RSA SecurID listo con los reguladores inalámbricos LAN y el ejemplo seguro de la configuración de Cisco ACS

Contenido

Introducción

Este documento explica cómo poner y configurar el protocolo ligero del Punto de acceso de Cisco (LWAPP) - APs capaces y los reguladores inalámbricos LAN (WLCs), así como el Cisco Secure Access Control Server (ACS) que se utilizará en un entorno WLAN autenticado SecurID RSA. Los guías de instrumentación SecurID-específicos RSA se pueden encontrar en www.rsasecured.com.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de WLCs y cómo configurar los parámetros básicos WLC.
- Conocimiento en cómo configurar el perfil del cliente de red inalámbrica de Cisco usando utilidad Aironet Desktop (ADU).

- Tenga conocimiento funcional de Cisco ACS seguro.
- Tenga conocimiento básico de LWAPP.
- Tenga la comprensión básica de los servicios del Active Directory de Microsoft Windows (ANUNCIO), así como el regulador del dominio y conceptos DNS.**Nota:** Antes de que usted intente esta configuración, asegúrese de que los ACS y el servidor de administración de la Autenticación RSA estén en el mismo dominio y su reloj del sistema está sincronizado exactamente. Si usted está utilizando los servicios del ANUNCIO de Microsoft Windows, refiera a la documentación de Microsoft para configurar al servidor de administración ACS y RSA en el mismo dominio. Refiérase configuran la base de datos del Active Directory y de usuario de Windows para la información pertinente.

Componentes Utilizados

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

- Encargado 6.1 de la Autenticación RSA
- Agente 6.1 de la Autenticación RSA para Microsoft Windows
- Estructura segura 27 de Cisco ACS 4.0(1)**Nota:** El servidor de RADIUS que es incluido puede ser utilizado en lugar de Cisco ACS. Vea la documentación RADIUS que fue incluida con el encargado de la Autenticación RSA en cómo configurar el servidor.
- Cisco WLCs y Puntos de acceso ligeros para la versión 4.0 (versión 4.0.155.0)

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 de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

El sistema RSA SecurID es una solución bifactorial de la autenticación de usuario. Utilizado conjuntamente con el encargado de la Autenticación RSA y un agente de la Autenticación RSA, el authenticator RSA SecurID requiere a los usuarios identificarse usando un mecanismo de autenticación bifactorial.

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

Los authenticators RSA SecurID son tan simples utilizar como ingresar una contraseña. Asignan cada usuario final un authenticator RSA SecurID que genera un código del uno-tiempo-uso. Al abrir una sesión, el usuario ingresa simplemente este número y un PIN del secreto que se autenticará con éxito. Como una ventaja agregada, los tokens de la dotación física RSA SecurID se preprograma generalmente para estar completamente - funcional sobre el recibo.

Esta demostración de destello explica cómo utilizar un dispositivo del authenticator del secureID

RSA: Versión parcial de programa RSA.

Con el programa listo RSA SecurID, Cisco WLCs y Cisco aseguran la derecha de la autenticación de SecurID de la ayuda RSA de los servidores ACS fuera del cuadro. El software del agente de la Autenticación RSA intercepta las peticiones del acceso, si local o telecontrol, de los usuarios (o de los grupos de usuarios) y los dirige al programa del encargado de la Autenticación RSA para la autenticación.

El software de administrador de la Autenticación RSA es el componente de administración de la solución RSA SecurID. Se utiliza para verificar las peticiones de la autenticación y centralmente para administrar las políticas de autenticación para las redes de empresas. Trabaja conjuntamente con los authenticators RSA SecurID y el software del agente de la Autenticación RSA.

En este documento, instalando utiliza a un servidor ACS de Cisco como el agente de la Autenticación RSA el software del agente en él. El WLC es el servidor del acceso a la red (NAS) (cliente AAA) que a su vez adelante las autenticaciones de cliente al ACS. El documento demuestra los conceptos y la disposición usando la autenticación de cliente protegida del protocolo extensible authentication (PEAP).

Para aprender sobre la autenticación PEAP, refiera al protocolo extensible authentication protegido Cisco.

Configurar

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

Este documento utiliza estas configuraciones:

- Configuración del host agente
- Configuración de agente de autenticación

Configuración del host agente

Usando Cisco asegure ACS como el servidor de RADIUS

Para facilitar la comunicación entre Cisco ACS seguro y el dispositivo del encargado/RSA SecurID de la Autenticación RSA, un expediente del host agente se debe agregar a la base de datos del administrador de la Autenticación RSA. El expediente del host agente identifica Cisco ACS seguro dentro de su base de datos y contiene la información sobre la comunicación y el cifrado.

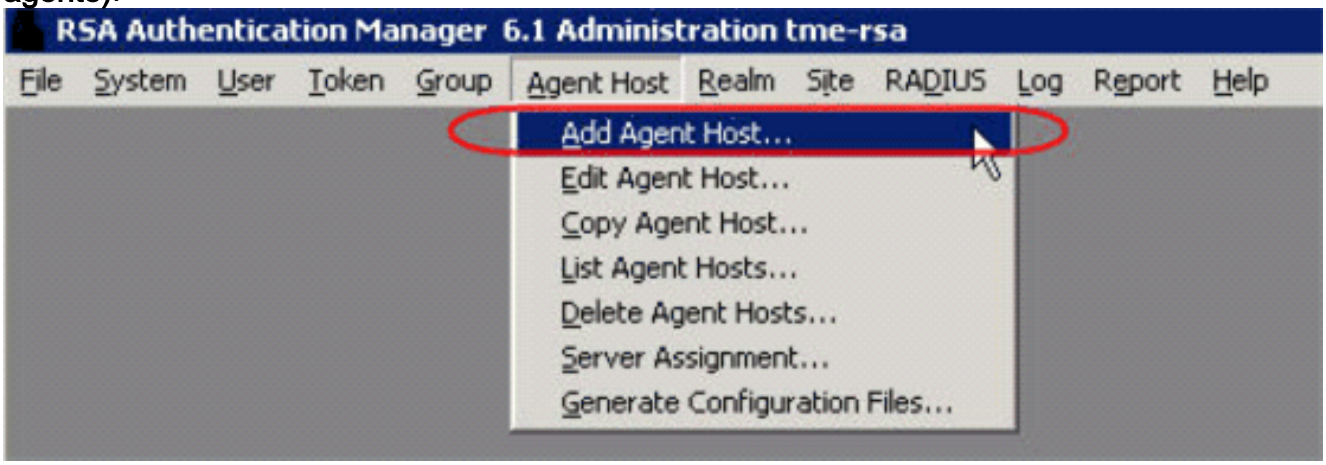
Para crear el expediente del host agente, usted necesita esta información:

- Hostname del servidor ACS de Cisco
- IP Addresses para todos los interfaces de red del servidor ACS de Cisco

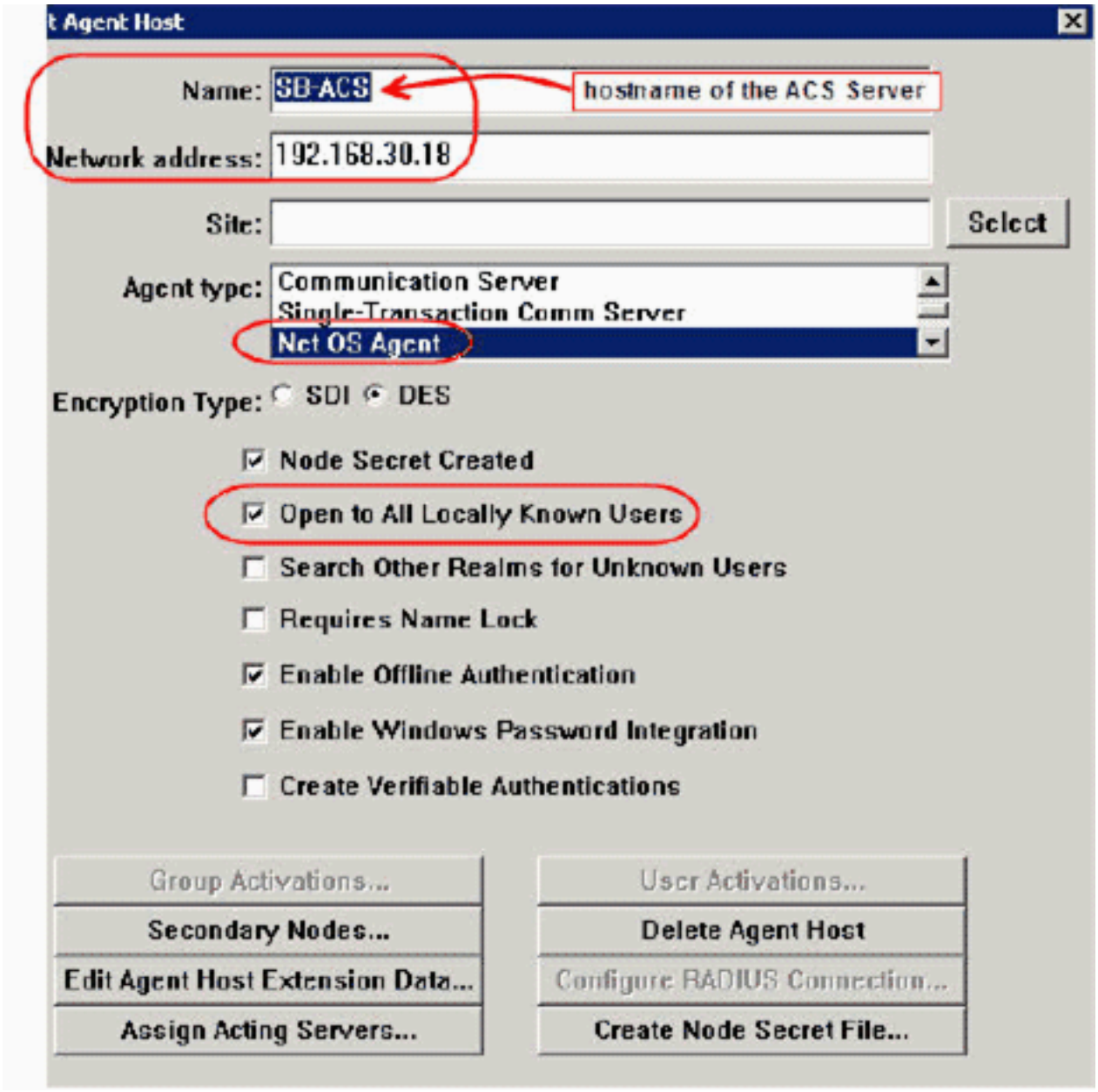
Complete estos pasos:

1. Abra la aplicación del modo del host del encargado de la Autenticación RSA.

2. Seleccione el **Agent Host (Host agente) > Add Agent Host (Agregar host agente)**.



Usted ve esta ventana:



3. Ingrese la información apropiada para el nombre y la dirección de red del servidor ACS de Cisco. Elija **NetOS** para el tipo del agente y controle el checkbox para saber si hay **Open en todos los usuarios localmente conocidos**.
4. Click OK.

Usando el servidor de RADIUS del encargado 6.1 de la Autenticación RSA

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

Para crear el expediente del host agente, usted necesita esta información:

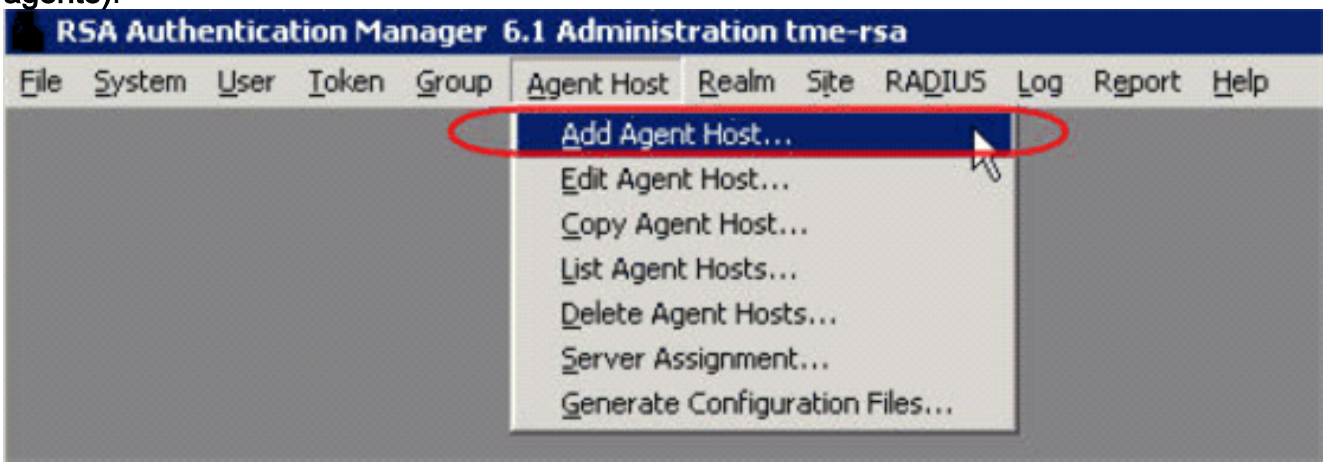
- El hostname WLC
- IP Addresses de la Administración del WLC
- Secreto RADIUS, que debe hacer juego el secreto RADIUS en Cisco WLC

Al agregar el expediente del host agente, el papel WLC se configura como a Communication Server (Servidor de comunicación). Esta configuración es utilizada por el encargado de la Autenticación RSA para determinar cómo ocurrirá la comunicación con el WLC.

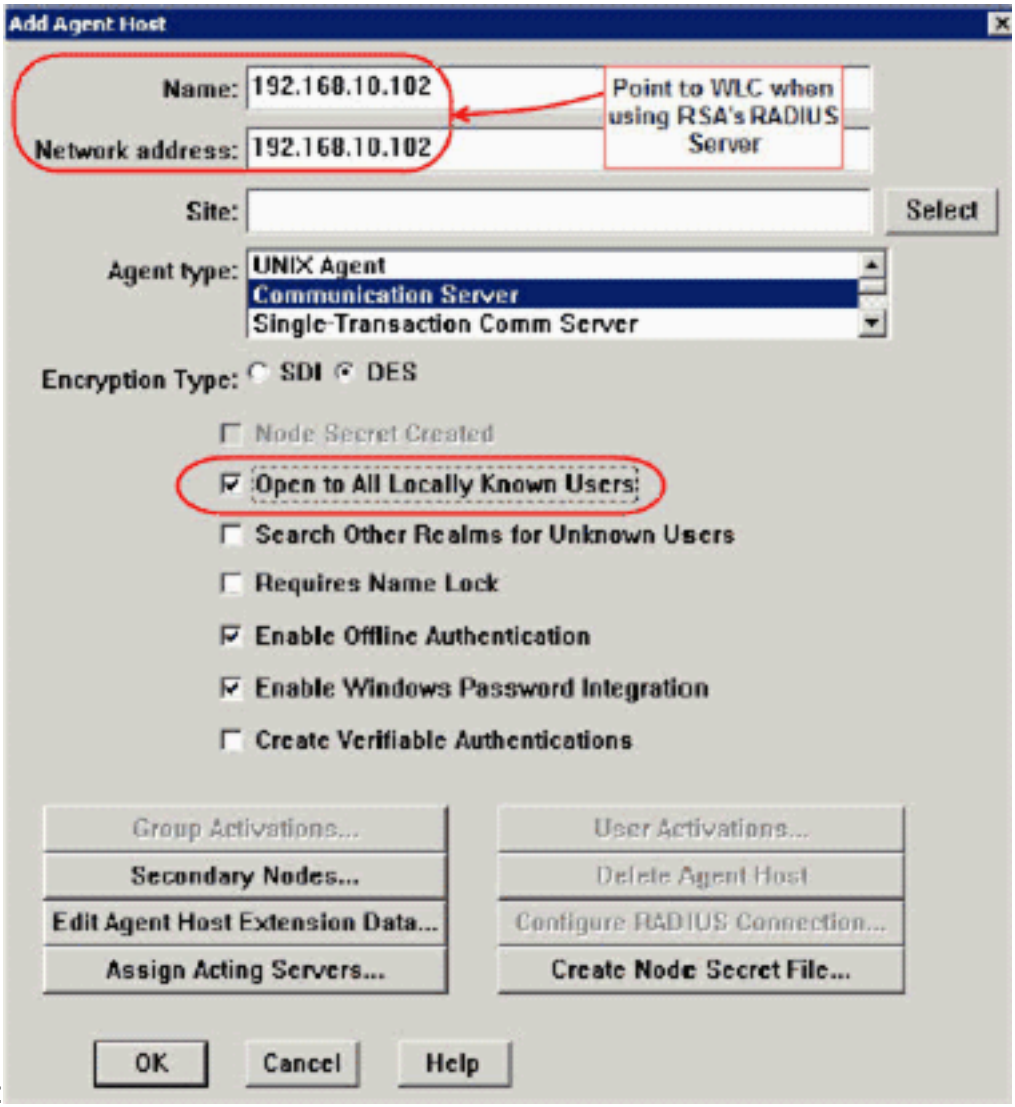
Nota: Los hostname dentro del dispositivo del encargado/RSA SecurID de la Autenticación RSA deben resolver a los IP Addresses válidos en la red local.

Complete estos pasos:

1. Abra la aplicación del modo del host del encargado de la Autenticación RSA.
2. Seleccione el **Agent Host (Host agente) > Add Agent Host (Agregar host agente)**.

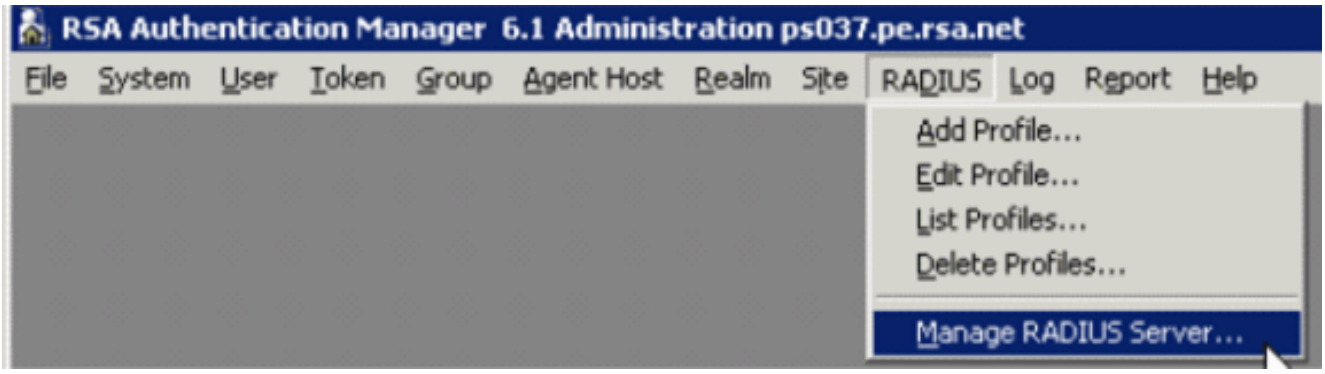


Usted ve esta



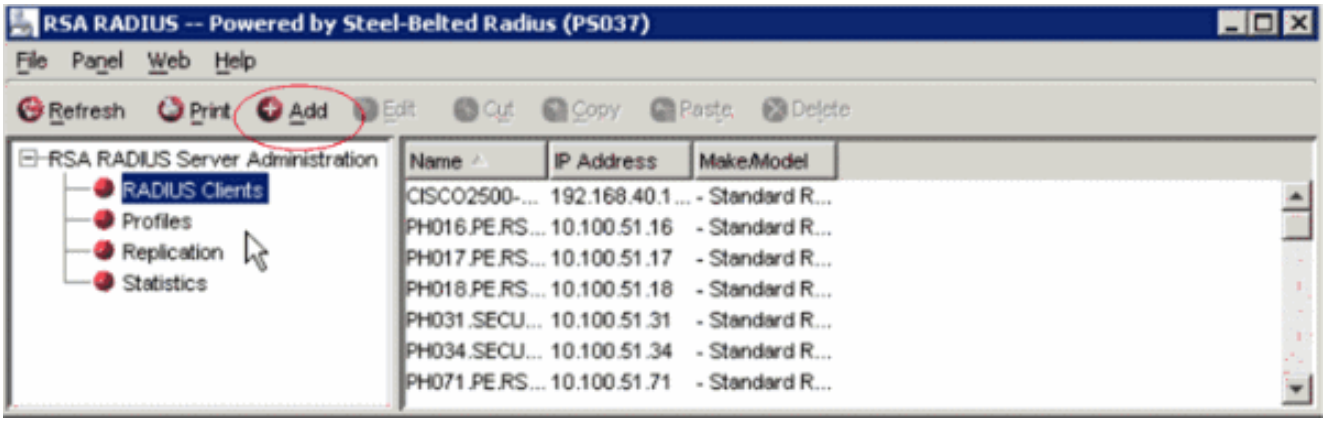
ventana:

3. Ingrese la información apropiada para el hostname WLC (un FQDN resoluble, en caso necesario) y la dirección de red. Elija **Communication Server (Servidor de comunicación)** para el tipo del agente y controle el checkbox para saber si hay **Open en todos los usuarios localmente conocidos**.
4. Click OK.
5. Del menú, selecto el **RADIUS > maneja al servidor de RADIUS**.

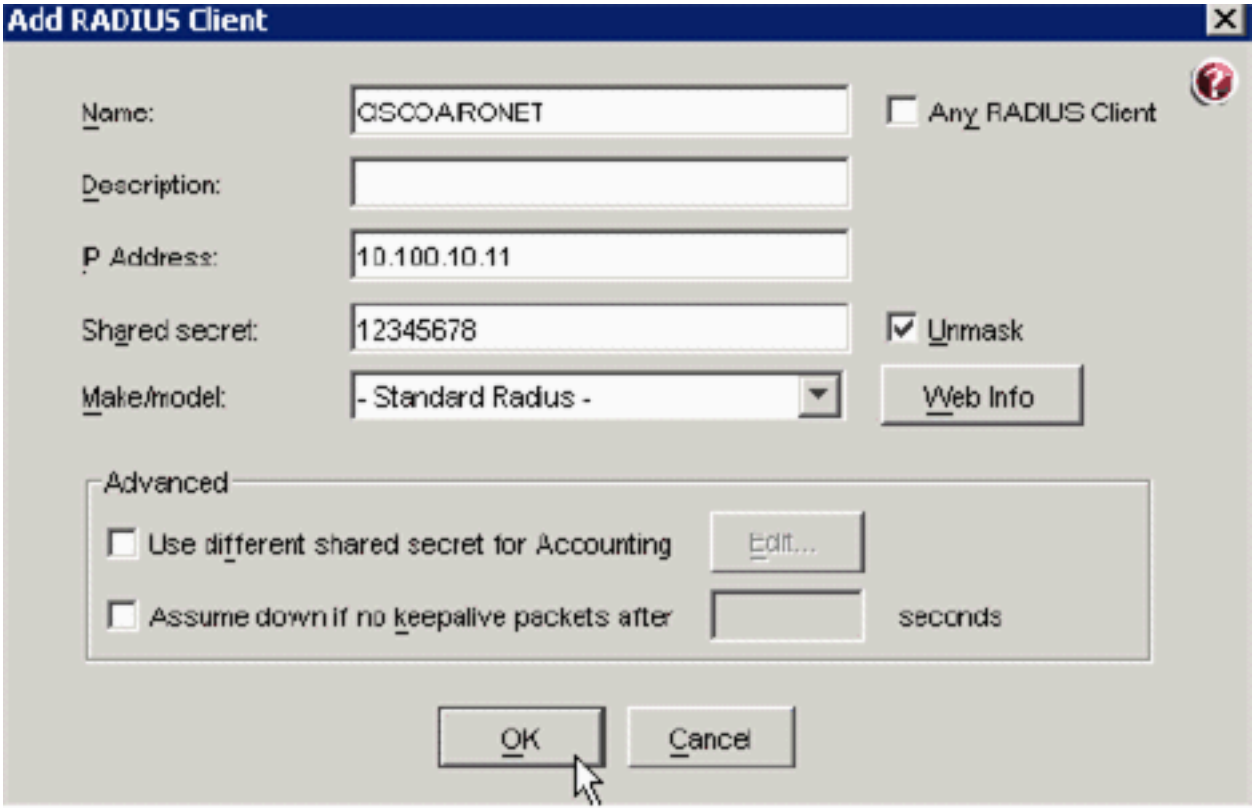


Una nueva ventana de administración se abre.

6. En esta ventana, los **clientes** selectos **RADIUS**, entonces hacen clic **agregan**.



7. Ingrese la información apropiada para el Cisco WLC. El secreto compartido debe hacer juego el secreto compartido definido en Cisco
WLC.



8. Click OK.

Configuración de agente de autenticación

Esta tabla representa las funciones del agente de la 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

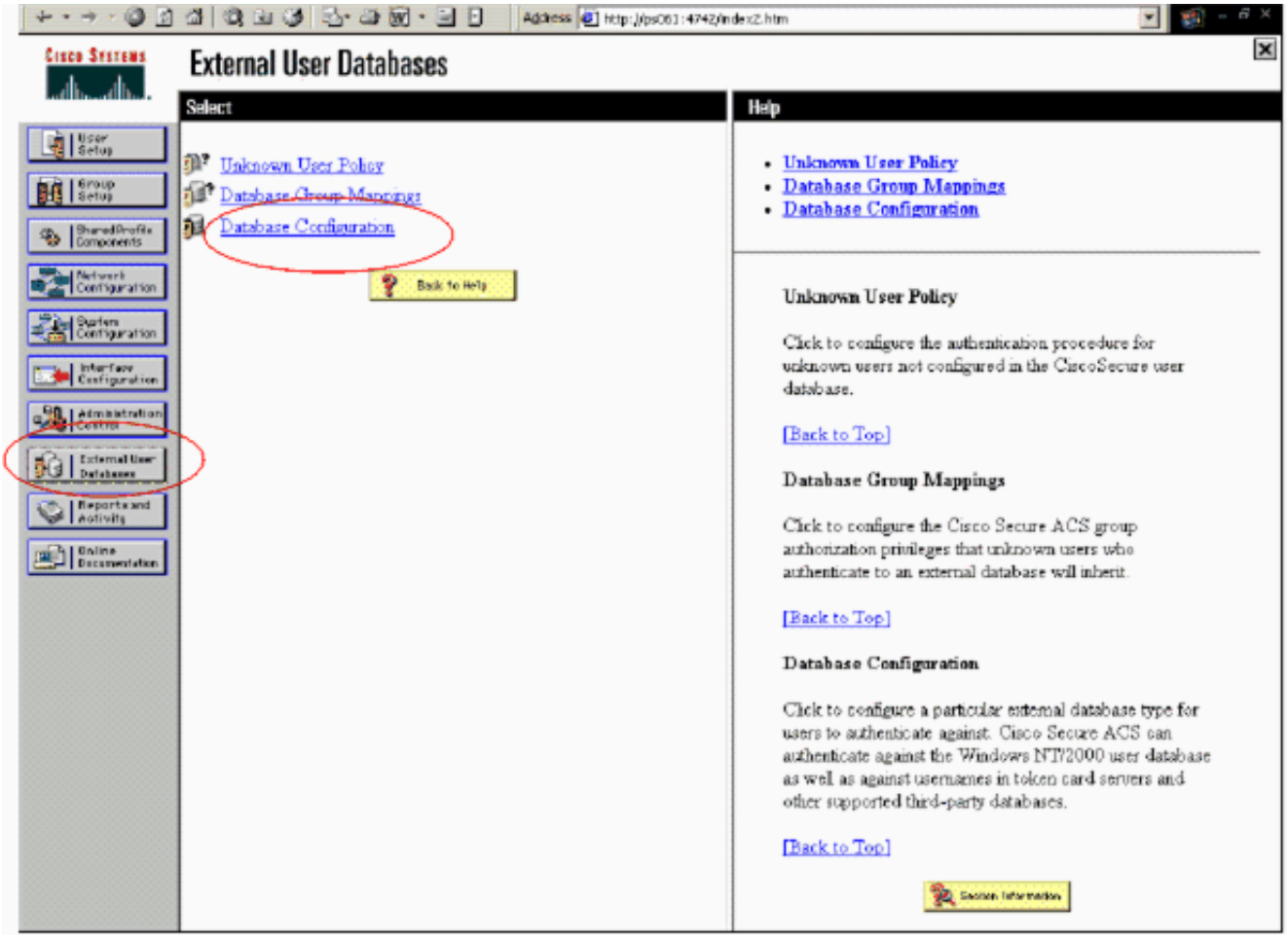
Nota: Vea la documentación RADIUS que fue incluida con el encargado de la Autenticación RSA en cómo configurar al servidor de RADIUS, si ése es el servidor de RADIUS que será utilizado.

Configure Cisco ACS

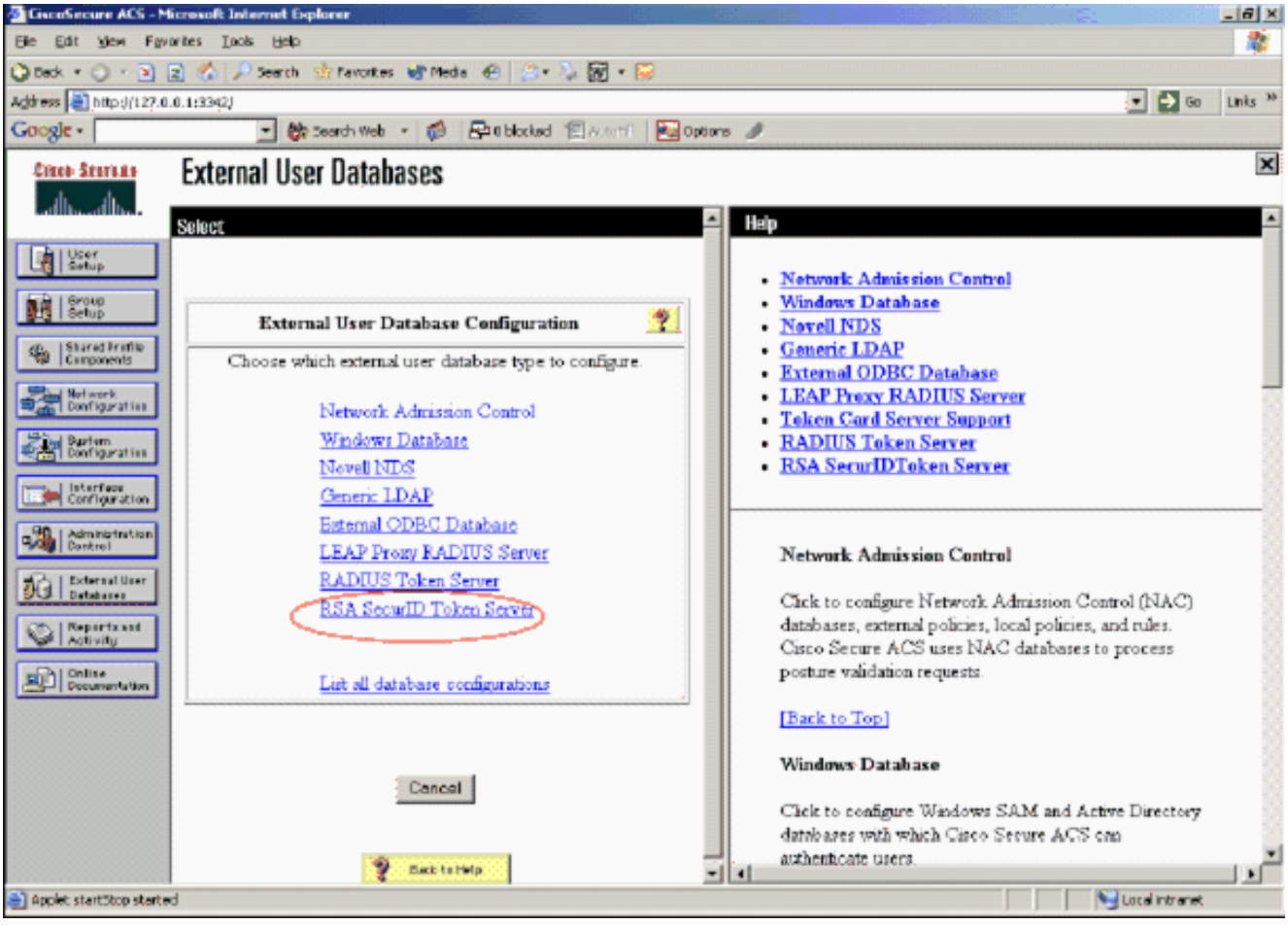
Active la autenticación de SecurID RSA

Cisco ACS seguro utiliza la autenticación de SecurID RSA de los usuarios. Complete estos pasos para configurar Cisco ACS seguro para autenticar a los usuarios con el encargado 6.1 de la autenticación:

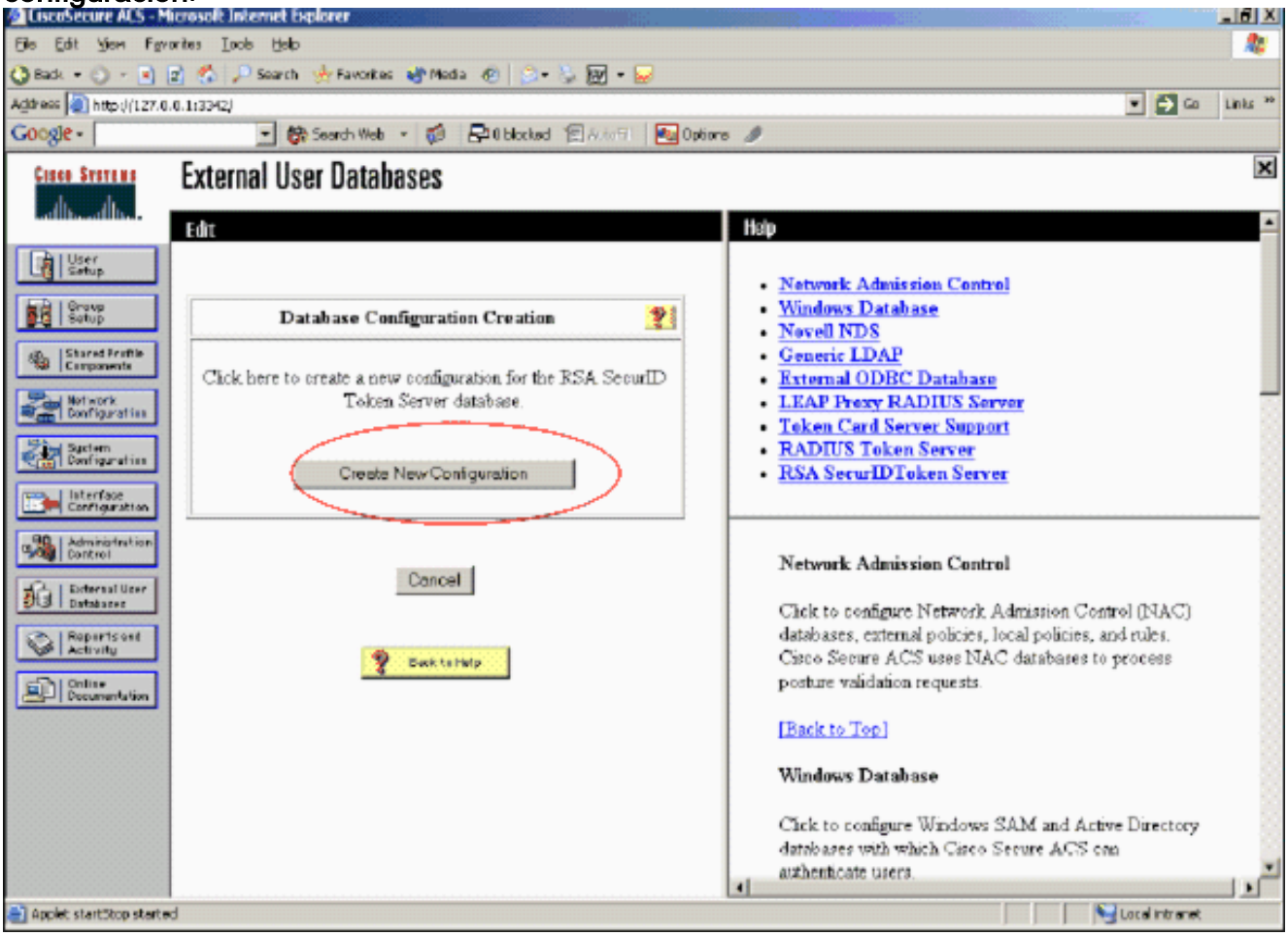
1. Instale el agente 5.6 de la Autenticación RSA o más adelante para Windows en el mismo sistema que Cisco asegura al servidor ACS.
2. Verifique la Conectividad funcionando con la función de la prueba de la autentificación del agente de autenticación.
3. Copie el fichero aceclnt.dll del **encargado de la Seguridad \ de la Autenticación RSA de** c:\Program Files\RSA del servidor RSA **\ del directorio del prog al directorio de** c:\WINNT\system32 del servidor ACS.
4. En la barra de navegación, haga clic la **Base de datos de usuarios externa**. Entonces, **configuración de la base de datos del** tecleo en la página de la base de datos externa.



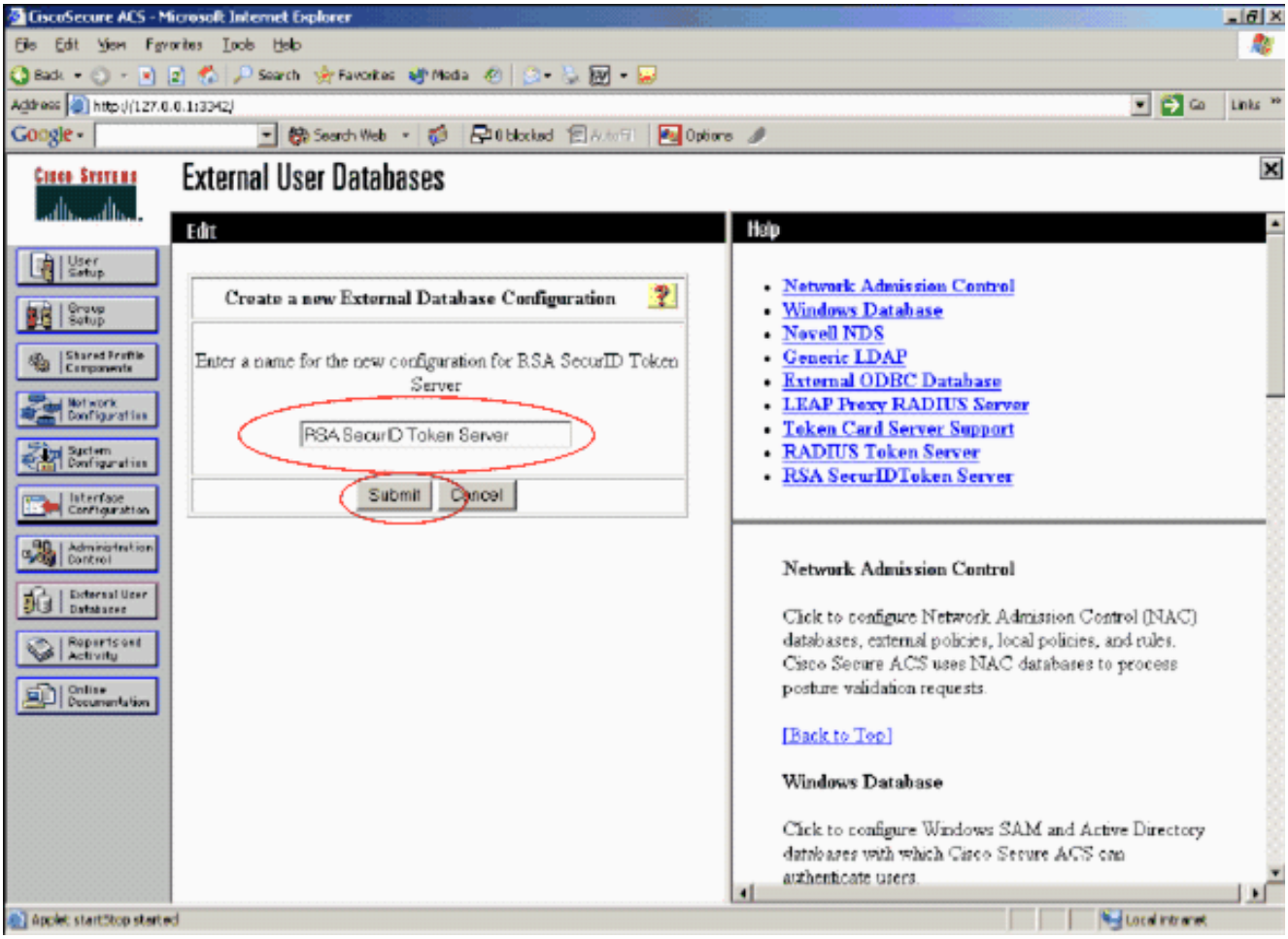
5. En la página de la Configuración de base de datos de usuarios externa, **servidor del token del** tecleo **RSA SecurID**.



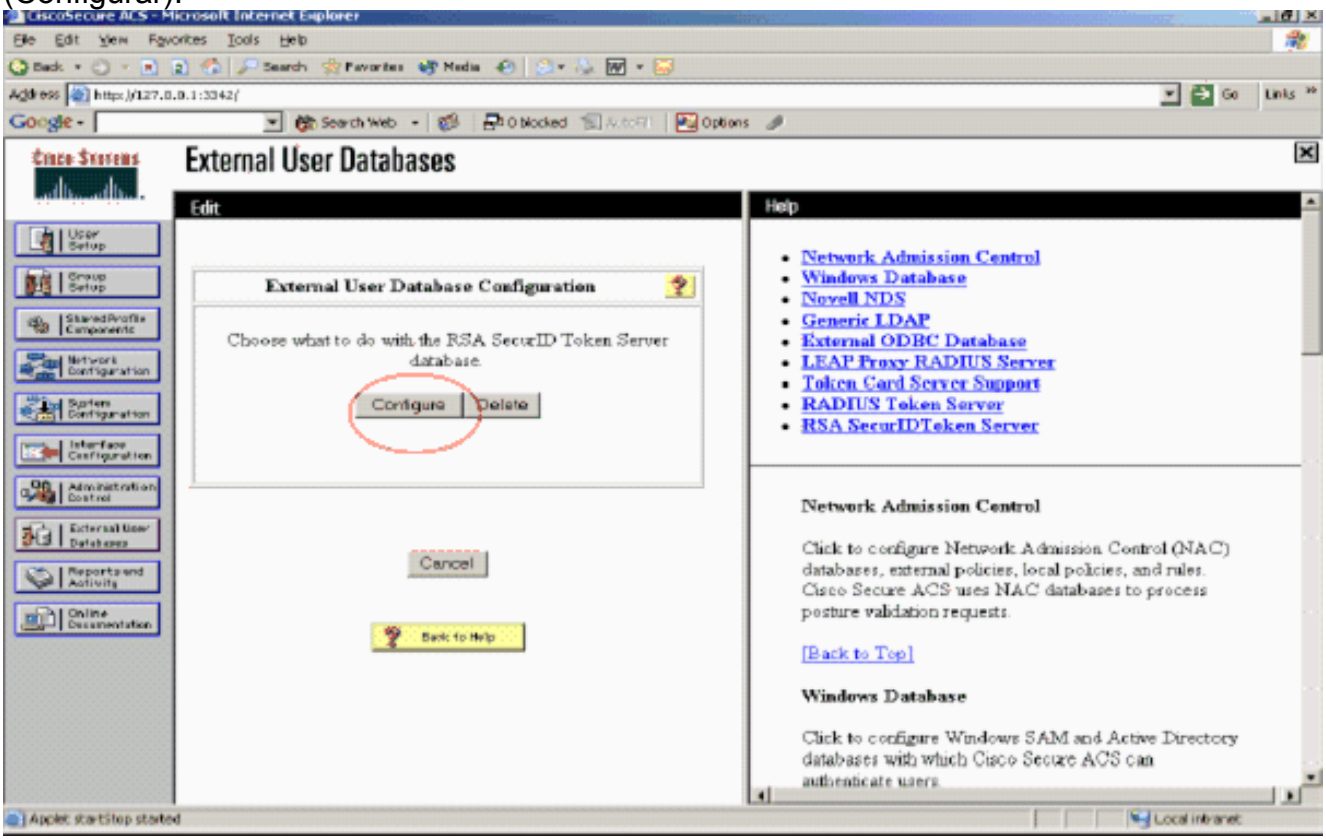
6. El tecleo **crea la nueva configuración**.



7. Ingrese un nombre, después haga clic **someten**.

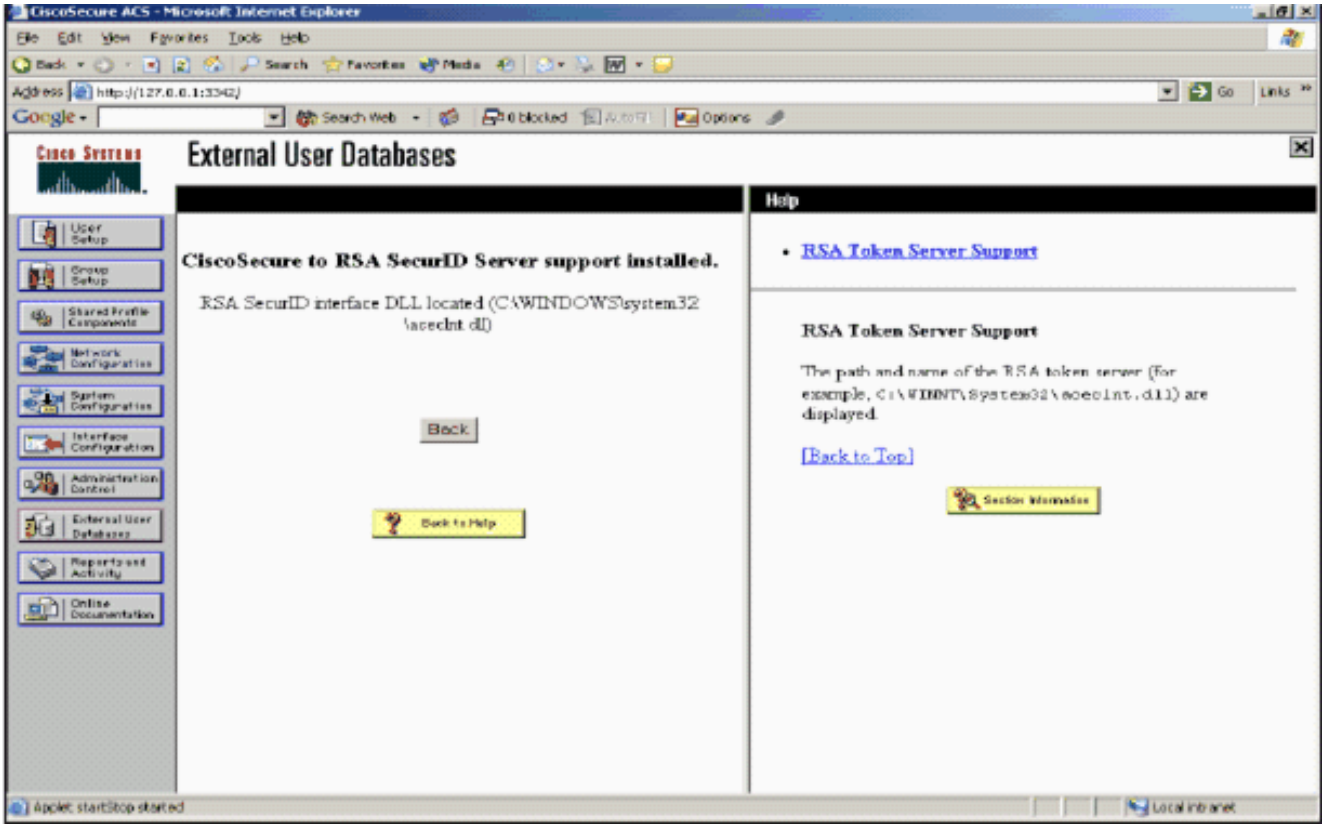


8. Haga clic en Configure (Configurar).



Cisco ACS seguro visualiza el nombre del servidor simbólico y de la trayectoria al authenticator DLL. Esta información confirma que Cisco ACS seguro puede entrar en contacto con el agente de la Autenticación RSA. Usted puede agregar la Base de datos de usuarios externa RSA SecurID a su Política de usuario desconocido o asignar las cuentas

de usuario específicas para utilizar esta base de datos para la autenticación.

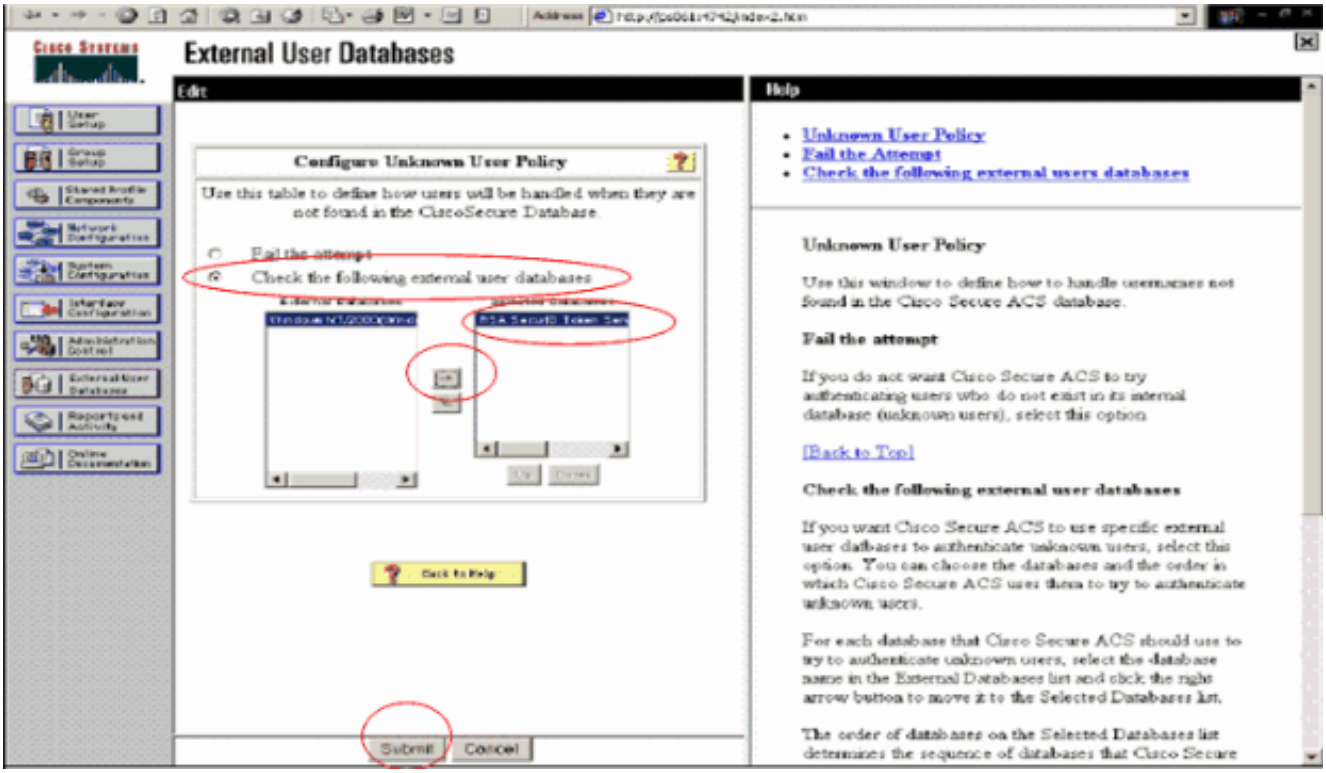


Agregue/configure la autenticación de SecurID RSA a su Política de usuario desconocido

Complete estos pasos:

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

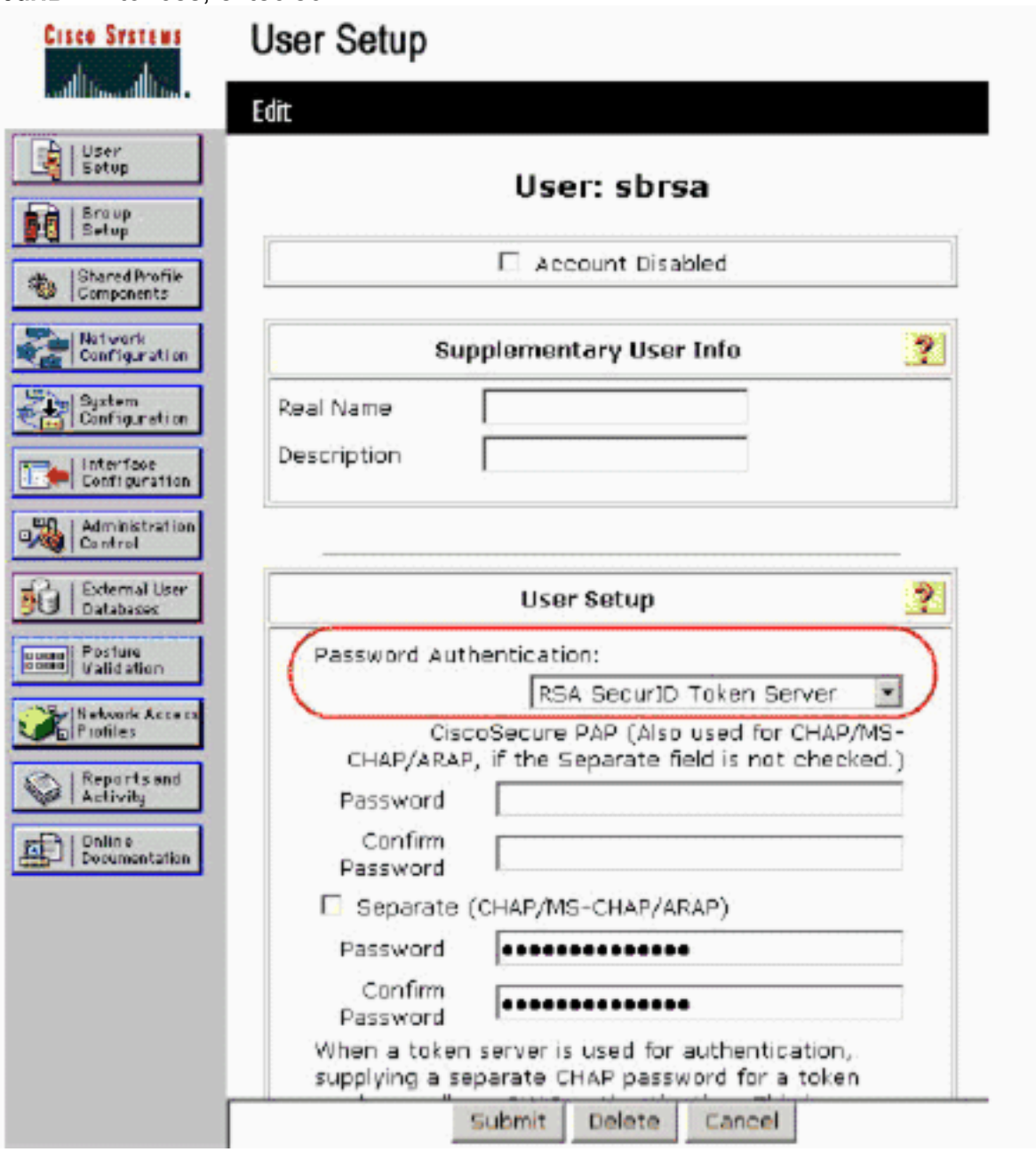
2. En la página de la **Política de usuario desconocido**, el **control** selecto las **Bases de datos de usuarios externas siguientes**, destaca el **servidor simbólico RSA SecurID** y lo mueve al cuadro de las bases de datos seleccionadas. Entonces, el tecleo **somete**.



Agregue/configure la autenticación de SecurID RSA para las cuentas de usuario específicas

Complete estos pasos:

1. Haga clic la **configuración de usuario del** GUI principal ACS Admin. Ingrese el username y el tecleo **agregan** (o seleccione a un usuario existente que usted desea modificarse).
2. Bajo la configuración de usuario > autenticación de contraseña, elija el **servidor del token RSA SecurID**. Entonces, el tecleo **somete**.

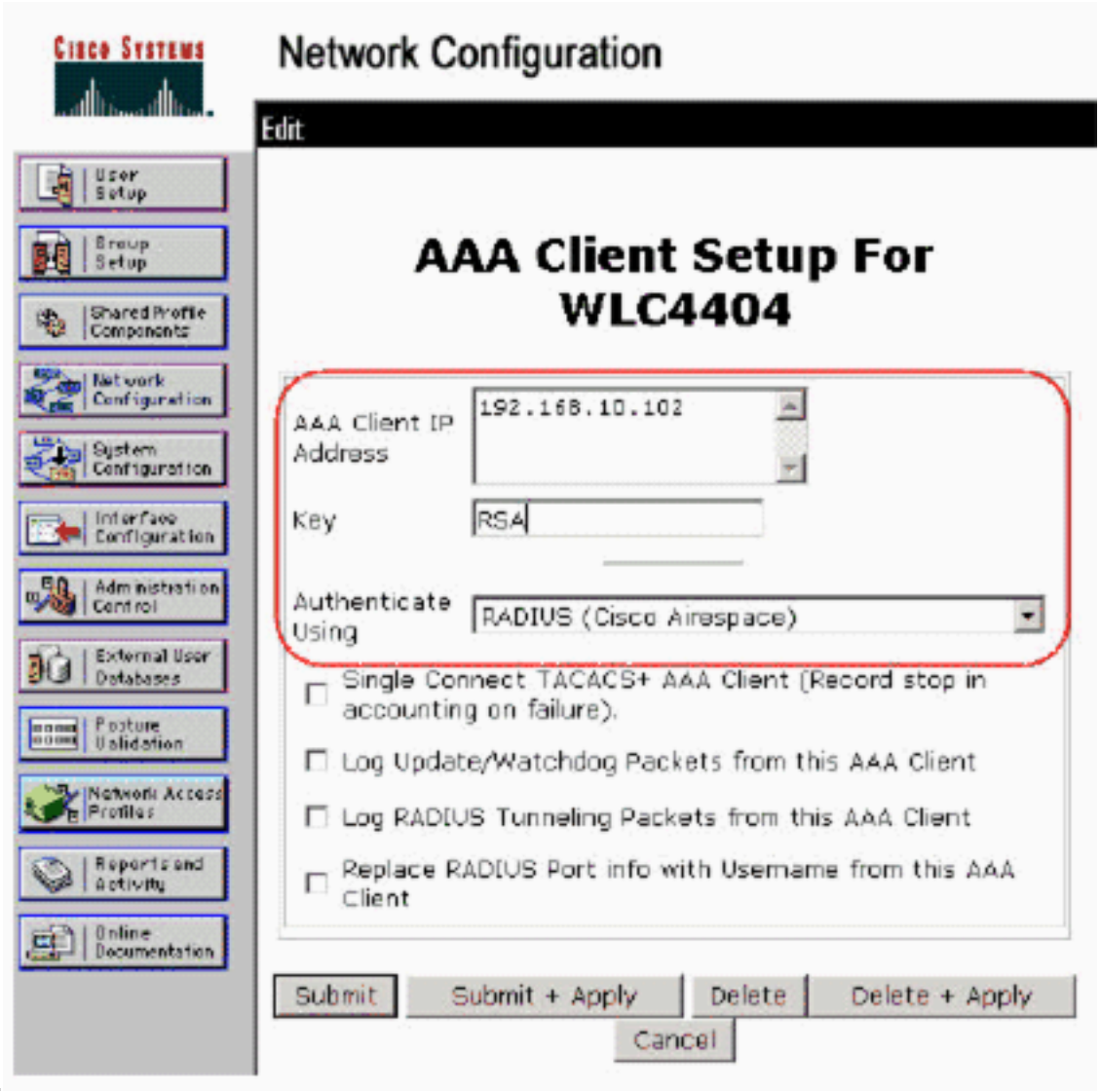


Agregue a un cliente RADIUS en Cisco ACS

El servidor ACS de Cisco instala necesitará los IP Addresses del WLC servir como NAS para remitir las autenticaciones PEAP del cliente al ACS.

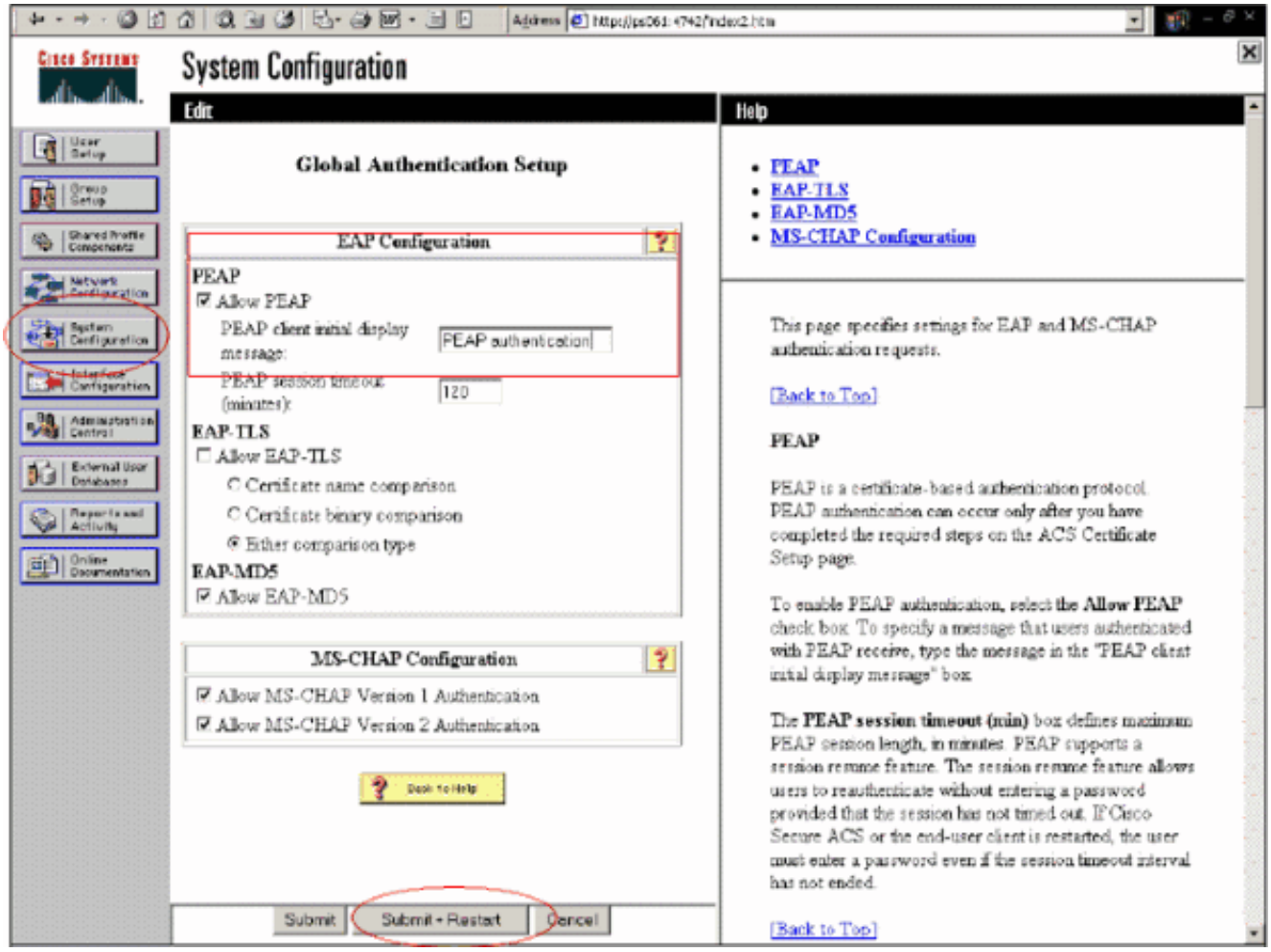
Complete estos pasos:

1. Bajo **configuración de red**, agregue/corrija al cliente AAA para el WLC que será utilizado. Ingrese la clave “secreta” compartida (común a WLC) que se utiliza entre el cliente AAA y el ACS. Selecto **autentique usando > RADIUS (Cisco Airespace)** para este cliente AAA. Entonces, el tecleo **somete + se**



aplica.

2. Solicite y instale un certificado de servidor de una autoridad de certificación conocida, de confianza tal como autoridad de certificación RSA Keon.Para más información sobre este proceso, refiera a la documentación que envía con Cisco ACS. Si usted está utilizando al Certificate Manager RSA, usted puede ver el guía de instrumentación RSA Keon Aironet para la ayuda adicional. Usted debe completar con éxito esta tarea antes de que usted continúe.**Nota:** Los certificados autofirmados pueden también ser utilizados. Refiera a la documentación segura de Cisco ACS en cómo utilizar éstos.
3. Bajo **configuración del sistema > la disposición global de la autenticación**, controla el checkbox para saber si hay **autenticación PEAP Allow**.



Configure la configuración inalámbrica del regulador LAN de Cisco para el 802.1x

Complete estos pasos:

1. Conecte con la interfaz de línea de comando WLC para configurar el regulador así que puede ser configurado para conectar con Cisco asegura al servidor ACS.
2. Ingrese el **comando ip-address auténtico del radio de los config del** WLC de configurar a un servidor de RADIUS para la autenticación.**Nota:** Cuando usted prueba con el servidor de RADIUS del encargado de la Autenticación RSA, ingrese el IP address del servidor de RADIUS del encargado de la Autenticación RSA. Cuando usted prueba con el servidor ACS de Cisco, ingrese el IP address del Cisco aseguran al servidor ACS.
3. Ingrese el **comando port auténtico del radio de los config del** WLC de especificar el puerto UDP para la autenticación. Los puertos 1645 o 1812 son activos por abandono en el encargado y el servidor ACS de Cisco de la Autenticación RSA.
4. Ingrese el **comando secreto auténtico del radio de los config del** WLC de configurar el secreto compartido en el WLC. Esto debe hacer juego el secreto compartido creado en los servidores de RADIUS para este cliente RADIUS.
5. Ingrese el **comando enable auténtico del radio de los config del** WLC de activar la autenticación. Cuando está deseado, ingrese el **comando disable auténtico del radio de los config** de inhabilitar la autenticación. Observe que la autenticación está inhabilitada por abandono.
6. Seleccione la opción de seguridad apropiada de la capa 2 para la red inalámbrica (WLAN) deseada en el WLC.
7. Utilice las **estadísticas auténticas del radio de la demostración** y **muestre los comandos**

summary del radio de verificar que las configuraciones RADIUS están configuradas correctamente.**Nota:** Los temporizadores del valor por defecto para el Petición-descanso EAP son bajos y pudieron necesitar ser modificado. Esto se puede hacer usando el comando **avanzado los config del *<seconds> del petición*-descanso del eap**. Puede ser que también ayude a pellizcar el descanso de la petición de la identidad basado en los requisitos. Esto se puede hacer usando el comando **avanzado los config del *<seconds> del identidad-petición*-descanso del eap**.

Configuración de cliente de red inalámbrica del 802.11

Para una explicación detallada de cómo configurar a su suplicante inalámbrico de la dotación física y del cliente, refiera a la diversa Documentación de Cisco.

Problemas conocidos

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

- Ficha de software RSA. El nuevo modo Pin y los modos siguientes de Tokencode no se utilizan al usar esta forma de autenticación con el XP2. (FIJADO como resultado de ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip)
- Si su puesta en práctica ACS es más vieja o usted no tiene la corrección antedicha, el cliente no podrá autenticar hasta que las transiciones del usuario de “activaran; Nuevo modo PIN” “a activado”. Usted puede lograr esto teniendo el usuario completa una autenticación de la no-Tecnología inalámbrica, o usando la aplicación RSA de la “prueba de la autentificación”.
- Niegue 4 dígitos/los contactos alfanuméricos. Si un usuario en el nuevo modo Pin va contra la directiva PIN, el proceso de autenticación falla, y el usuario está inconsciente cómo o del porqué. Típicamente, si un usuario va contra la directiva, serán enviados un mensaje que el PIN fue rechazado y ser incitado otra vez mientras que mostraba al usuario otra vez cuál es la directiva PIN (por ejemplo, si la directiva PIN es 5-7 dígitos, con todo el usuario ingresa 4 dígitos).

Información Relacionada

- La asignación VLAN dinámica con WLCs basó en ACS al ejemplo de la configuración de la asignación del grupo del Active Directory
- Ejemplo de Configuración del Cliente VPN sobre LAN Inalámbrica con WLC
- Autenticación en los ejemplos inalámbricos de la configuración de los reguladores LAN
- Autenticación del EAP-FAST con los reguladores inalámbricos LAN y el ejemplo externo de la configuración de servidor de RADIUS
- Tipos inalámbricos de la autenticación en ISR fijo con el ejemplo de la configuración de SDM
- Tipos inalámbricos de la autenticación en un ejemplo fijo de la configuración ISR
- Cisco protegió el protocolo extensible authentication
- Autenticación EAP con el servidor de RADIUS
- Soporte Técnico y Documentación - Cisco Systems