AP.
- **Pregunta: En el AP de infraestructura, supongo que no se necesita ninguna de las configuraciones del Administrador del servidor y de las Propiedades globales porque el AP recibe información del WDS. ¿Se necesita alguno de estos comandos específicos para el AP de infraestructura?radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multipleradius-server timeoutradius-server deadtimeRespuesta:** No es necesario tener Server Manager y Global Properties para los AP de infraestructura. El WDS se encarga de esa tarea y no hay necesidad de tener estas configuraciones:**radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multipleradius-server timeoutradius-server deadtime**La configuración **del atributo radius-server 32 include-in-access-req format %h** permanece de forma predeterminada y es necesaria.

Un AP es un dispositivo de Capa 2. Por lo tanto, el AP no soporta la movilidad de Capa 3 cuando el AP se configura para actuar como un dispositivo WDS. Solo puede lograr la movilidad de Capa 3 cuando configure el WLSM como dispositivo WDS. Consulte la sección *Arquitectura de Movilidad de Capa 3* del Módulo de Servicios LAN Inalámbricos Cisco Catalyst 6500 Series: Informe técnico para obtener más información.

Por lo tanto, cuando configura un AP como dispositivo WDS, no utilice el comando **mobility network-id**. Este comando se aplica a la movilidad de Capa 3 y necesita tener un WLSM como dispositivo WDS para configurar correctamente la movilidad de Capa 3. Si utiliza el comando **mobility network-id** incorrectamente, puede ver algunos de estos síntomas:

- Los clientes de red inalámbrica no pueden asociarse al AP.
- Los clientes inalámbricos pueden asociarse al AP, pero no reciben una dirección IP del servidor DHCP.
- Un teléfono inalámbrico no se autentica cuando tiene una implementación de voz sobre WLAN.
- La autenticación EAP no se produce. Con el **ID de red de movilidad** configurado, el AP intenta construir un túnel GRE (Generic Routing Encapsulation) para reenviar paquetes EAP. Si no se establece ningún túnel, los paquetes no van a ninguna parte.
- Un AP configurado como dispositivo WDS no funciona como se espera y la configuración WDS no funciona.**Nota:** No puede configurar el Cisco Aironet 1300 AP/Bridge como un maestro WDS. El 1300 AP/Bridge no soporta esta funcionalidad. El 1300 AP/Bridge puede participar en una red WDS como un dispositivo de infraestructura en el cual algún otro AP o WLSM se configura como un maestro WDS.

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 Debug antes de utilizar los comandos **debug**.

- **debug dot11 aaa authenticator all**: muestra las diversas negociaciones que atraviesa un cliente mientras éste se asocia y autentica a través del proceso 802.1x o EAP. Esta depuración se introdujo en la versión 12.2(15)JA del software Cisco IOS. Este comando toma obsoleto el comando debug dot11 aaa dot1x en esa versión y en las posteriores.
- **debug aaa authentication**: muestra el proceso de autenticación desde una perspectiva AAA genérica.
- **debug wlccp ap**—Muestra las negociaciones WLCCP involucradas cuando un AP se une a un WDS.
- **debug wlccp packet**: muestra la información detallada sobre las negociaciones de WLCCP.
- **debug wlccp leap-client**: muestra los detalles a medida que un dispositivo de infraestructura se une a un WDS.

Información Relacionada

- Configuración de WDS, Fast Secure Roaming y Administración de Radio
- Nota de Configuración del Módulo de Servicios LAN Inalámbricos Catalyst 6500 Series
- Configuración de conjuntos Cipher y WEP
- Configuración de los tipos de autenticación
- Páginas de soporte de LAN inalámbrica
- Soporte Técnico y Documentación - Cisco Systems