Ejemplo de Configuración de RSA SecurID Ready with Wireless LAN Controllers y Cisco Secure ACS

Contenido

Introducción

Este documento explica cómo configurar y configurar los controladores de LAN inalámbrica (WLC) y los puntos de acceso ligeros (LWAPP) de Cisco, así como Cisco Secure Access Control Server (ACS) para que se utilicen en un entorno WLAN autenticado RSA SecurID. Las guías de implementación específicas de SecurID de RSA se pueden encontrar en www.rsasecured.com.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de los WLC y cómo configurar los parámetros básicos del WLC.
- Conocimientos sobre cómo configurar el perfil de Cisco Wireless Client mediante Aironet Desktop Utility (ADU).
- Conocimientos funcionales de Cisco Secure ACS.

- Tener conocimientos básicos del LWAPP.
- Conozca los servicios de Microsoft Windows Active Directory (AD), así como los conceptos de controlador de dominio y DNS.**Nota:** Antes de intentar esta configuración, asegúrese de que el ACS y el servidor RSA Authentication Manager estén en el mismo dominio y que el reloj del sistema esté exactamente sincronizado. Si utiliza Microsoft Windows AD Services, consulte la documentación de Microsoft para configurar el servidor ACS y RSA Manager en el mismo dominio. Refiérase a Configurar Active Directory y la Base de Datos de Usuarios de Windows para obtener información relevante.

Componentes Utilizados

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

- RSA Authentication Manager 6.1
- Agente de autenticación RSA 6.1 para Microsoft Windows
- Cisco Secure ACS 4.0(1), versión 27**Nota:** El servidor RADIUS que se incluye se puede utilizar en lugar del Cisco ACS. Consulte la documentación RADIUS que se incluyó con el administrador de autenticación RSA sobre cómo configurar el servidor.
- WLC de Cisco y Lightweight Access Points para la versión 4.0 (versión 4.0.155.0)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Antecedentes

El sistema RSA SecurID es una solución de autenticación de usuario de dos factores. Utilizado junto con RSA Authentication Manager y un RSA Authentication Agent, el autenticador RSA SecurID requiere que los usuarios se identifiquen usando un mecanismo de autenticación de dos factores.

Uno es el código RSA SecurID, un número aleatorio generado cada 60 segundos en el dispositivo autenticador RSA SecureID. El otro es el número de identificación personal (PIN).

Los autenticadores RSA SecurID son tan simples de usar como ingresar una contraseña. A cada usuario final se le asigna un autenticador RSA SecurID que genera un código de uso único. Al iniciar sesión, el usuario simplemente introduce este número y un PIN secreto para autenticarse correctamente. Como ventaja adicional, los tokens de hardware RSA SecurID suelen estar preprogramados para funcionar completamente al recibirlos.

Esta demostración flash explica cómo utilizar un dispositivo de autenticación RSA secureID: Demostración RSA.

A través del programa RSA SecurID Ready, los Cisco WLC y los servidores Cisco Secure ACS

soportan la autenticación RSA SecurID inmediatamente. El software RSA Authentication Agent intercepta las solicitudes de acceso, ya sean locales o remotas, de los usuarios (o grupos de usuarios) y las dirige al programa RSA Authentication Manager para la autenticación.

El software RSA Authentication Manager es el componente de administración de la solución RSA SecurID. Se utiliza para verificar las solicitudes de autenticación y administrar de forma centralizada las políticas de autenticación para las redes empresariales. Funciona junto con los autenticadores RSA SecurID y el software RSA Authentication Agent.

En este documento, un servidor Cisco ACS se utiliza como agente de autenticación RSA al instalar el software del agente en él. El WLC es el servidor de acceso a la red (NAS) (cliente AAA) que a su vez reenvía las autenticaciones del cliente al ACS. El documento muestra los conceptos y la configuración mediante la autenticación de cliente de protocolo de autenticación extensible protegido (PEAP).

Para obtener información sobre la autenticación PEAP, consulte Protocolo de autenticación extensible protegido de Cisco.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

En este documento, se utilizan estas configuraciones:

- Configuración del host del agente
- Configuración del agente de autenticación

Configuración del host del agente

Uso de Cisco Secure ACS como servidor RADIUS

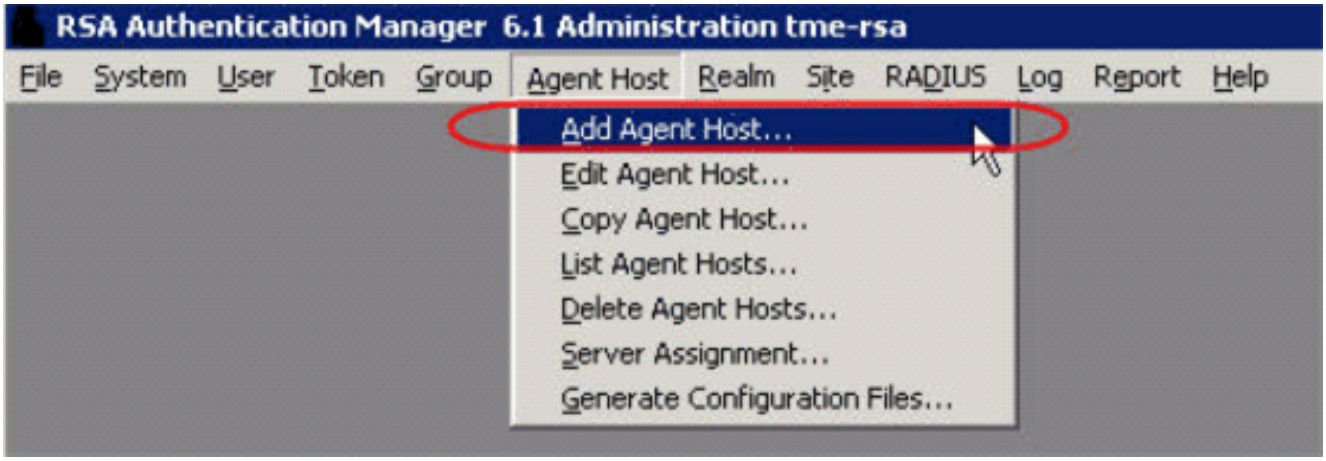
Para facilitar la comunicación entre Cisco Secure ACS y el dispositivo RSA Authentication Manager / RSA SecurID, se debe agregar un registro Agent Host a la base de datos de RSA Authentication Manager. El registro Host de agente identifica el Cisco Secure ACS dentro de su base de datos y contiene información sobre la comunicación y el cifrado.

Para crear el registro Host de agente, necesita esta información:

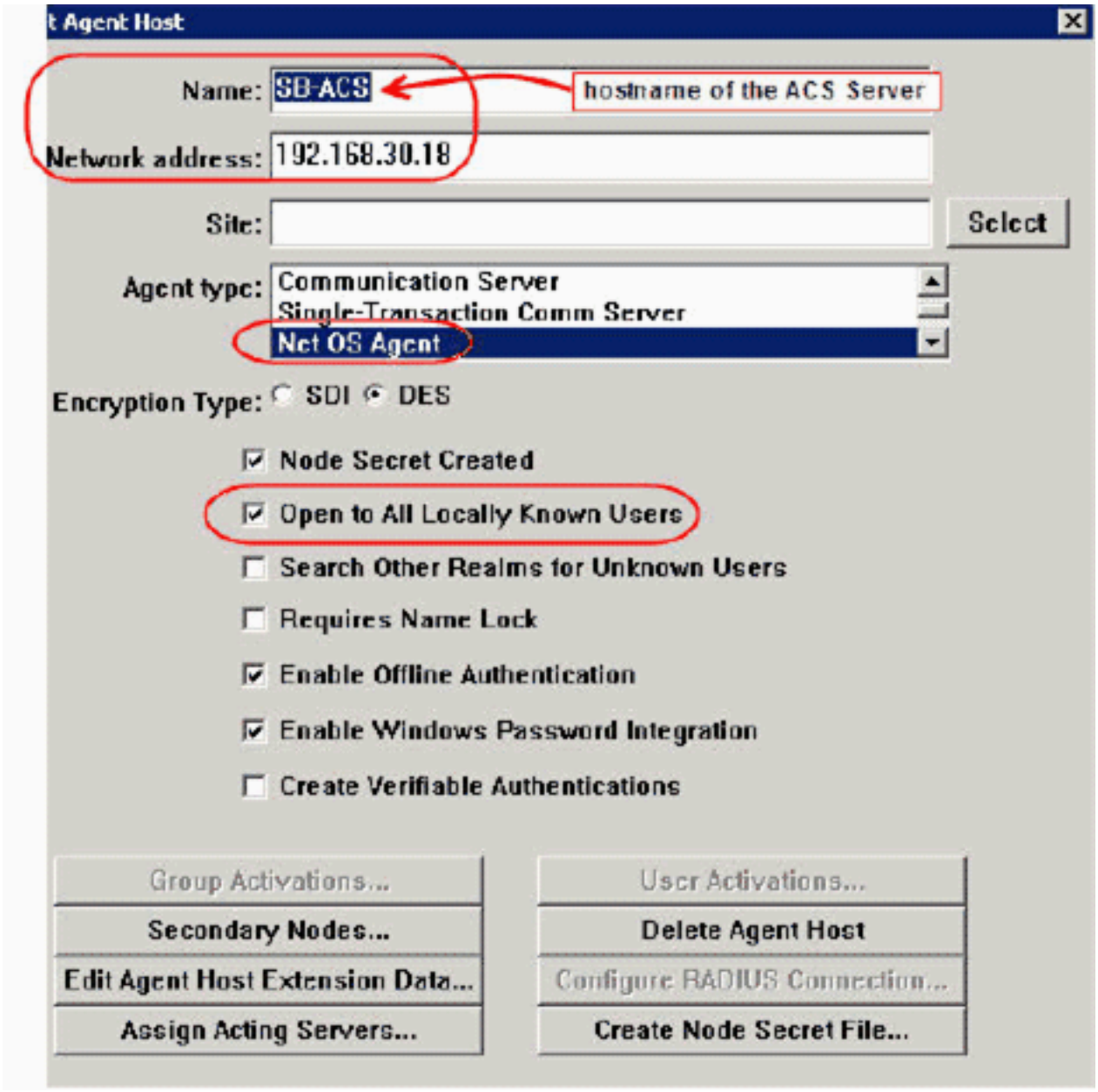
- Nombre de host del servidor Cisco ACS
- Direcciones IP para todas las interfaces de red del servidor Cisco ACS

Complete estos pasos:

1. Abra la aplicación Modo host de RSA Authentication Manager.
2. Seleccione **Host de agente > Agregar host de agente**.



Usted ve esta ventana:



3. Introduzca la información adecuada para el nombre del servidor Cisco ACS y la dirección de red. Elija **NetOS** para el tipo de agente y marque la casilla de verificación **Open to All Locally Known Users**.
4. Click OK.

Uso del servidor RADIUS RSA Authentication Manager 6.1

Para facilitar la comunicación entre el WLC de Cisco y el administrador de autenticación RSA, se debe agregar un registro de host de agente a la base de datos del administrador de autenticación RSA y a la base de datos del servidor RADIUS. El registro de host de agente identifica el WLC de Cisco dentro de su base de datos y contiene información sobre la comunicación y el cifrado.

Para crear el registro Host de agente, necesita esta información:

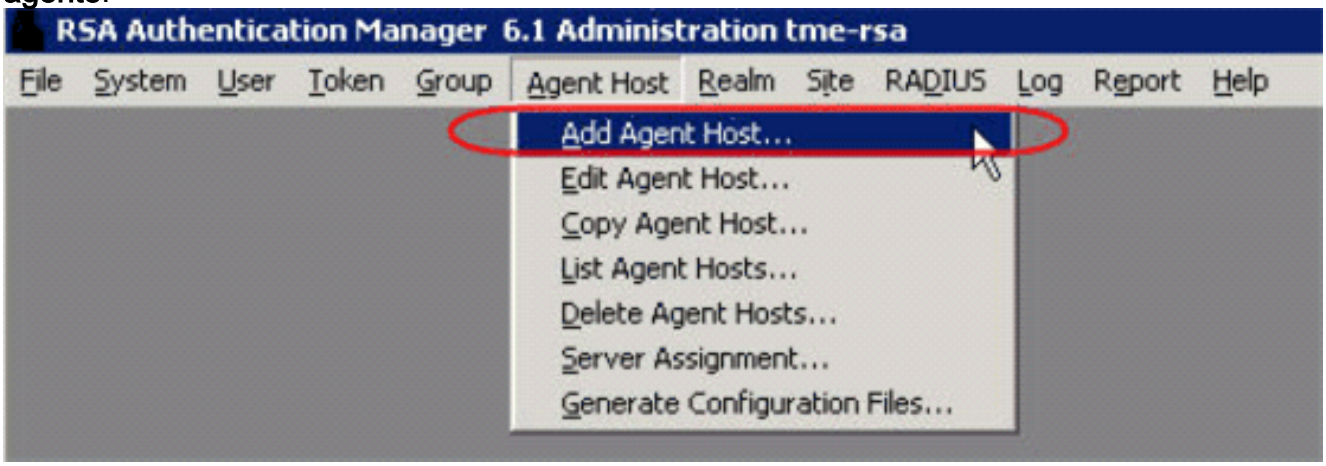
- Nombre de host del WLC
- Direcciones IP de administración del WLC
- Secreto RADIUS, que debe coincidir con el secreto RADIUS en el WLC de Cisco

Al agregar el registro de host del agente, el rol del WLC se configura como servidor de comunicación. El administrador de autenticación RSA utiliza esta configuración para determinar cómo se producirá la comunicación con el WLC.

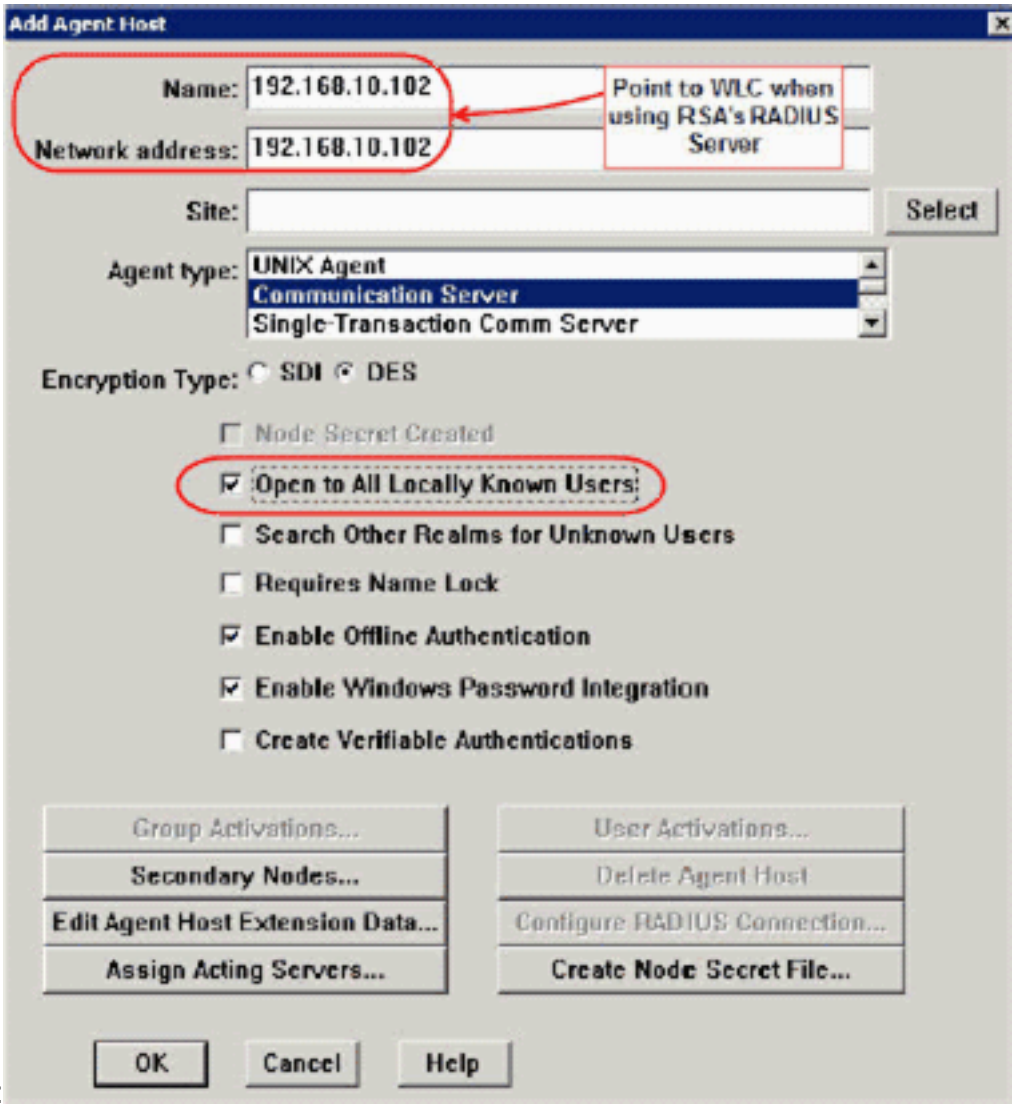
Nota: Los nombres de host dentro del dispositivo RSA Authentication Manager / RSA SecurID deben resolver a direcciones IP válidas en la red local.

Complete estos pasos:

1. Abra la aplicación Modo host de RSA Authentication Manager.
2. Seleccione **Host de agente > Agregar host de agente**.

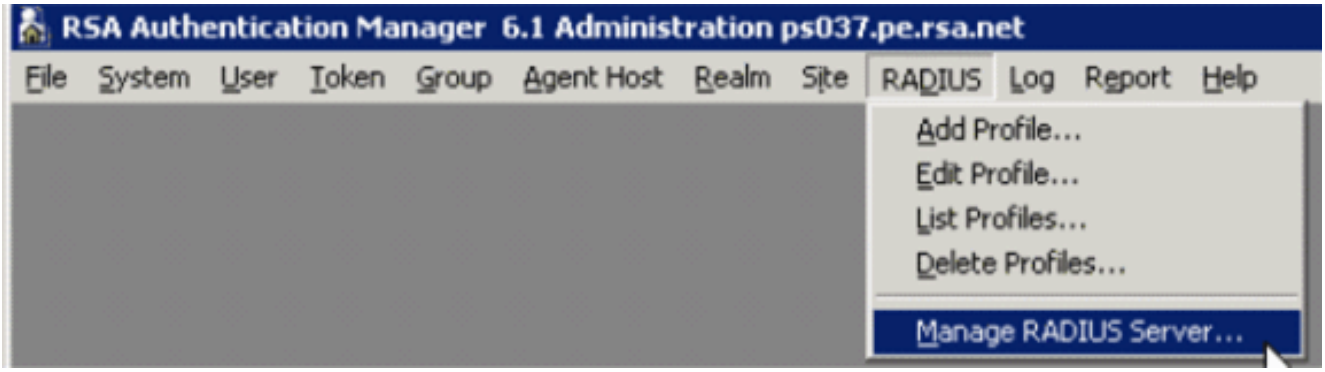


Usted ve esta



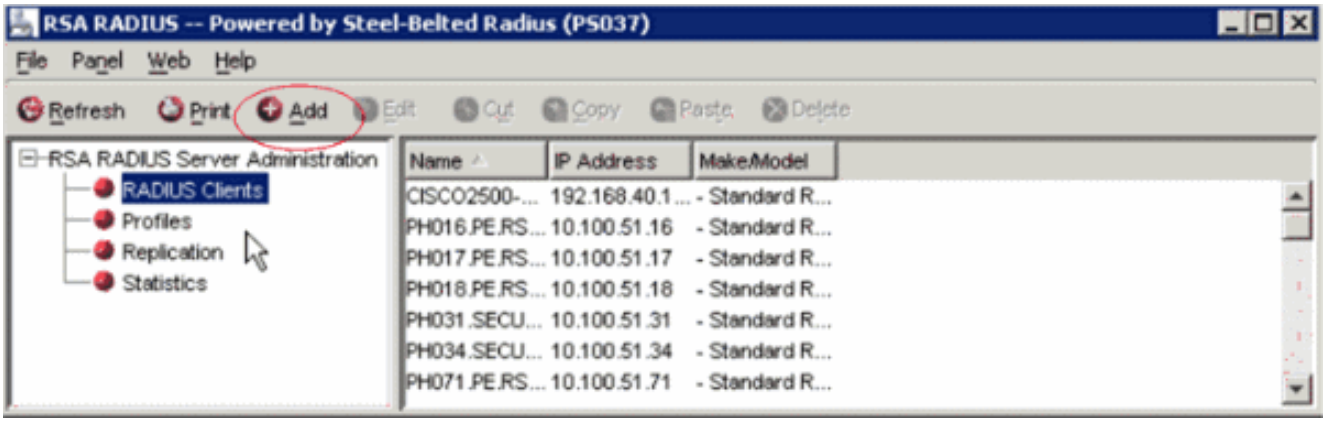
ventana:

3. Introduzca la información adecuada para el nombre de host del WLC (un FQDN resoluble, si es necesario) y la dirección de red. Elija **Communication Server** para el tipo de agente y marque la casilla de verificación **Open to All Locally Known Users**.
4. Click OK.
5. En el menú, seleccione **RADIUS > Manage RADIUS Server**.

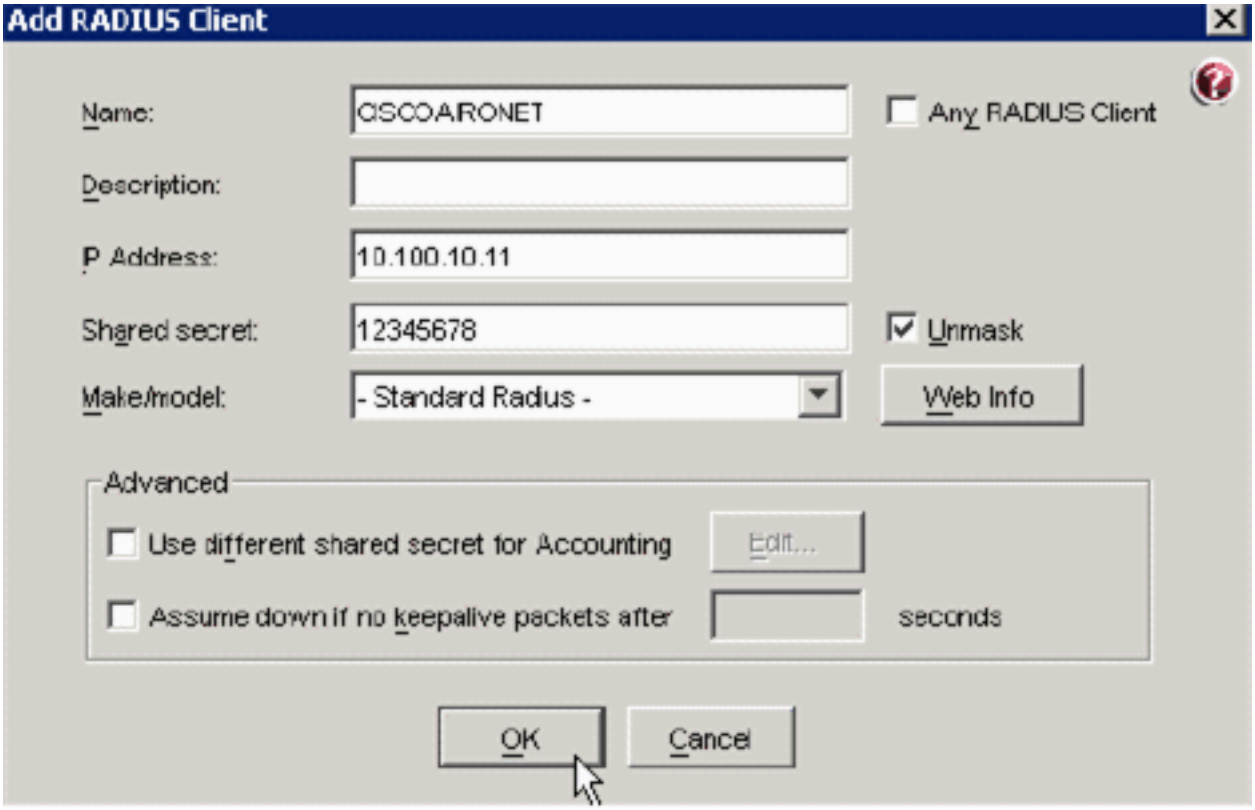


Se abre una nueva ventana de administración.

6. En esta ventana, seleccione **Clientes RADIUS** y luego haga clic en **Agregar**.



7. Introduzca la información adecuada para el WLC de Cisco. El secreto compartido debe coincidir con el secreto compartido definido en el WLC de Cisco.



8. Click OK.

Configuración del agente de autenticación

Esta tabla representa la funcionalidad del Agente de Autenticación RSA de ACS:

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication, RADIUS, Both
List Library Version Used	5.0.3
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
Location of Node Secret on Agent	'None stored'
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No

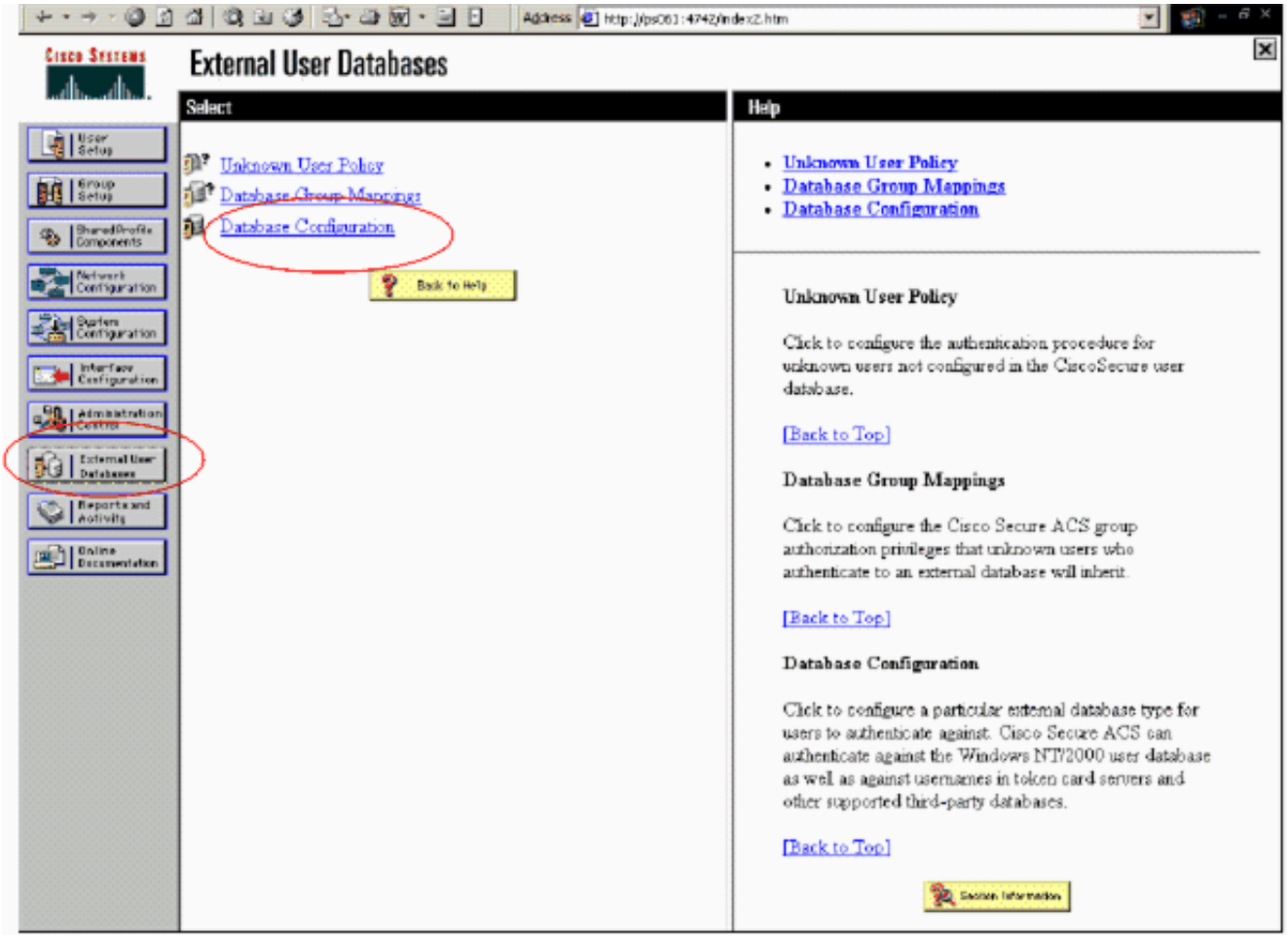
Nota: Vea la documentación RADIUS que se incluyó con el administrador de autenticación RSA sobre cómo configurar el servidor RADIUS, si ese es el servidor RADIUS que se utilizará.

Configuración de Cisco ACS

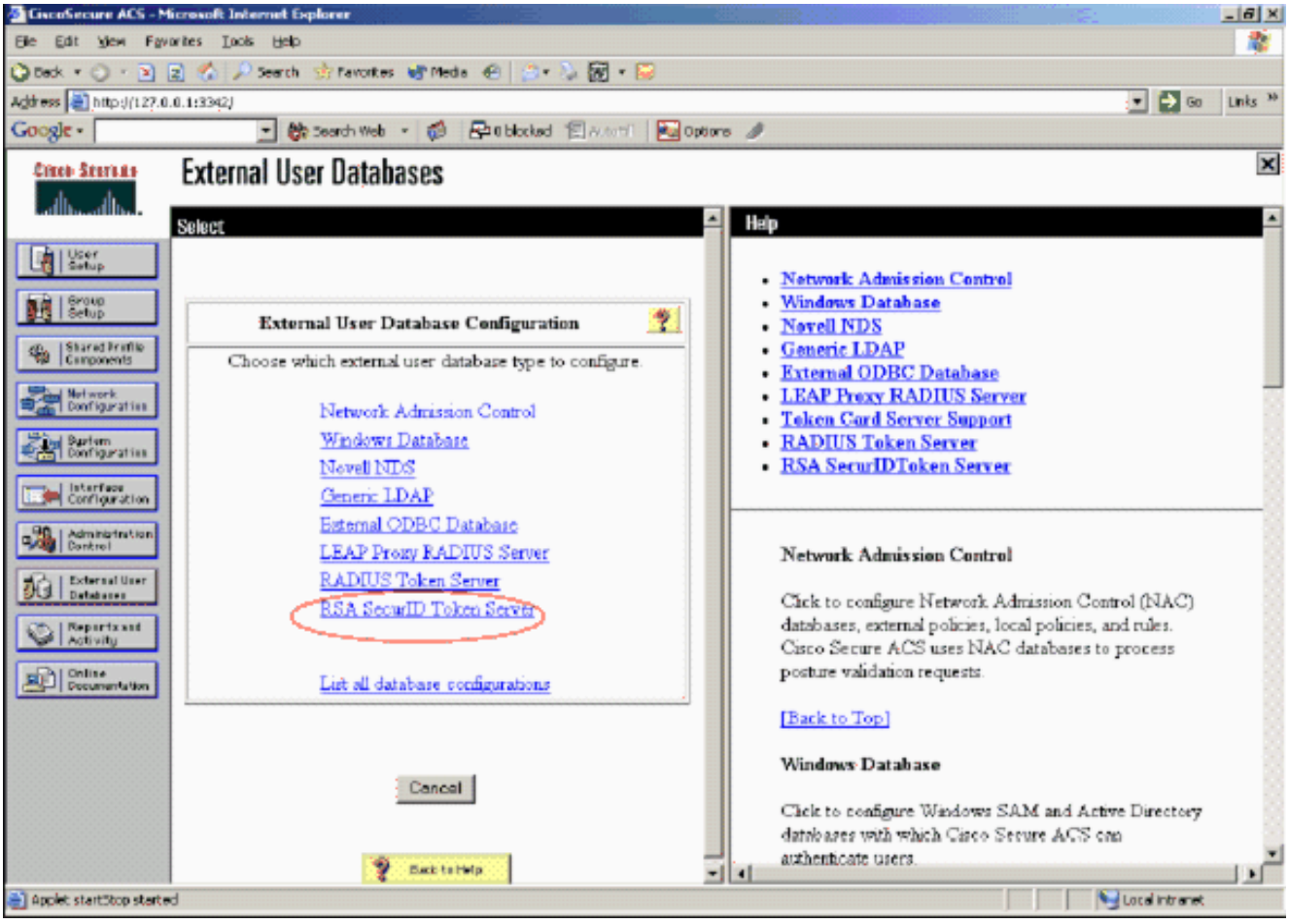
Activar autenticación RSA SecurID

Cisco Secure ACS soporta la autenticación RSA SecurID de los usuarios. Complete estos pasos para configurar Cisco Secure ACS para autenticar a los usuarios con Authentication Manager 6.1:

1. Instale RSA Authentication Agent 5.6 o posterior para Windows en el mismo sistema que el servidor Cisco Secure ACS.
2. Verifique la conectividad ejecutando la función de autenticación de prueba del agente de autenticación.
3. Copie el archivo aceclnt.dll del directorio **c:\Program Files\RSA Security\RSA Authentication Manager\prog** del servidor RSA al **directorio c:\WINNT\system32** del servidor ACS.
4. En la barra de navegación, haga clic en **Base de datos de usuario externa**. A continuación, haga clic en **Configuración de base de datos** en la página Base de datos externa.

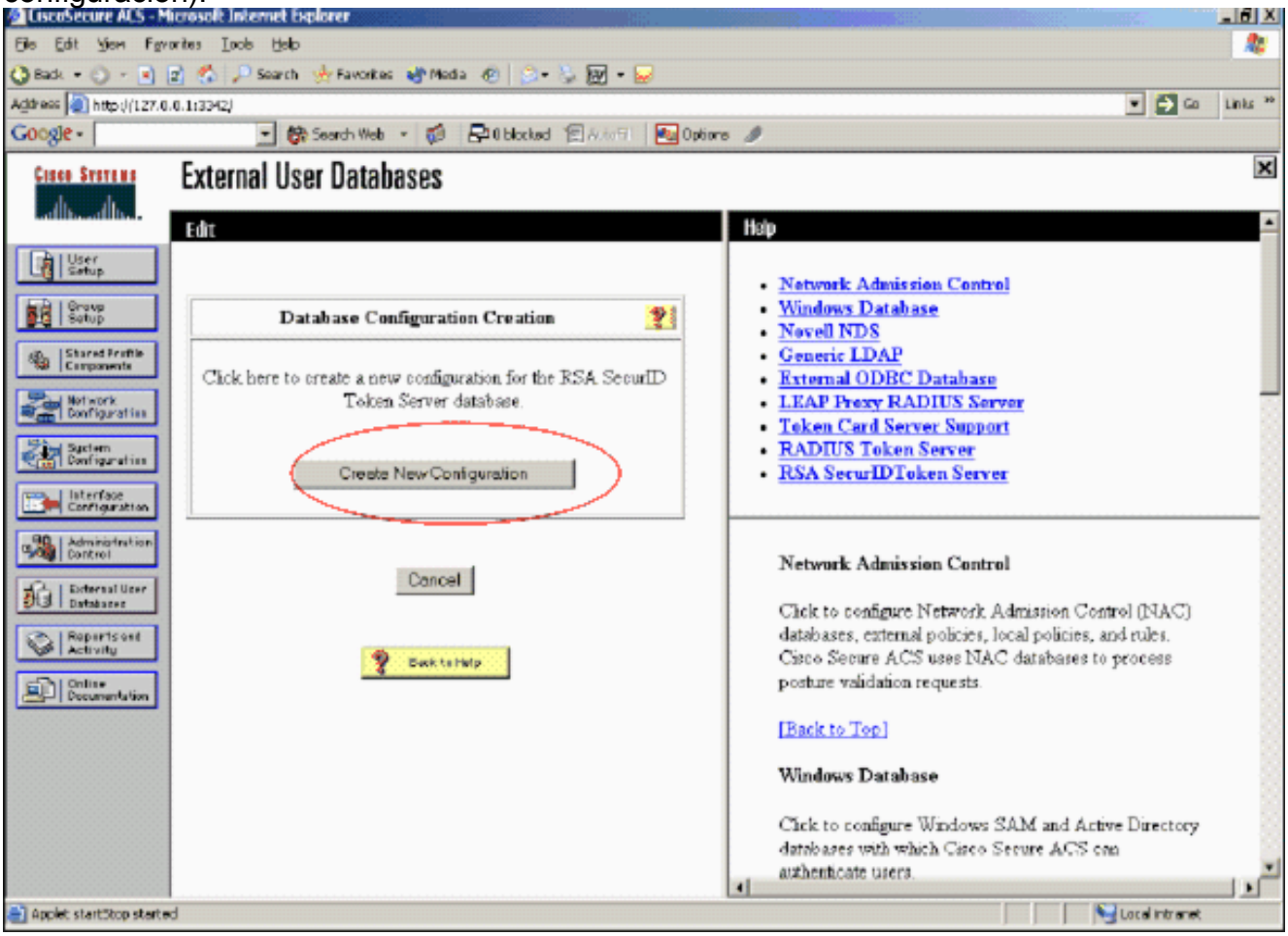


5. En la página External User Database Configuration, haga clic en **RSA SecurID Token Server**.

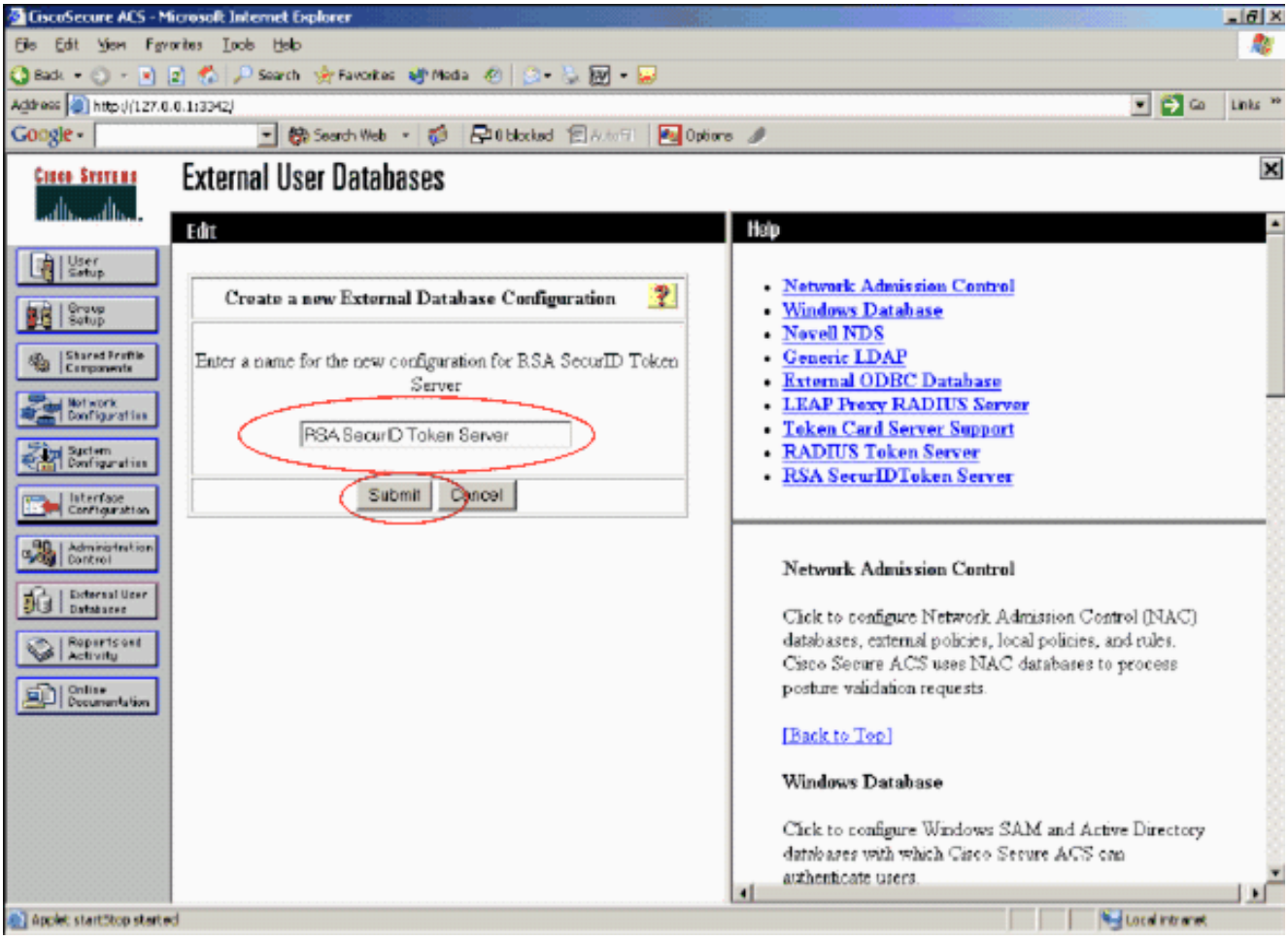


6. Haga clic en Create New Configuration (Crear nueva

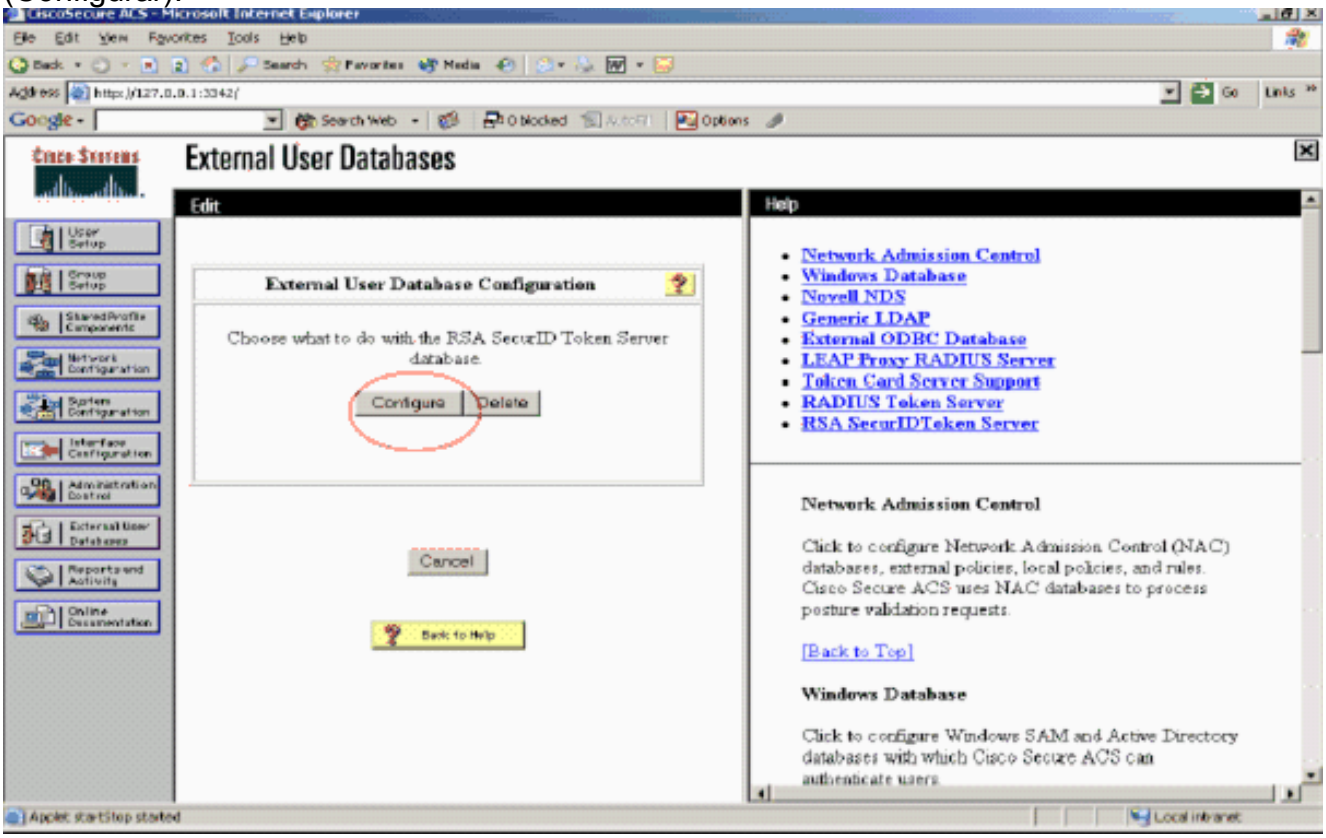
configuración).



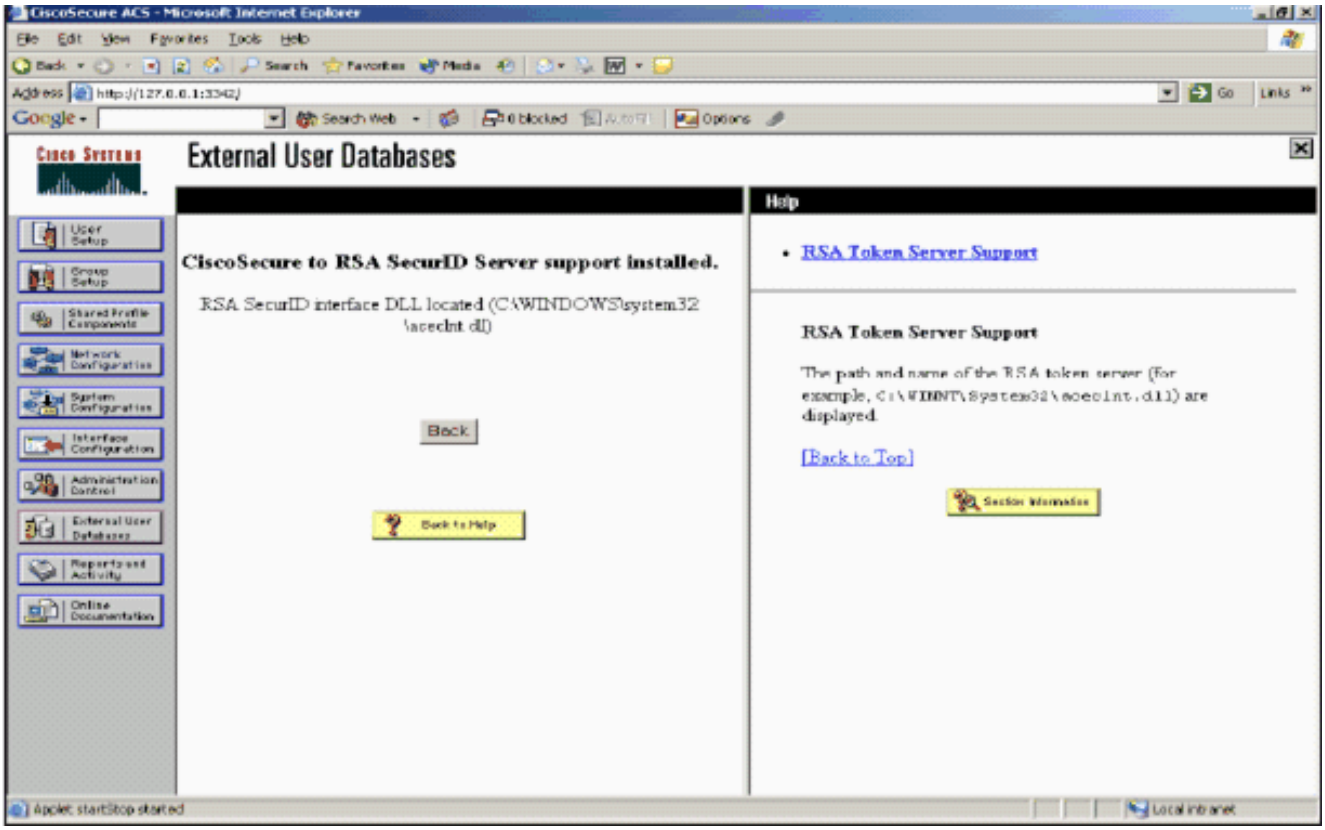
7. Introduzca un nombre y, a continuación, haga clic en **Enviar**.



8. Haga clic en Configure (Configurar).



Cisco Secure ACS muestra el nombre del servidor de token y la trayectoria al archivo DLL de autenticador. Esta información confirma que Cisco Secure ACS puede ponerse en contacto con el agente de autenticación RSA. Puede agregar la base de datos de usuarios externos RSA SecurID a su política de usuario desconocida o asignar cuentas de usuario específicas para utilizar esta base de datos para la autenticación.

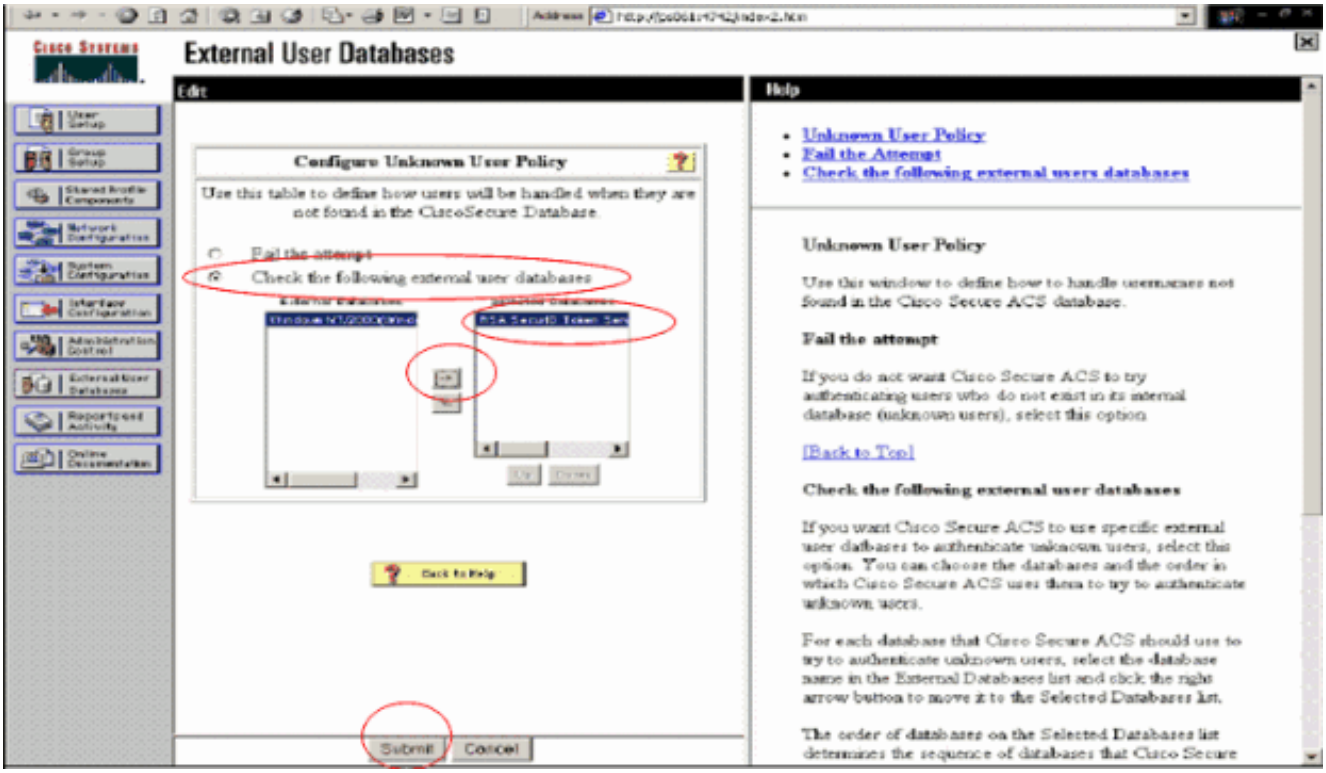


Agregar/configurar la autenticación RSA SecurID a su política de usuario desconocida

Complete estos pasos:

1. En la barra de navegación ACS, haga clic en **Base de datos de usuario externa > Política de usuario desconocida**.

2. En la página **Unknown User Policy**, seleccione **Check the following external user database**, resalte **RSA SecurID Token Server** y muévalo al cuadro Selected Datdatabase. A continuación, haga clic en **Enviar**.

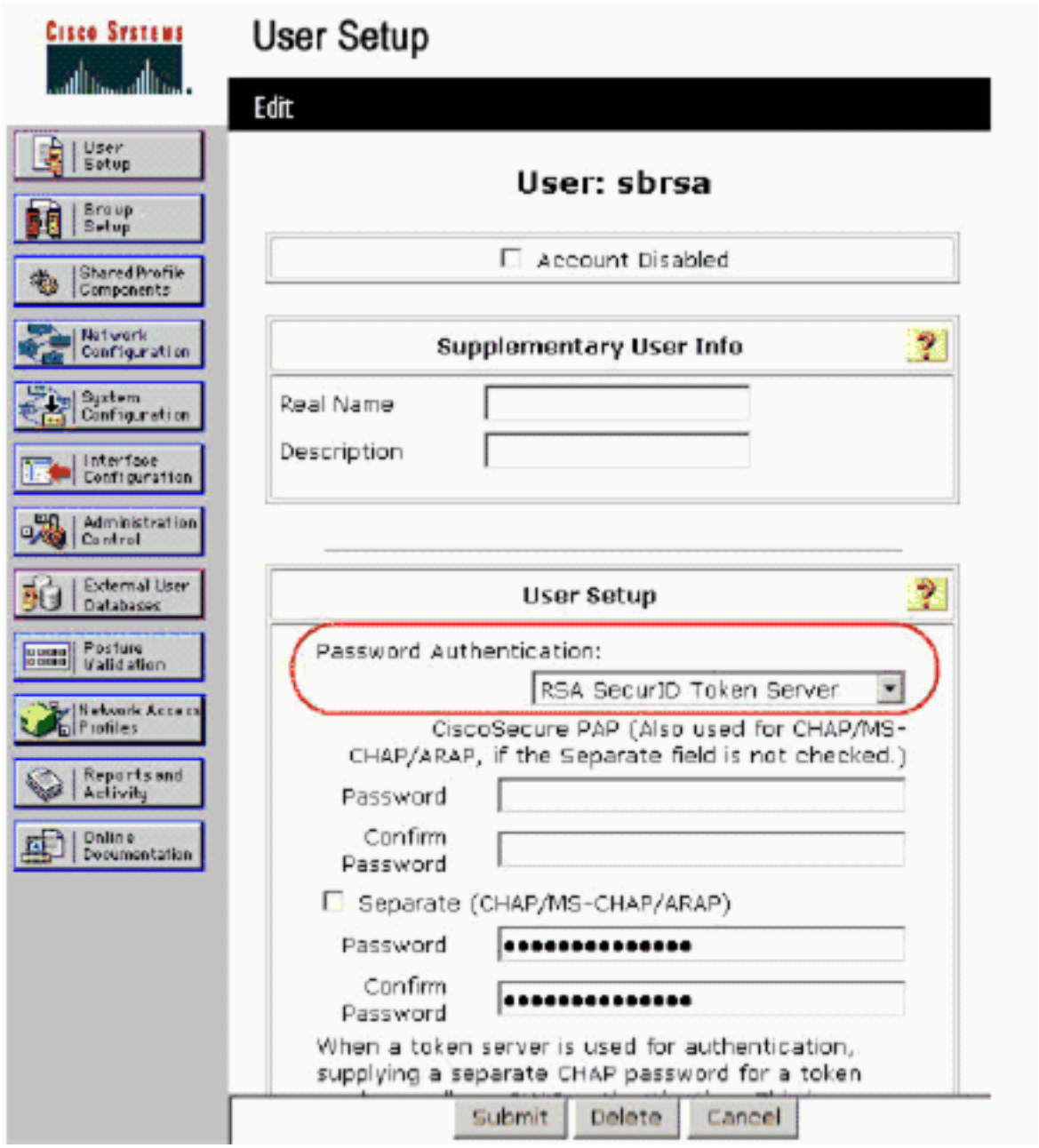


Agregar/Configurar la Autenticación RSA SecurID para Cuentas de Usuario Específicas

Complete estos pasos:

1. Haga clic en **User Setup** desde la GUI principal de ACS Admin. Ingrese el nombre de usuario y haga clic en **Agregar** (o seleccione un usuario existente que desee modificar).
2. En User Setup > Password Authentication , elija **RSA SecurID Token Server**. A continuación, haga clic en

Enviar.

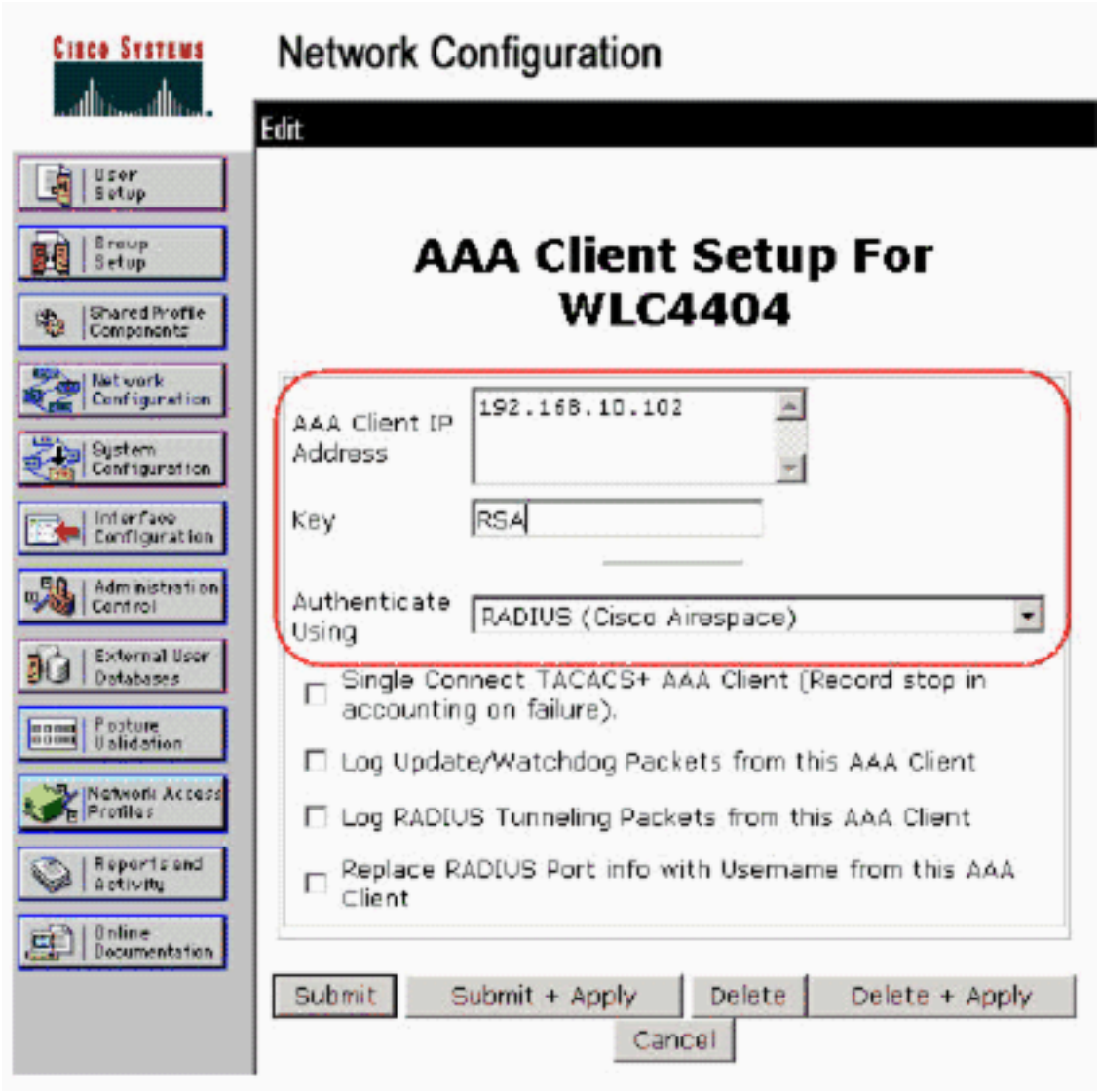


[Agregar un cliente RADIUS en Cisco ACS]

La instalación del servidor Cisco ACS necesitará las direcciones IP del WLC para funcionar como NAS para reenviar las autenticaciones PEAP del cliente al ACS.

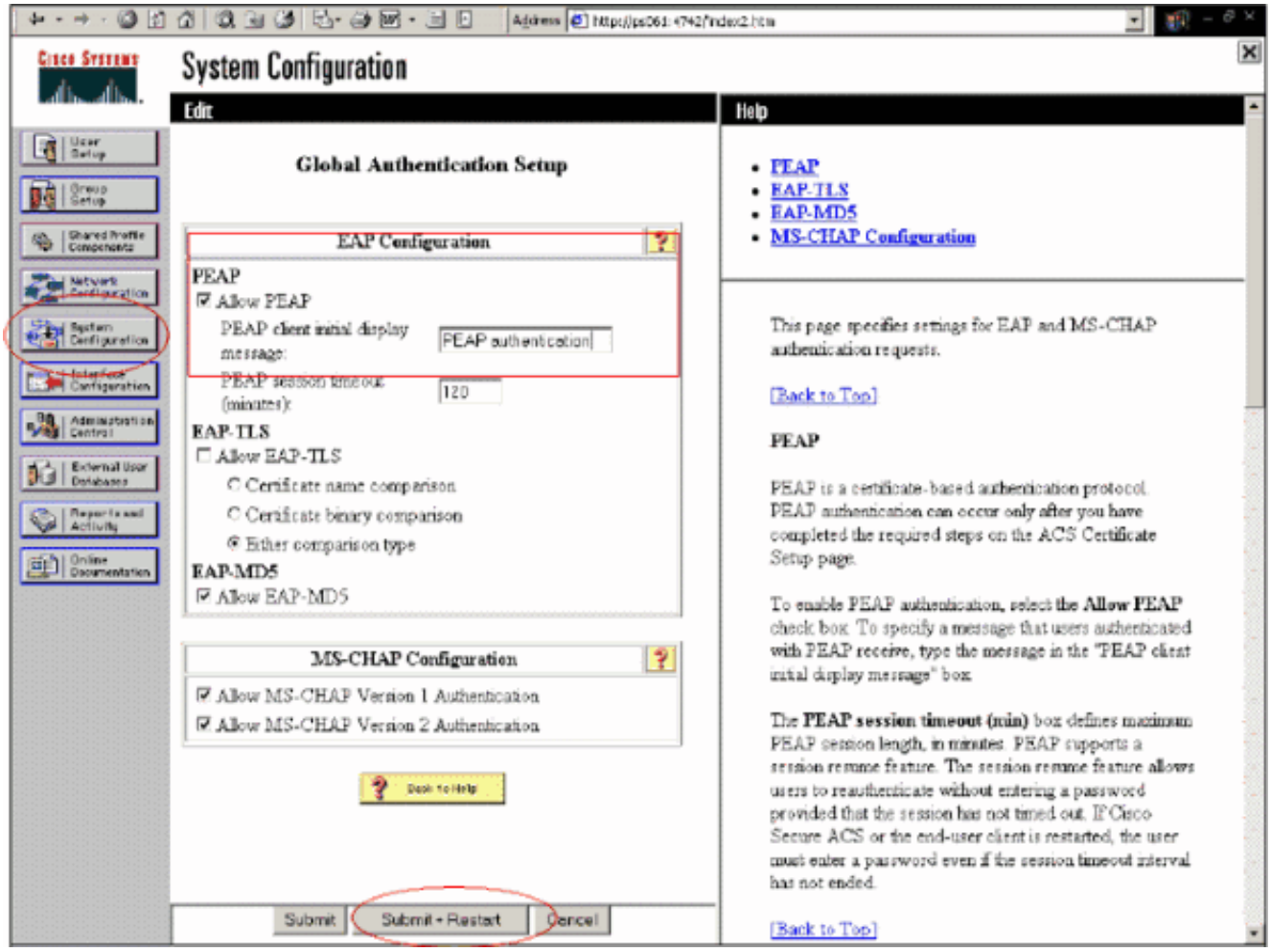
Complete estos pasos:

1. En **Configuración de Red**, agregue/edite el cliente AAA para el WLC que se utilizará. Introduzca la clave "secreto compartido" (común al WLC) que se utiliza entre el cliente AAA y ACS. Seleccione **Authenticate Using > RADIUS (Cisco Airespace)** para este cliente AAA. A continuación, haga clic en **Enviar +**



Aplicar.

2. Solicite e instale un certificado de servidor de una autoridad certificadora de confianza conocida como RSA Keon Certificate Authority.Para obtener más información sobre este proceso, consulte la documentación que se envía con Cisco ACS. Si utiliza RSA Certificate Manager, puede ver la guía de implementación de RSA Keon Aironet para obtener ayuda adicional. Debe completar esta tarea correctamente antes de continuar.**Nota:** También se pueden utilizar certificados autofirmados. Consulte la documentación de Cisco Secure ACS sobre cómo utilizarlos.
3. En **Configuración del sistema > Configuración de autenticación global**, marque la casilla de verificación **Permitir** autenticación
PEAP.



Configuración de Cisco Wireless LAN Controller para 802.1x

Complete estos pasos:

1. Conéctese a la interfaz de línea de comandos del WLC para configurar el controlador de modo que se pueda configurar para conectarse al servidor Cisco Secure ACS.
2. Ingrese el comando **config radius auth ip-address** del WLC para configurar un servidor RADIUS para la autenticación.**Nota:** Cuando realice la prueba con el servidor RADIUS de RSA Authentication Manager, ingrese la dirección IP del servidor RADIUS de RSA Authentication Manager. Cuando realice la prueba con el servidor Cisco ACS, introduzca la dirección IP del servidor Cisco Secure ACS.
3. Ingrese el comando **config radius auth port** del WLC para especificar el puerto UDP para la autenticación. Los puertos 1645 o 1812 están activos de forma predeterminada tanto en el RSA Authentication Manager como en el servidor Cisco ACS.
4. Ingrese el comando **config radius auth secret** del WLC para configurar el secreto compartido en el WLC. Esto debe coincidir con el secreto compartido creado en los servidores RADIUS para este cliente RADIUS.
5. Ingrese el comando **config radius auth enable** del WLC para habilitar la autenticación. Cuando lo desee, ingrese el comando **config radius auth disable** para inhabilitar la autenticación. Tenga en cuenta que la autenticación está desactivada de forma predeterminada.
6. Seleccione la opción de seguridad de Capa 2 adecuada para la WLAN deseada en el WLC.
7. Utilice los comandos **show radius auth statistics** y **show radius summary** para verificar que la configuración de RADIUS esté configurada correctamente.**Nota:** Los temporizadores

predeterminados para EAP Request-timeout son bajos y es posible que deban modificarse. Esto se puede hacer usando el comando **config advanced eap request-timeout** ***<seconds>.*** También podría ayudar a ajustar el tiempo de espera de la solicitud de identidad en función de los requisitos. Esto se puede hacer usando el comando **config advanced eap identity-request-timeout** ***<seconds>.***

Configuración del cliente inalámbrico 802.11

Para obtener una explicación detallada sobre cómo configurar el hardware inalámbrico y el suplicante del cliente, consulte la documentación de Cisco.

Problemas conocidos

Estos son algunos de los problemas conocidos con la autenticación RSA SecureID:

- Token de software RSA. No se admiten los modos Pin nuevo y Next Tokencode cuando se utiliza esta forma de autenticación con XP2. (FIJADO como resultado de ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip)
- Si la implementación de ACS es anterior o no tiene el parche anterior, el cliente no podrá autenticarse hasta que el usuario pase de "Activado;Nuevo modo PIN" a "Activado". Para lograrlo, el usuario debe completar una autenticación no inalámbrica o utilizar la aplicación RSA "test authentication".
- Denegar PIN de 4 dígitos/alfanuméricos. Si un usuario en modo Nuevo PIN se opone a la política PIN, el proceso de autenticación falla y el usuario no sabe cómo o por qué. Normalmente, si un usuario se opone a la política, se le enviará un mensaje en el que se indica que el PIN se ha rechazado y se le volverá a indicar al usuario que es la política de PIN (por ejemplo, si la política de PIN es de 5 a 7 dígitos, pero el usuario introduce 4 dígitos).

Información Relacionada

- Ejemplo de Configuración de Asignación de VLAN Dinámica con WLCs Basada en ACS a Asignación de Grupos de Directorios Activos
- Ejemplo de Configuración del Cliente VPN sobre LAN Inalámbrica con WLC
- Ejemplos de configuración de autenticación de controladores para redes LAN inalámbricas
- Ejemplo de Configuración de EAP-FAST Authentication with Wireless LAN Controllers and External RADIUS Server
- Ejemplo de Configuración de Tipos de Autenticación Inalámbrica en ISR Fijo a través de SDM
- Ejemplo de Configuración de Tipos de Autenticación Inalámbrica en un ISR Fijo
- Protocolo de autenticación extensible protegido de Cisco
- Autenticación del EAP con servidor RADIUS
- Soporte Técnico y Documentación - Cisco Systems