SecurID RSA listo con los reguladores del Wireless LAN y el ejemplo de configuración del Cisco Secure ACS

Contenido

Introducción

Este documento explica cómo configurar y configurar el protocolo del Punto de acceso de las livianas de Cisco (LWAPP) - los AP capaces y los reguladores del Wireless 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 del WLCs y cómo configurar los parámetros básicos del WLC.
- Conocimiento en cómo configurar el perfil del cliente de la tecnología inalámbrica de Cisco usando utilidad Aironet Desktop (ADU).

- Tenga conocimiento funcional del Cisco Secure ACS.
- Tenga conocimiento básico del LWAPP.
- Tenga comprensión básica de los servicios del Active Directory de Microsoft Windows (AD), así como del controlador de dominio y de los conceptos DNS.**Nota:** Antes de que usted intente esta configuración, asegúrese de que el 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 de Microsoft Windows AD, refiera a la documentación de Microsoft para configurar al servidor de administración ACS y RSA en el mismo dominio. Refiera al Active Directory de la configuración y a la base de datos 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.

- Administrador 6.1 de la Autenticación RSA
- Agente 6.1 de la Autenticación RSA para Microsoft Windows
- Estructura 27 del Cisco Secure 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 administrador de la Autenticación RSA en cómo configurar el servidor.
- WLCs y Puntos de acceso ligeros de Cisco 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 del SecurID RSA es una solución bifactorial de la autenticación de usuario. Utilizado conjuntamente con el administrador de la Autenticación RSA y un agente de la Autenticación RSA, el authenticator del SecurID RSA requiere a los usuarios identificarse usando un mecanismo de autenticación bifactorial.

Uno es el código del SecurID RSA, 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 del SecurID RSA son tan simples utilizar como ingresar una contraseña. Asignan cada usuario final un authenticator del SecurID RSA que genere un código del uno-tiempo-uso. Al abrir una sesión, el usuario ingresa simplemente este número y un PIN secreto que se autenticará con éxito. Como una ventaja agregada, los tokens del hardware del SecurID RSA 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.

A través del cuadro de los de la derecha de la autenticación de SecurID del soporte RSA de los servidores del programa listo del SecurID RSA, del WLCs de Cisco y del Cisco Secure ACS. Las peticiones del acceso de las interceptaciones del software agente de la Autenticación RSA, si local o telecontrol, de los usuarios (o de los grupos de usuarios) y los dirigen al programa del administrador de la Autenticación RSA para la autenticación.

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

En este documento, se utilizan estas configuraciones:

- Configuración del host agente
- Configuración de agente de autenticación

Configuración del host agente

Usando el Cisco Secure ACS como el servidor de RADIUS

Para facilitar la comunicación entre el Cisco Secure ACS y el dispositivo del SecurID del administrador/RSA 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 el Cisco Secure ACS dentro de su base de datos y contiene la información sobre la comunicación y el cifrado.

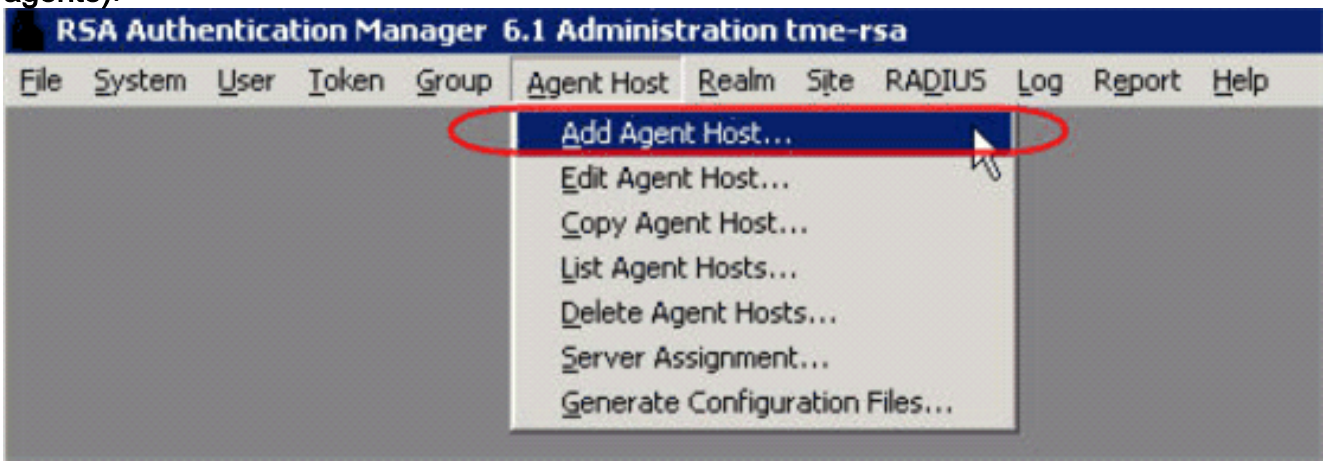
Para crear el expediente del host agente, usted necesita esta información:

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

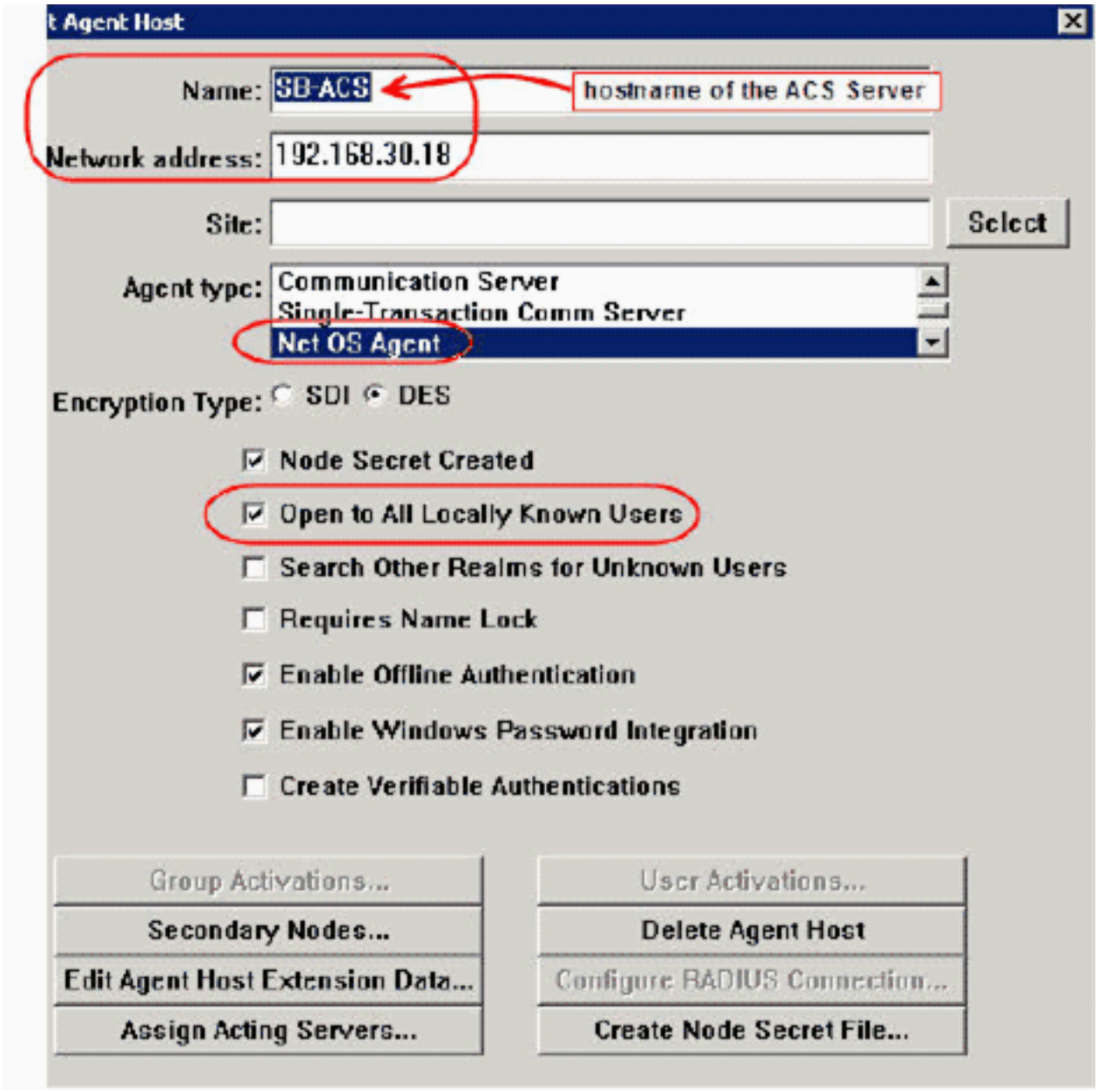
Complete estos pasos:

1. Abra la aplicación del modo del host del administrador 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 marque el checkbox para **Open en todos los usuarios localmente conocidos**.
4. Haga clic en OK.

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

Para facilitar la comunicación entre el WLC de Cisco y el administrador 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 el WLC de Cisco 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:

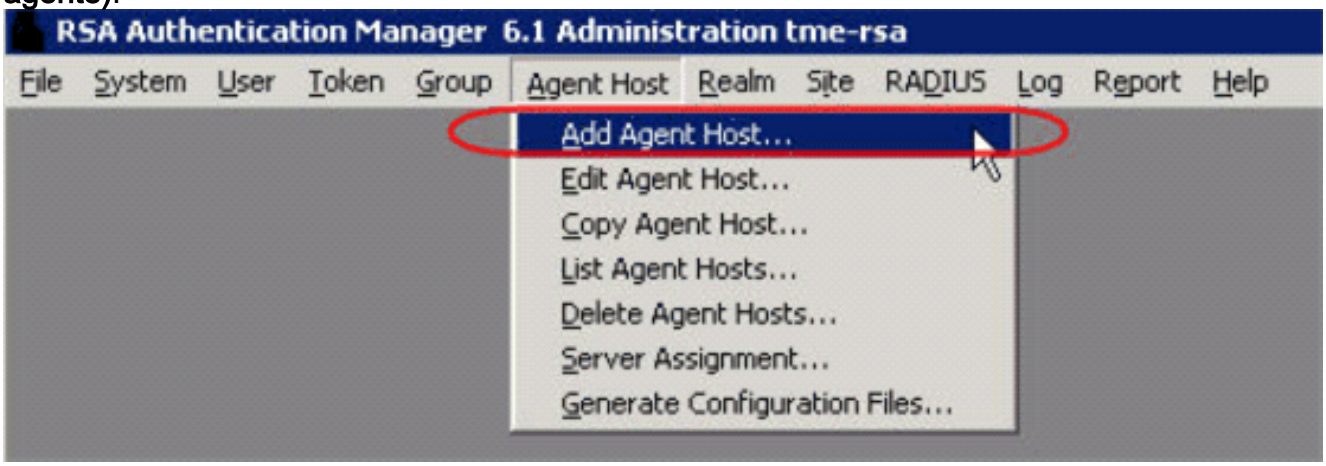
- El nombre de host WLC
- IP Address de administración del WLC
- Secreto RADIUS, que debe hacer juego el secreto RADIUS en el WLC de Cisco

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 administrador de la Autenticación RSA para determinar cómo ocurrirá la comunicación con el WLC.

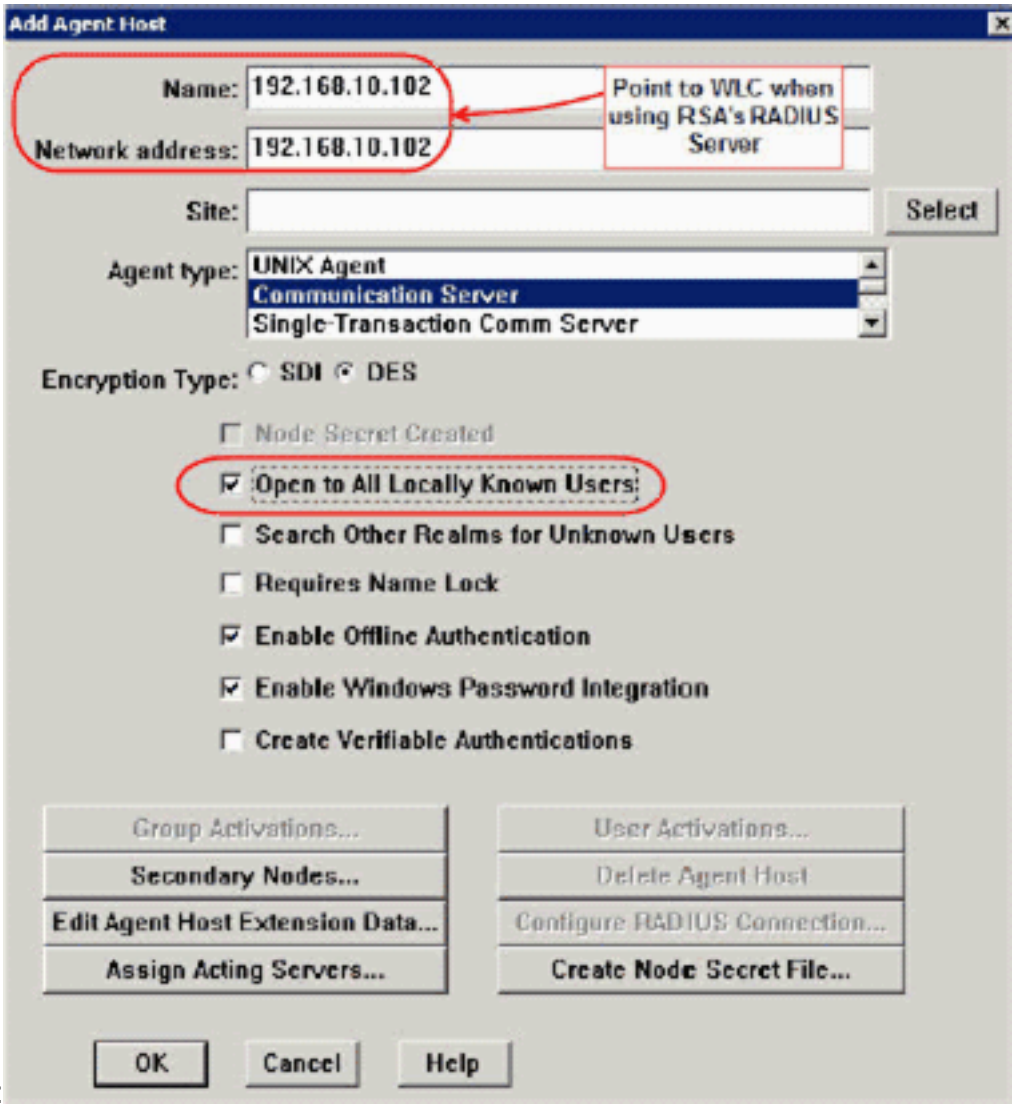
Nota: Los nombres de host dentro del dispositivo del SecurID del administrador/RSA de la Autenticación RSA deben resolver a los IP Address válidos en la red local.

Complete estos pasos:

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

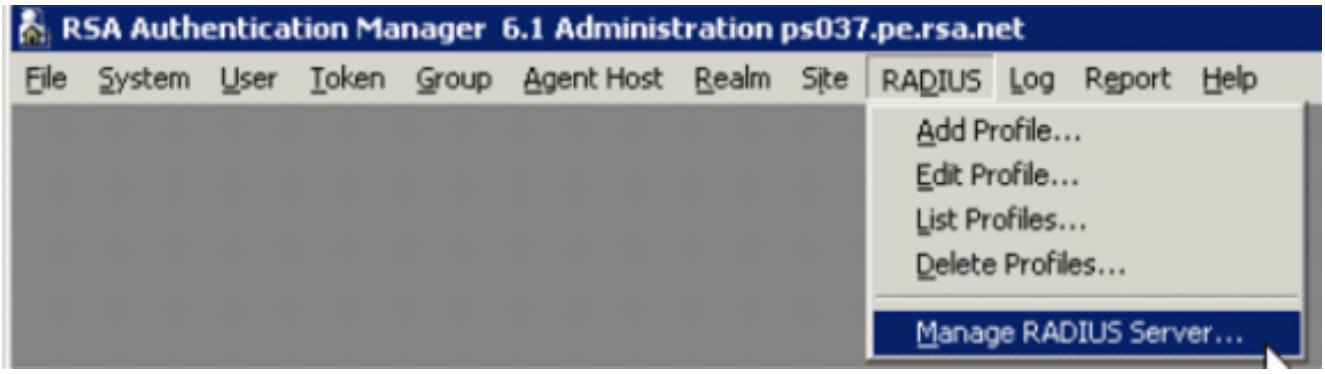


Usted ve esta



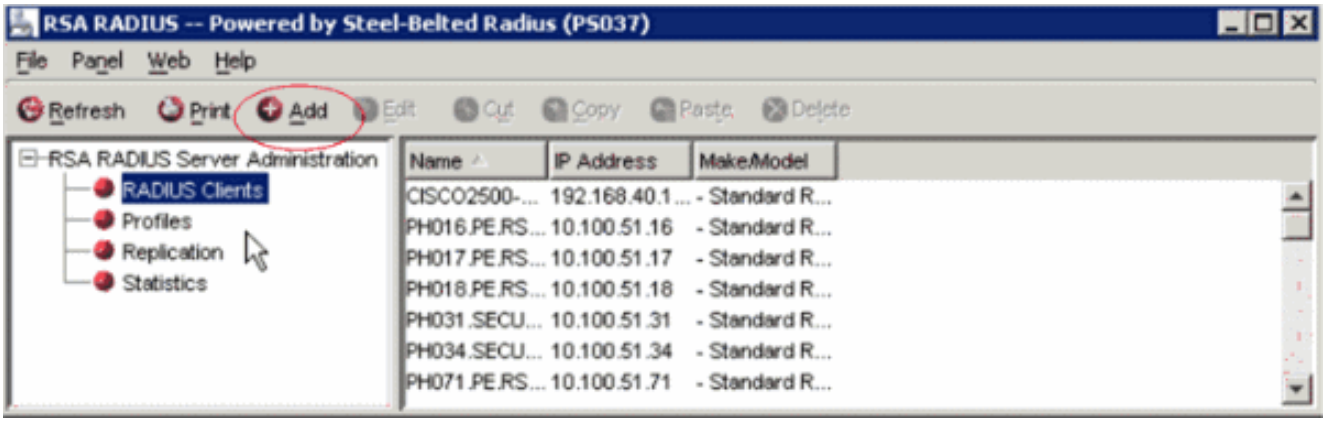
ventana:

3. Ingrese la información apropiada para el nombre de host del WLC (un FQDN resolvable, en caso necesario) y la dirección de red. Elija **Communication Server (Servidor de comunicación)** para el tipo del agente y marque el checkbox para **Open en todos los usuarios localmente conocidos**.
4. Haga clic en OK.
5. Del menú, selecto el **RADIUS > maneja al servidor de RADIUS**.

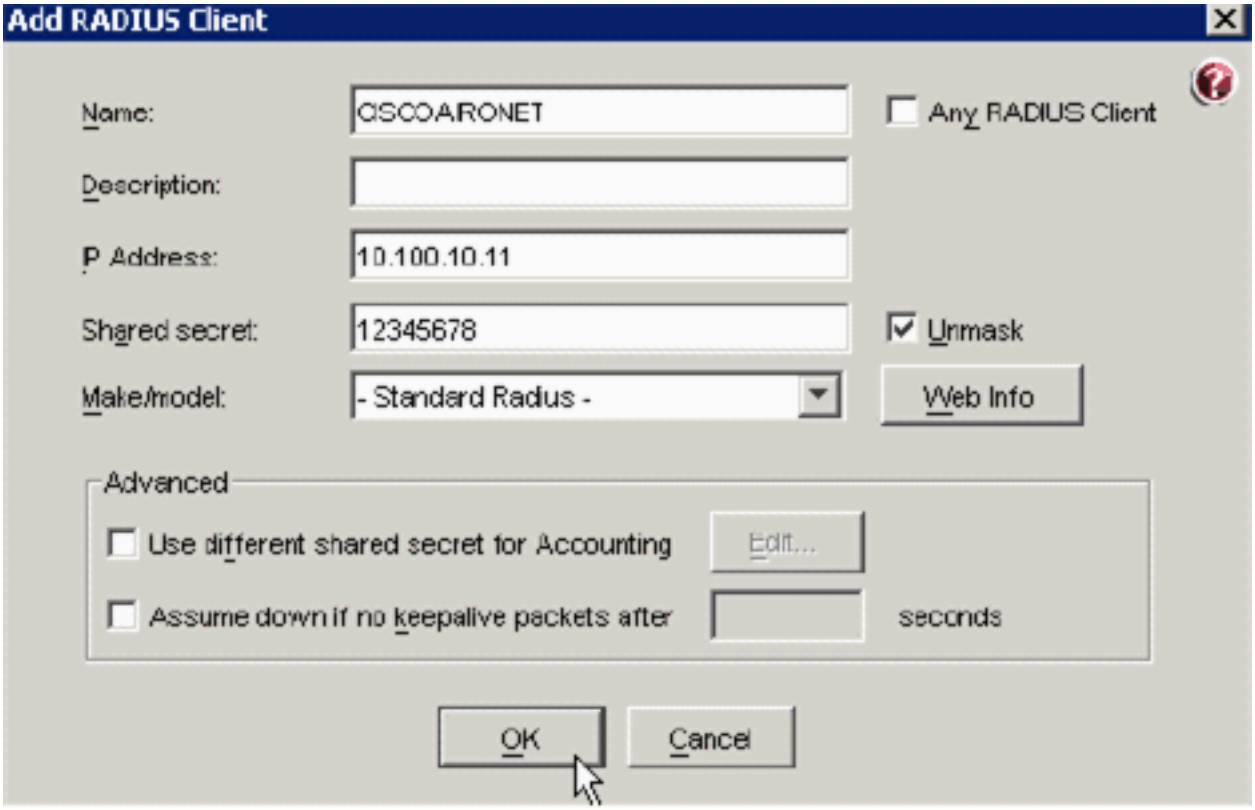


Una nueva ventana de administración se abre.

6. En esta ventana, seleccione a los **clientes RADIUS**, entonces haga click en Add



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



8. Haga clic en OK.

Configuración de agente de autenticación

Esta tabla representa las funciones del agente de la Autenticación RSA del 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

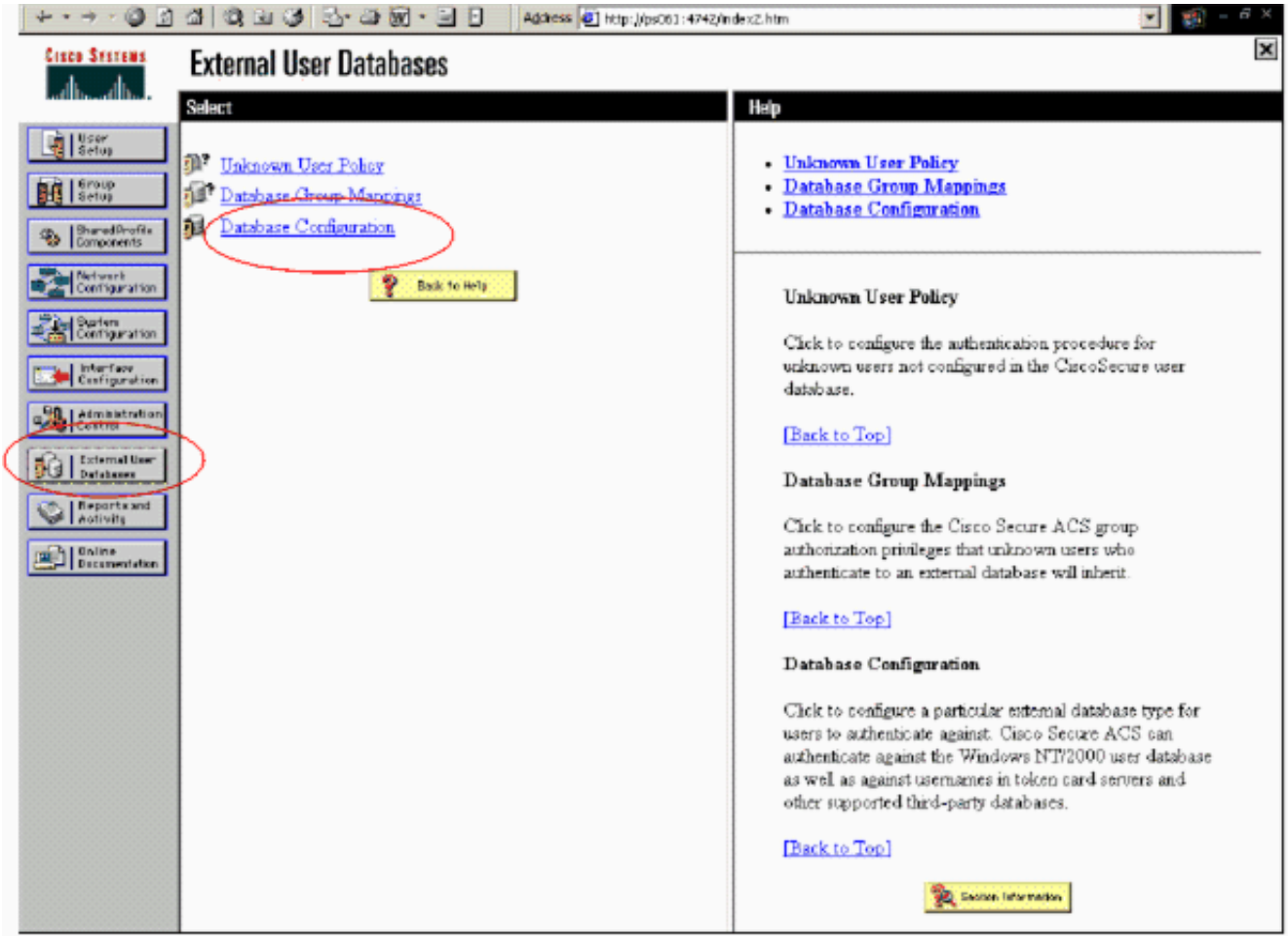
Nota: Vea la documentación RADIUS que fue incluida con el administrador de la Autenticación RSA en cómo configurar al servidor de RADIUS, si ése es el servidor de RADIUS que será utilizado.

Configure Cisco ACS

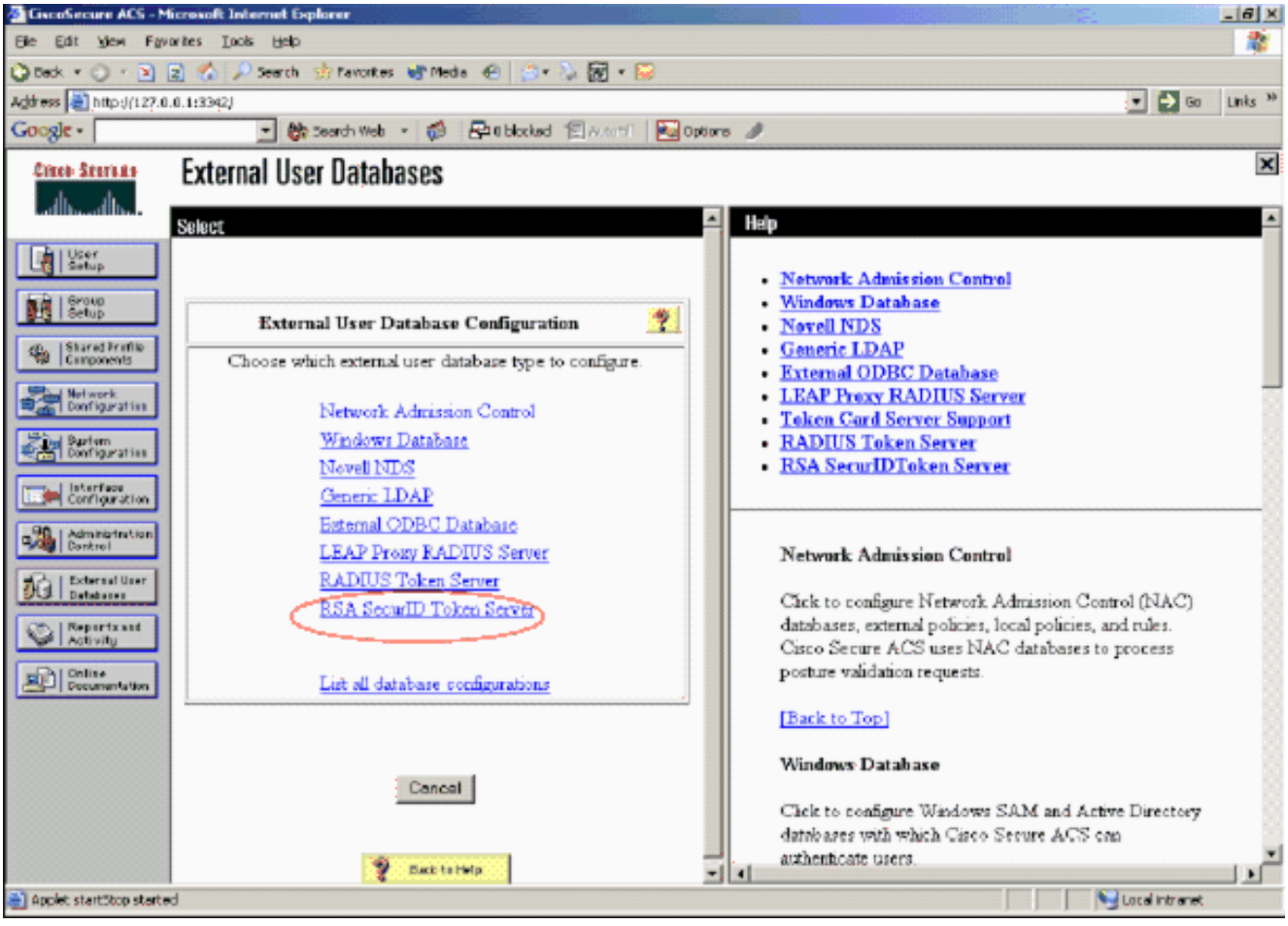
Active la autenticación de SecurID RSA

Autenticación de SecurID de los soportes RSA del Cisco Secure ACS de los usuarios. Complete estos pasos para configurar el Cisco Secure ACS para autenticar a los usuarios con el administrador 6.1 de la autenticación:

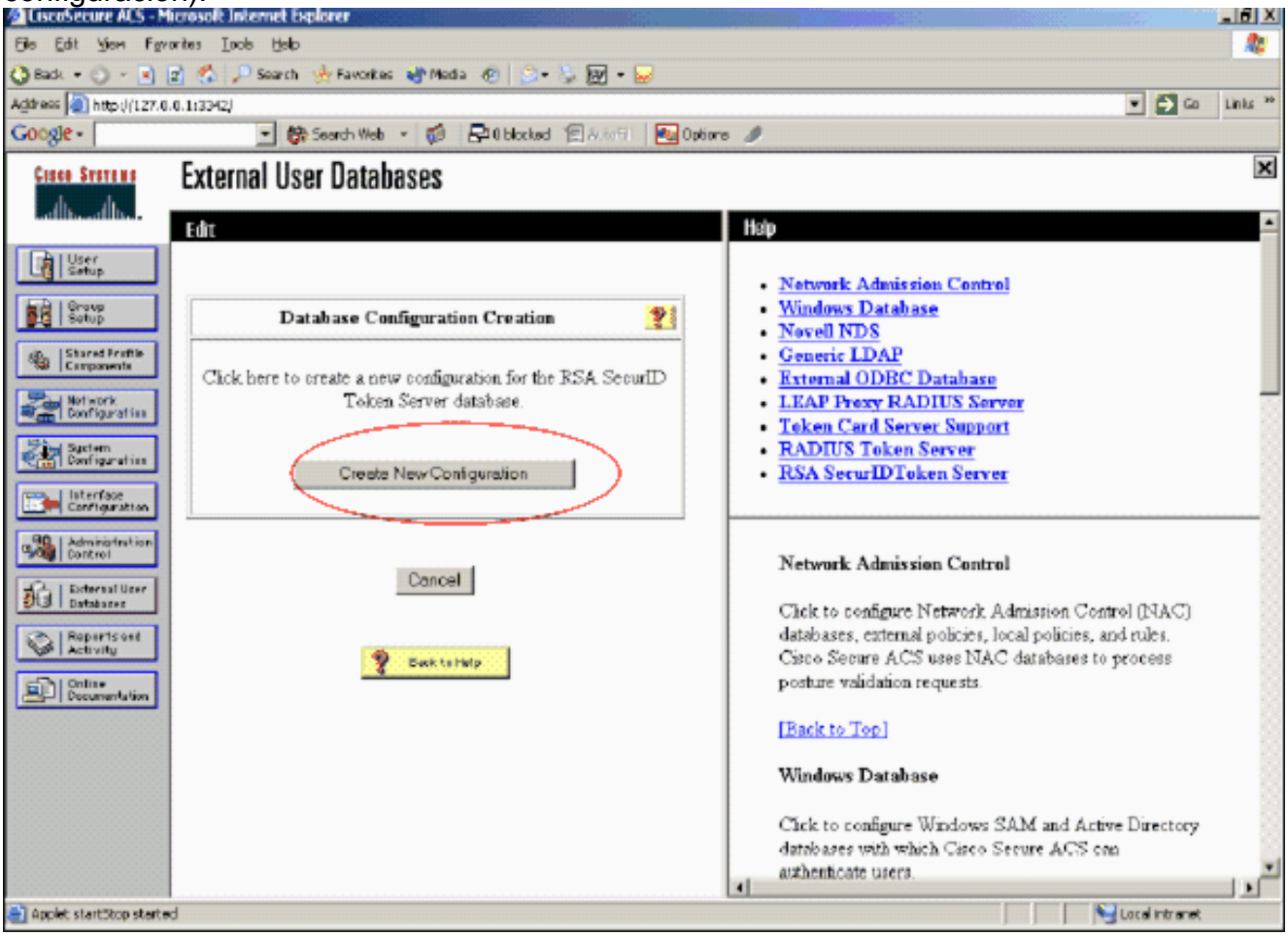
1. Instale el agente 5.6 de la Autenticación RSA o más adelante para Windows en el mismo sistema que el servidor del Cisco Secure ACS.
2. Verifique la Conectividad funcionando con la función de la prueba de la autentificación del agente de autenticación.
3. Copie el archivo aceclnt.dll del **administrador 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.



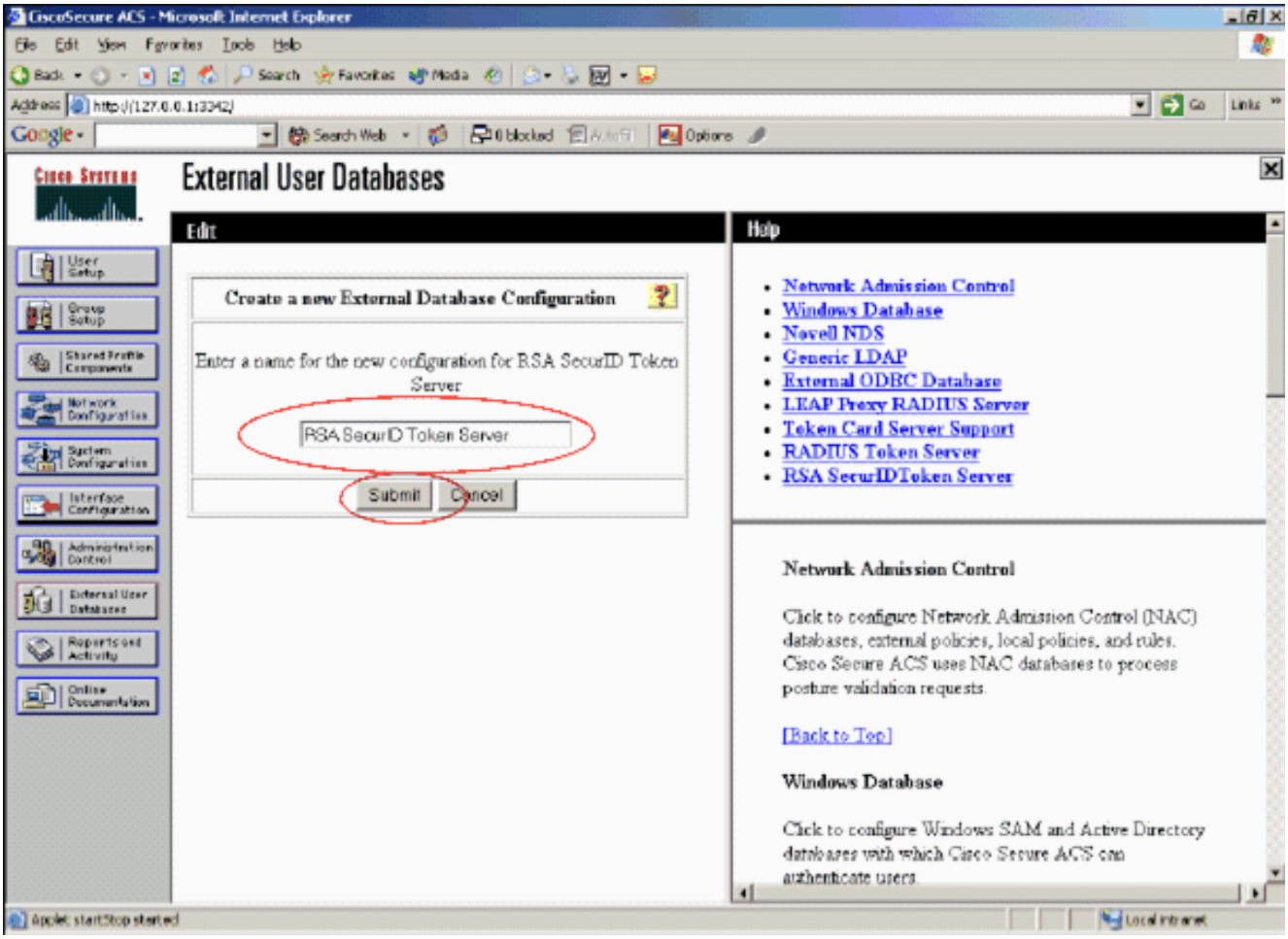
5. En la página de la Configuración de base de datos de usuarios externa, **servidor Token del SecurID del** tecleo **RSA**.



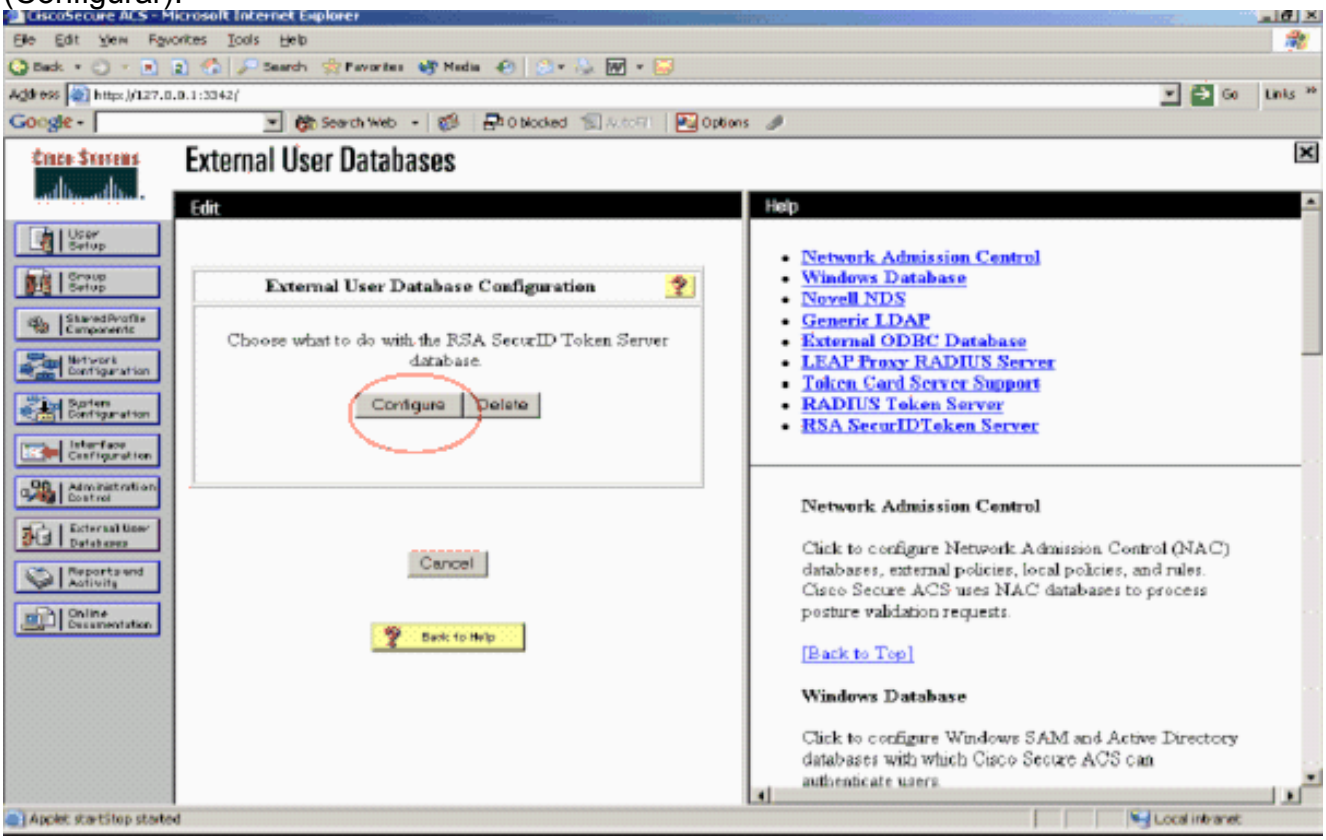
6. Haga clic en Create New Configuration (Crear nueva configuración).



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

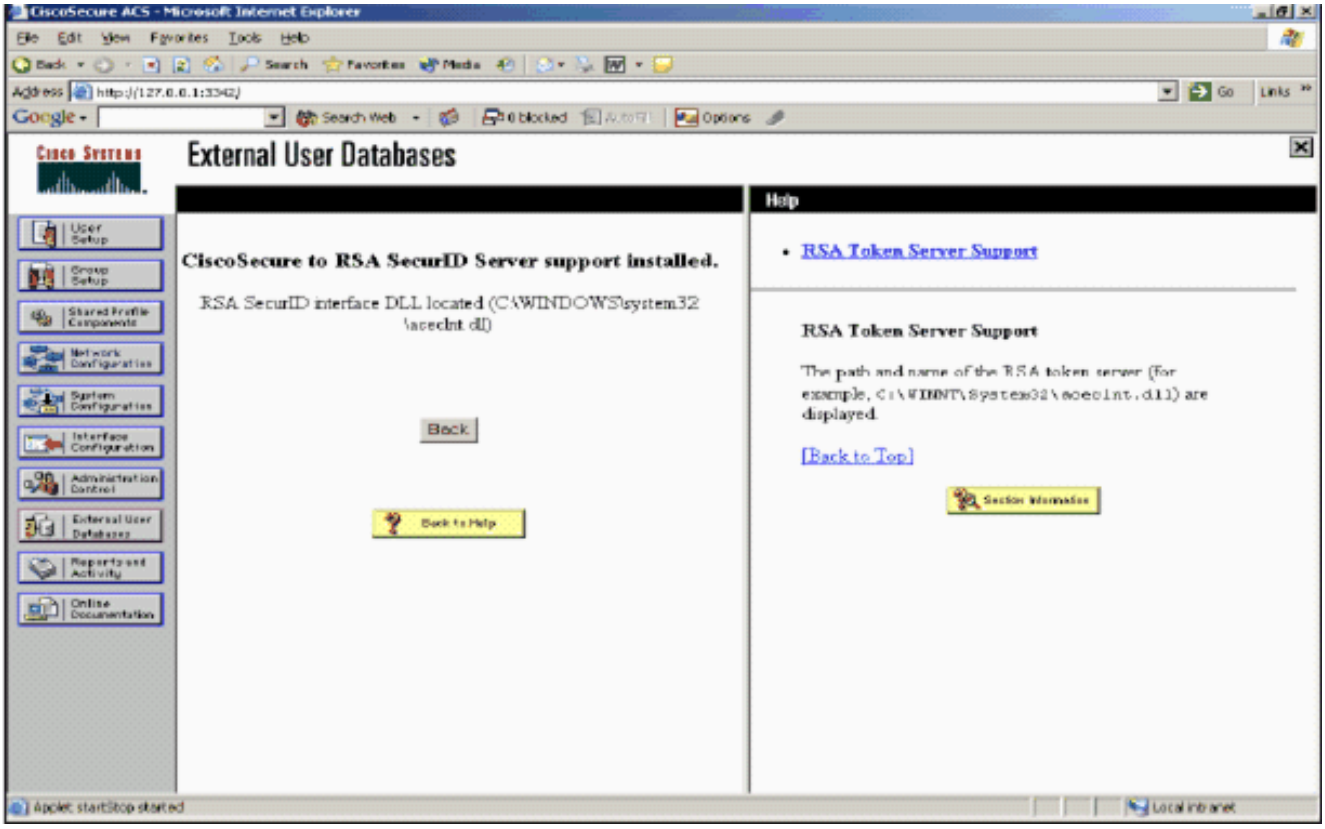


8. Haga clic en Configure (Configurar).



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

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

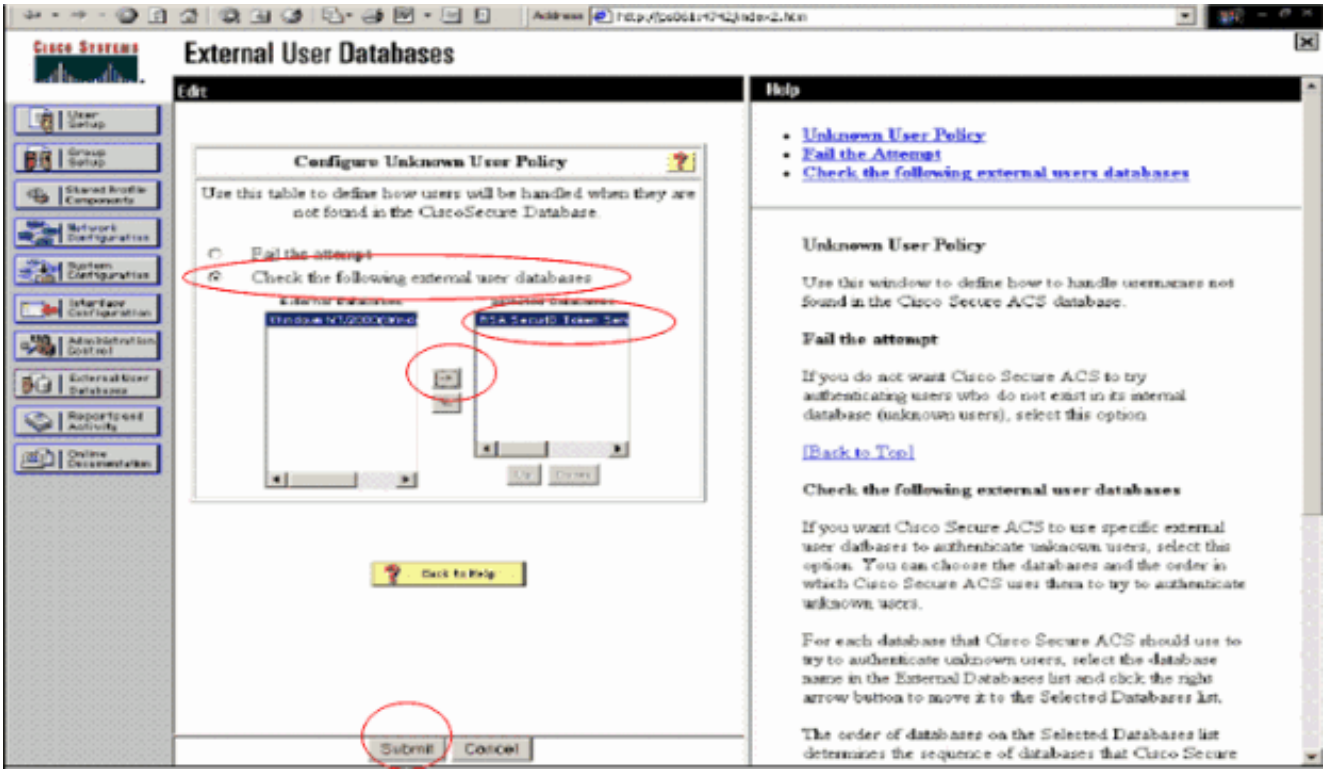


Agregue/autenticación de SecurID de la configuración RSA a su Política de usuario desconocido

Complete estos pasos:

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

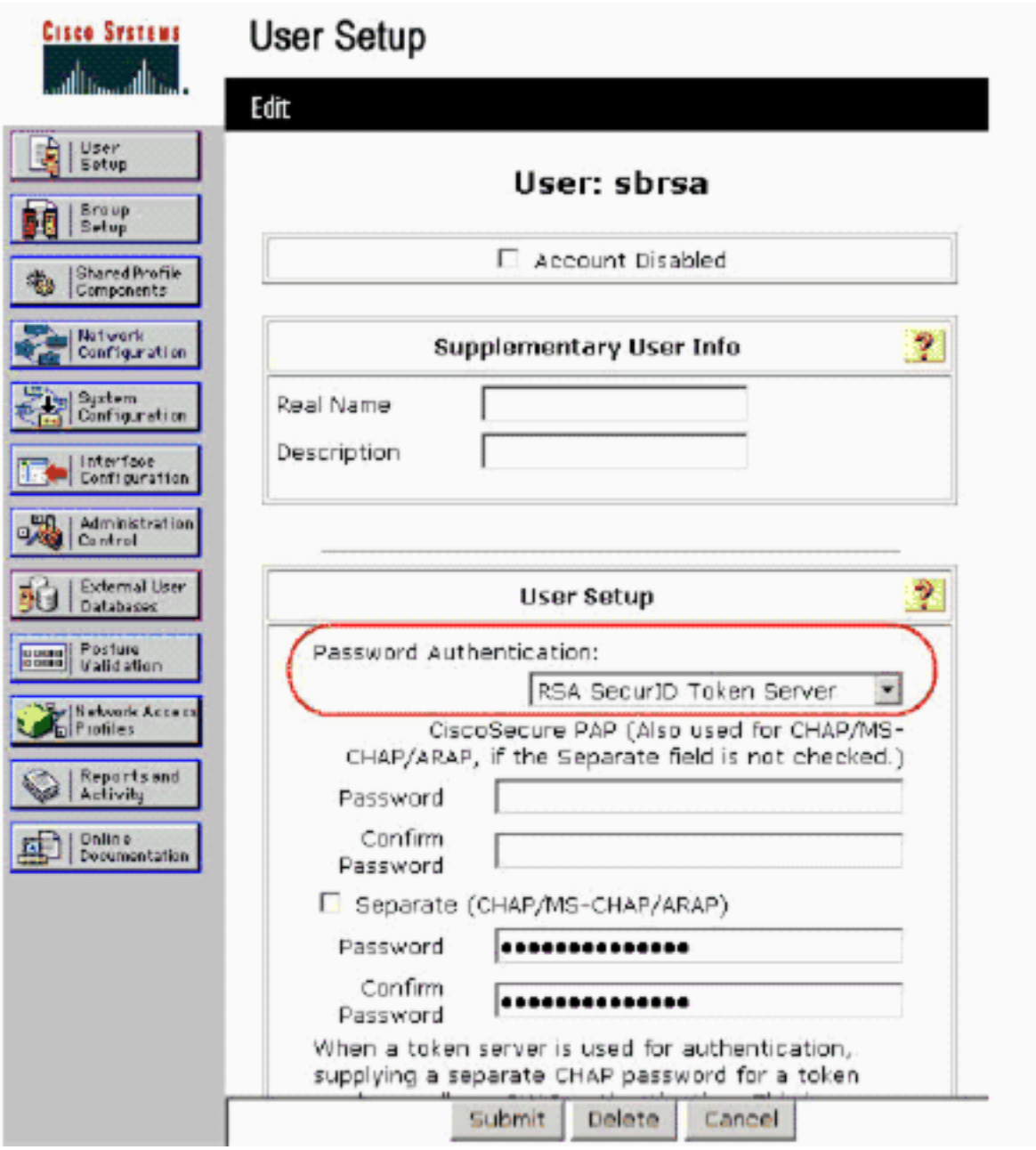
2. En la página de la **Política de usuario desconocido**, el **control** selecto las **Bases de datos de usuarios externas siguientes**, resalta al **servidor Token del SecurID RSA** y lo mueve al cuadro de las bases de datos seleccionadas. Entonces, el tecleo **somete**.



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

Complete estos pasos:

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

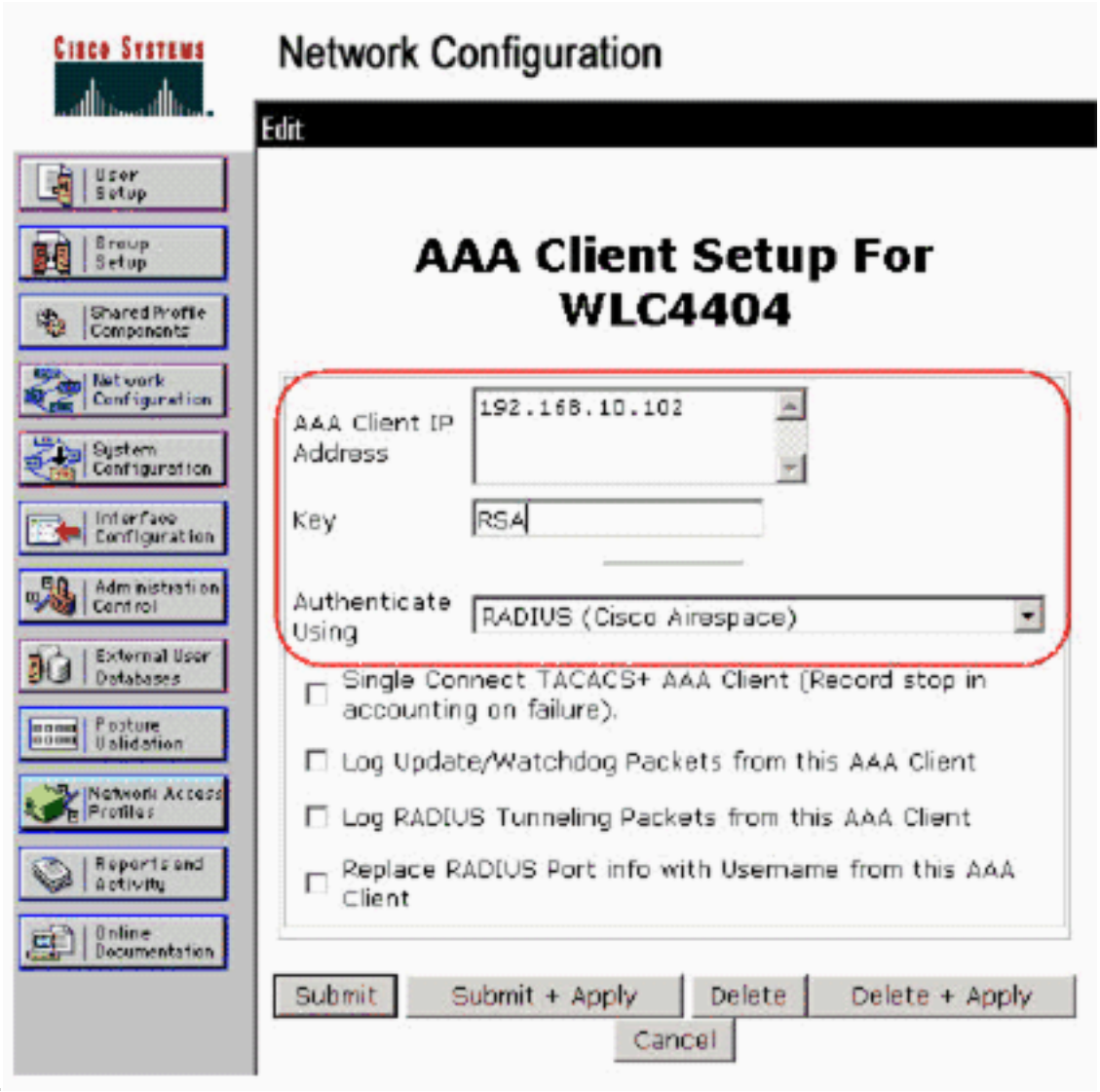


Agregue a un cliente RADIUS en Cisco ACS

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

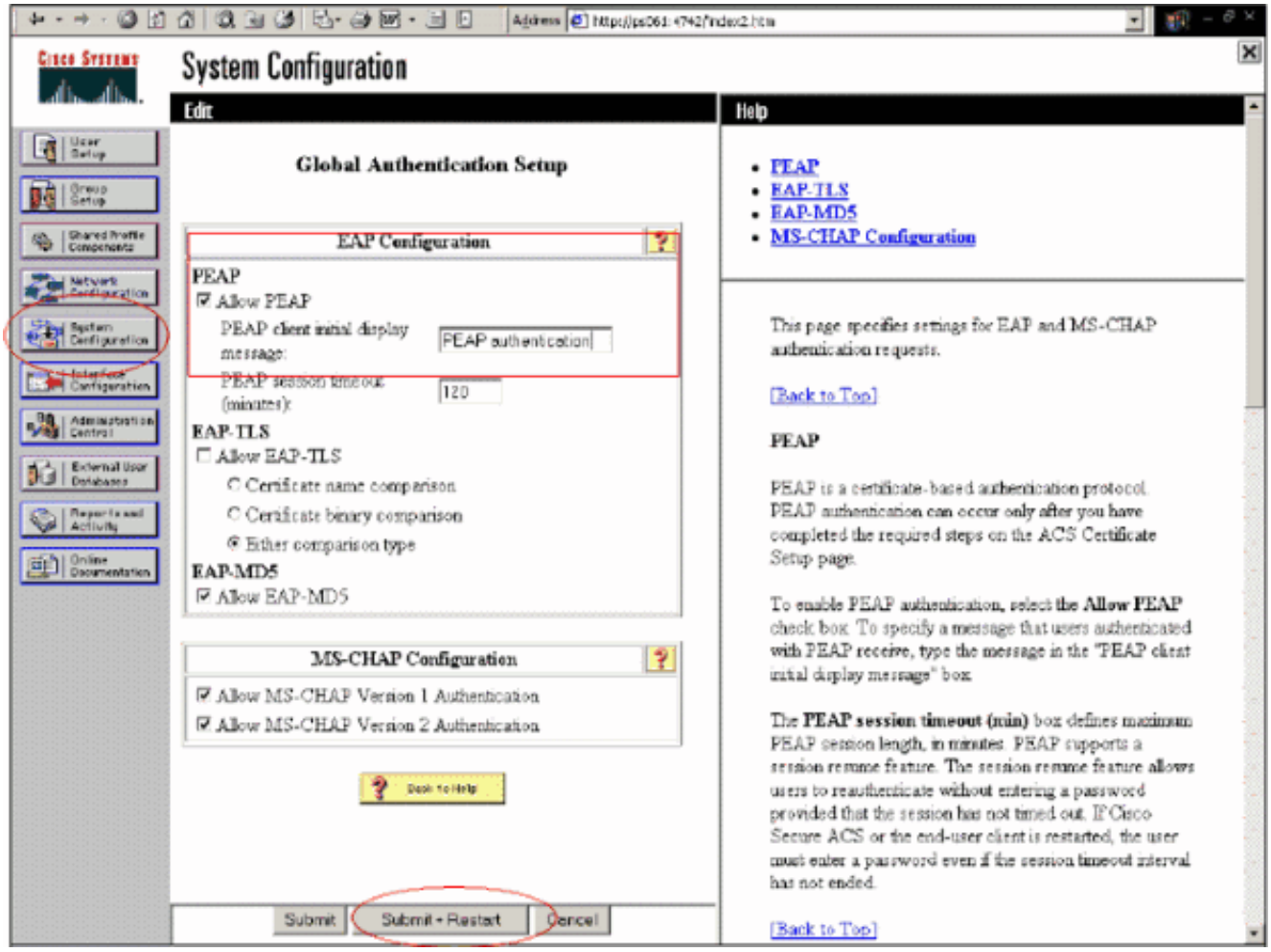
Complete estos pasos:

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



aplica.

2. Solicite y instale un certificado de servidor de un Certificate Authority sabido, de confianza tal como Certificate Authority 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 del Aironet RSA Keon 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 del Cisco Secure ACS en cómo utilizar éstos.
3. Bajo **configuración de la configuración del sistema > de la autenticación global**, marque el checkbox para la **autenticación PEAP**
Allow.



Configure la configuración del controlador LAN de la tecnología inalámbrica 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 el Cisco Secure ACS el servidor.
2. Ingrese el **comando ip-address del auth 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 administrador de la Autenticación RSA, ingrese el IP Address del servidor de RADIUS del administrador de la Autenticación RSA. Cuando usted prueba con el servidor ACS de Cisco, ingrese el IP Address del servidor del Cisco Secure ACS.
3. Ingrese el **comando port del auth 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 administrador y el servidor ACS de Cisco de la Autenticación RSA.
4. Ingrese el **comando secreto del auth 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 del auth del radio de los config del** WLC de habilitar la autenticación. Cuando está deseado, ingrese el **comando disable del auth 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 del auth del radio de la demostración** y **muestre los comandos summary del radio** de verificar que las configuraciones RADIUS están configuradas correctamente.**Nota:** Los temporizadores predeterminados 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 el supplicant de su hardware inalámbrico 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 del pin y los modos siguientes del Tokencode no se soportan al usar esta forma de autenticación con el XP2. (REPARADO como resultado de ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip)
- Si su implementación ACS es más vieja o usted no tiene la corrección antedicha, el cliente no podrá autenticar hasta las transiciones del usuario de “habilitado; El nuevo modo del PIN” a “habilitó”. Usted puede lograr esto teniendo el usuario completa una autenticación de la NON-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 del pin va contra la directiva del 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 indicado otra vez mientras que mostraba al usuario otra vez cuál es la directiva del PIN (por ejemplo, si la directiva del PIN es 5-7 dígitos, con todo el usuario ingresa 4 dígitos).

Información Relacionada

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