SecurID RSA pronto com controladores do Wireless LAN e exemplo de configuração do Cisco Secure ACS

Índice

Introdução

Este documento explica como estabelecer e configurar o protocolo do Access point da leve Cisco (LWAPP) - AP capazes e controladores do Wireless LAN (WLC), assim como o Serviço de controle de acesso Cisco Secure (ACS) a ser usado em um ambiente de WLAN autenticado SecurID RSA. Os guias de execução SecurID-específicos RSA podem ser encontrados em www.rsasecured.com.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento dos WLC e como configurar os parâmetros básicos WLC.
- Conhecimento em como configurar o perfil do cliente do Cisco Wireless usando o utilitário de Desktop de Aironet (ADU).

- Tenha o conhecimento funcional do Cisco Secure ACS.
- Tenha o conhecimento básico do LWAPP.
- Tenha a compreensão básica de serviços do diretório ativo de Microsoft Windows (AD), assim como de controlador de domínio e de conceitos DNS.**Nota:** Antes que você tente esta configuração, assegure-se de que o ACS e o servidor do gerenciador da autenticação de RSA estejam no mesmo domínio e seu relógio de sistema esteja sincronizado exatamente. Se você está usando serviços de Microsoft Windows AD, refira a documentação Microsoft para configurar o servidor do gerenciador ACS e RSA no mesmo domínio. Consulte para configurar o diretório ativo e a base de dados de usuário de Windows para a informação relevante.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Gerente 6.1 da autenticação de RSA
- Agente 6.1 da autenticação de RSA para Microsoft Windows
- Construção 27 do Cisco Secure ACS 4.0(1)**Nota:** O servidor Radius que é incluído pode ser usado no lugar de Cisco ACS. Veja a documentação do RAIO que foi incluída com o gerente da autenticação de RSA em como configurar o server.
- Cisco WLC e Lightweight Access Points para a liberação 4.0 (versão 4.0.155.0)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O sistema do SecurID RSA é uma solução de dois fatoras da autenticação de usuário. Usado conjuntamente com o gerente da autenticação de RSA e um agente da autenticação de RSA, o autenticador do SecurID RSA exige usuários identificar-se que usam um mecanismo de autenticação de dois fatores.

Um é o código do SecurID RSA, um número aleatório gerou cada 60 segundos no dispositivo do autenticador RSA SecureID. O outro é o número de identificação pessoal (PIN).

Os autenticadores do SecurID RSA são tão simples de usar quanto incorporando uma senha. Cada utilizador final é atribuído um autenticador do SecurID RSA que gerencia um código do um-tempo-uso. Ao entrar, o usuário incorpora simplesmente este número e um PIN do segredo a ser autenticado com sucesso. Como um benefício adicionado, tokens do hardware do SecurID RSA PRE-é programado geralmente para ser inteiramente - funcional em cima do recibo.

Esta demonstração instantânea explica como usar um dispositivo do autenticador do secureID RSA: Programa demonstrativo RSA.

Com o direito da autenticação securid do apoio RSA do programa pronto do SecurID RSA, dos server de Cisco WLC e do Cisco Secure ACS fora da caixa. O agente de software da autenticação de RSA intercepta pedidos do acesso, se local ou telecontrole, dos usuários (ou dos grupos de usuários) e dirige-os ao programa do gerente da autenticação de RSA para a autenticação.

O software de gerenciador da autenticação de RSA é o componente de gerenciamento da solução do SecurID RSA. É usado para verificar pedidos de autenticação e para administrar centralmente políticas de autenticação para redes de empreendimento. Trabalha conjuntamente com autenticadores do SecurID RSA e agente de software da autenticação de RSA.

Neste documento, um servidor ACS Cisco é usado como o agente da autenticação de RSA instalando o agente de software nele. O WLC é o servidor do acesso de rede (NAS) (cliente de AAA) que por sua vez para a frente as authenticações do cliente ao ACS. O documento demonstra os conceitos e a instalação usando a authenticação do cliente protegida do protocolo extensible authentication (PEAP).

A fim aprender sobre a autenticação de PEAP, refira Cisco protegeu o protocolo extensible authentication.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Este documento utiliza as seguintes configurações:

- Configuração do host do agente
- Configuração de Agente de Autenticação

Configuração do host do agente

Usando o Cisco Secure ACS como o servidor Radius

A fim facilitar uma comunicação entre o Cisco Secure ACS e o dispositivo do SecurID do gerente da autenticação de RSA/RSA, um registro do host do agente deve ser adicionado ao base de dados de gerenciador da autenticação de RSA. O registro do host do agente identifica o Cisco Secure ACS dentro de seu base de dados e contém a informação sobre uma comunicação e a criptografia.

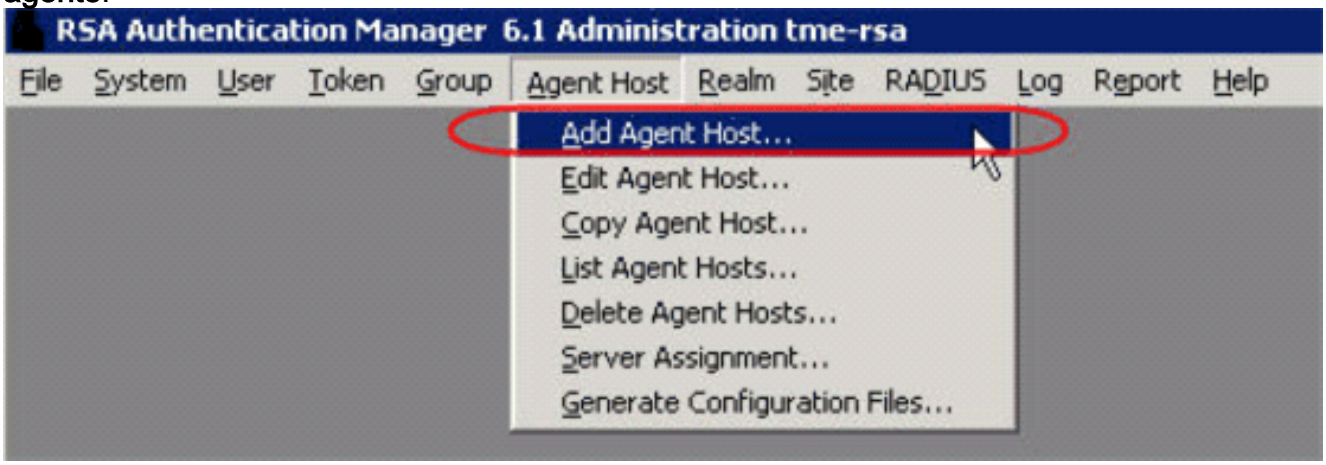
A fim criar o registro do host do agente, você precisa esta informação:

- Hostname do servidor ACS Cisco
- Endereços IP de Um ou Mais Servidores Cisco ICM NT para todas as interfaces de rede do servidor ACS Cisco

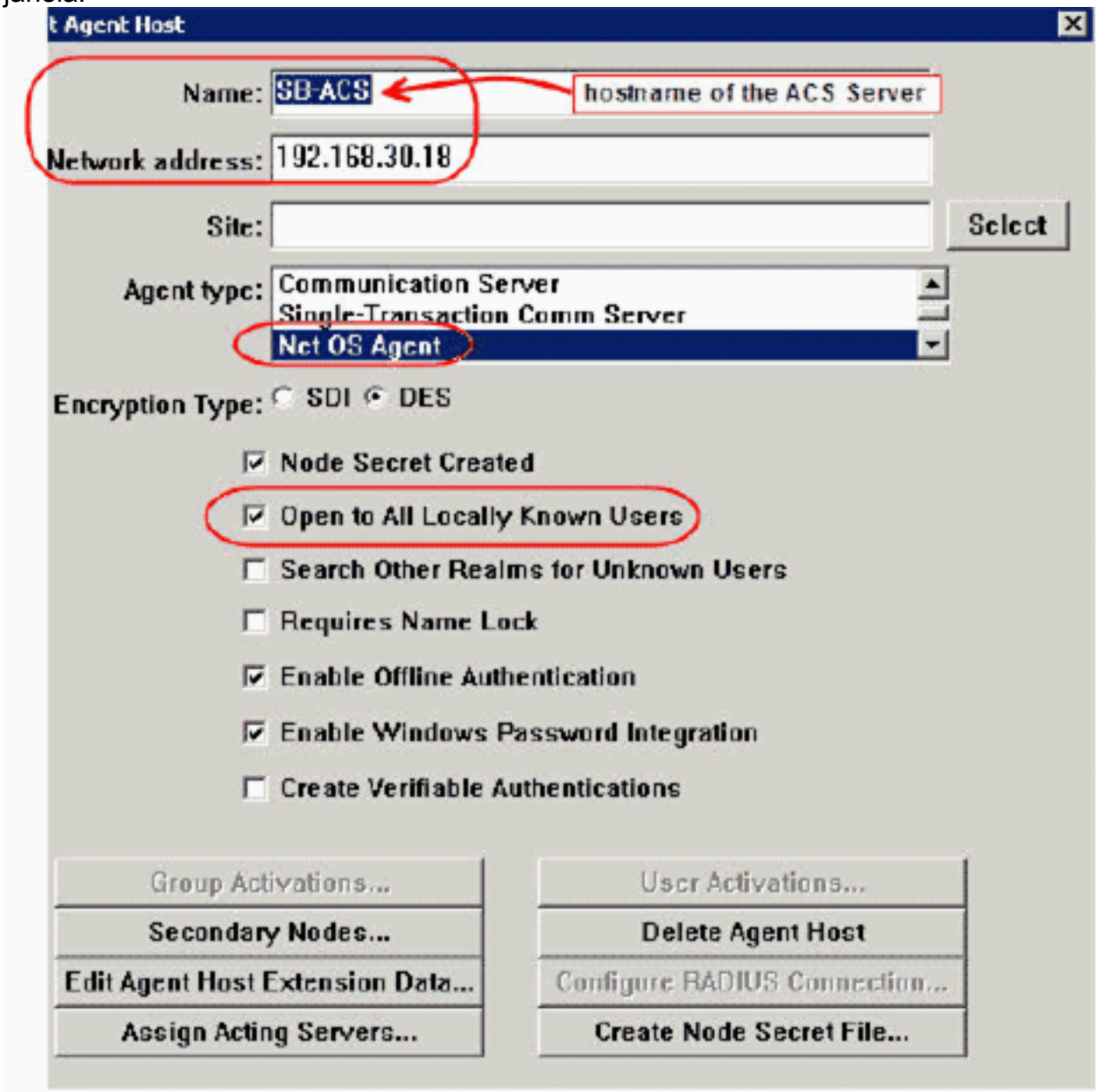
Conclua estes passos:

1. Abra o aplicativo do modo do host do gerente da autenticação de RSA.
2. Selecione o **host de agente > adicionar host de**

agente.



Você verá esta janela.



3. Incorpore a informação apropriada para o nome e o endereço de rede de servidor ACS Cisco. Escolha **NetOS** para o tipo do agente e verifique a caixa de seleção para ver se há **Open a todos os usuários localmente conhecidos**.
4. Clique em **OK**.

Usando o servidor Radius do gerente 6.1 da autenticação de RSA

A fim facilitar uma comunicação entre Cisco WLC e gerente da autenticação de RSA, um registro do host do agente deve ser adicionado ao base de dados de gerenciador e à base de dados do servidor radius da autenticação de RSA. O registro do host do agente identifica Cisco WLC dentro de seu base de dados e contém a informação sobre uma comunicação e a criptografia.

A fim criar o registro do host do agente, você precisa esta informação:

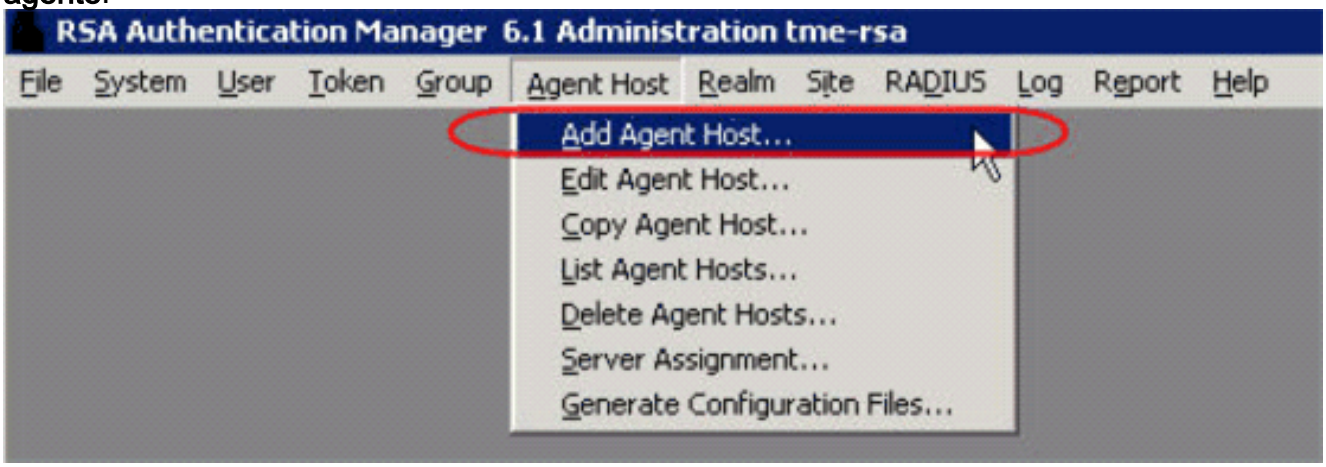
- O hostname do WLC
- Endereços IP de gerenciamento do WLC
- Segredo do RAIO, que deve combinar o segredo do RAIO em Cisco WLC

Ao adicionar o registro do host do agente, o papel do WLC é configurado como um servidor de comunicação. Este ajuste é usado pelo gerente da autenticação de RSA para determinar como uma comunicação com o WLC ocorrerá.

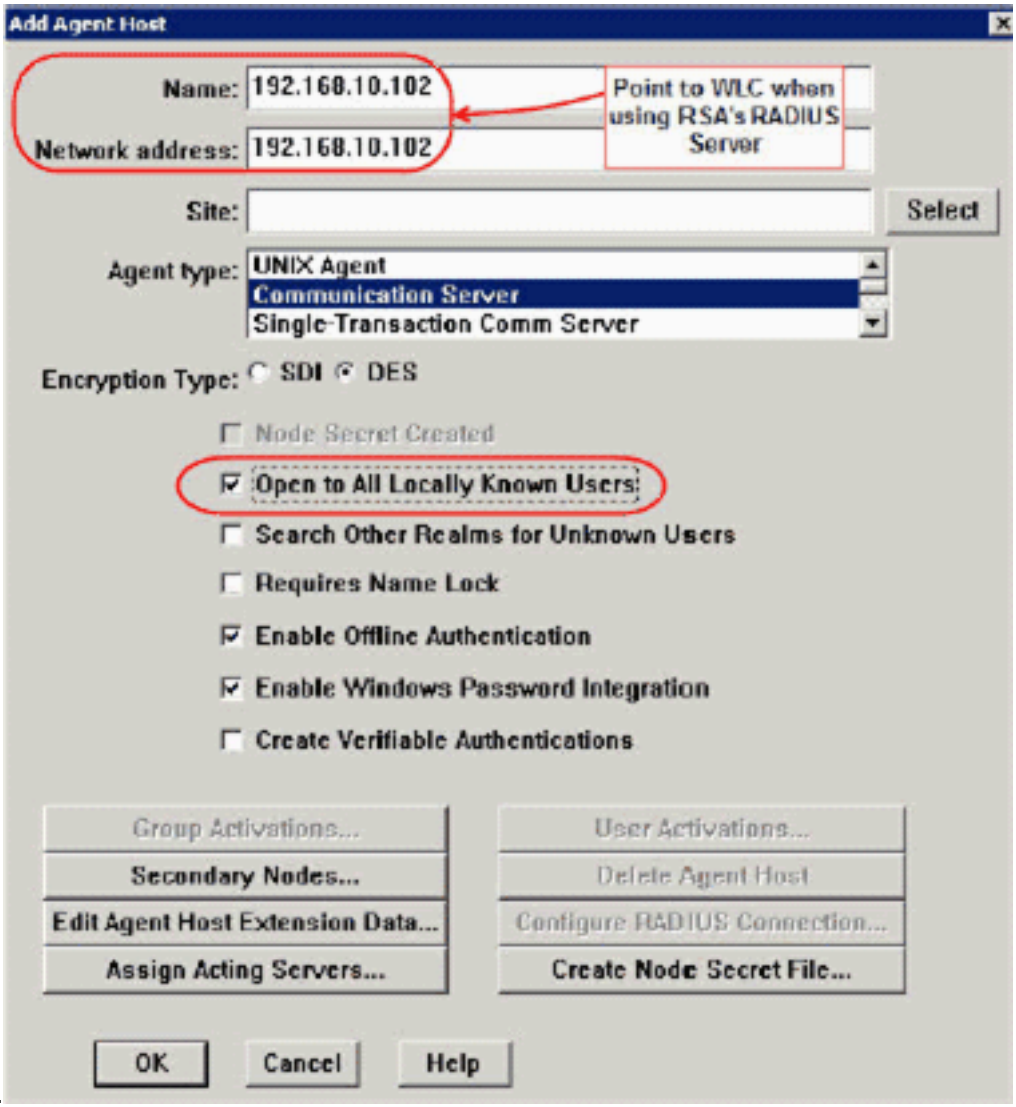
Nota: Os nomes de host dentro do dispositivo do SecurID do gerente da autenticação de RSA/RSA devem resolver aos endereços IP válidos na rede local.

Conclua estes passos:

1. Abra o aplicativo do modo do host do gerente da autenticação de RSA.
2. Selecione o **host de agente > adicionar host de agente**.

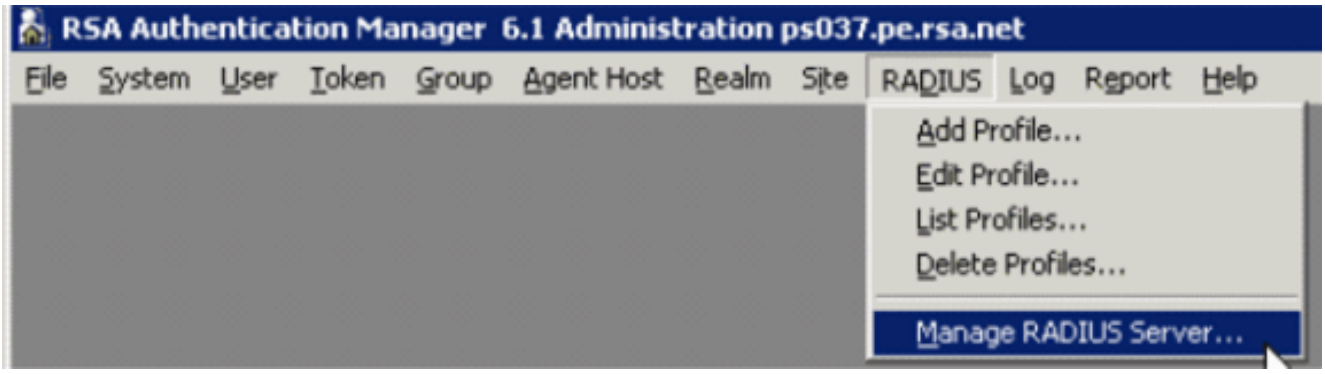


Você verá esta



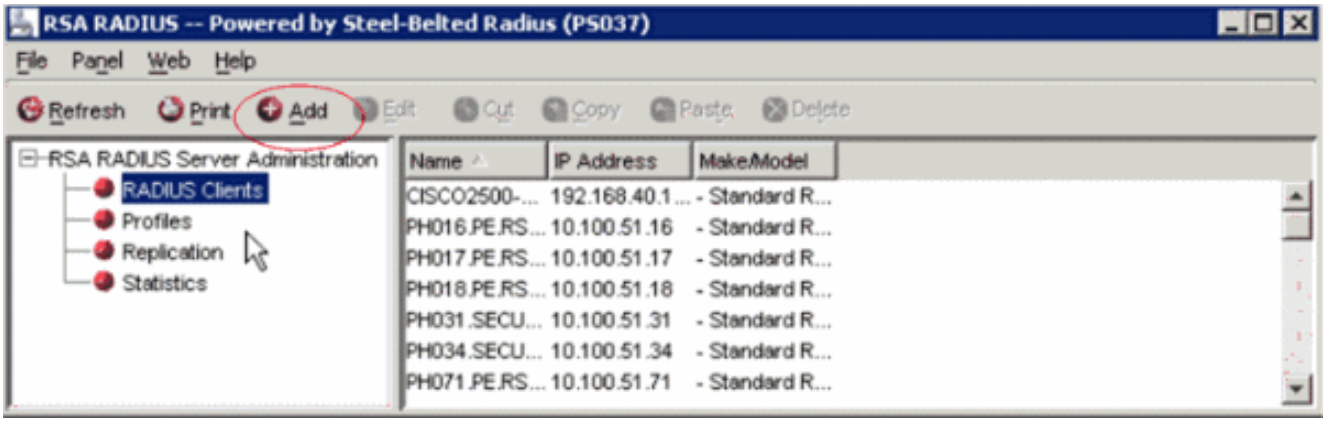
janela.

3. Incorpore a informação apropriada para o hostname WLC (um FQDN do pode ser resolvido, caso necessário) e o endereço de rede. Escolha o **servidor de comunicação** para o tipo do agente e verifique a caixa de seleção para ver se há **Open a todos os usuários localmente conhecidos**.
4. Clique em **OK**.
5. Do menu, o **RAIO** seleto > **controla o servidor Radius**.

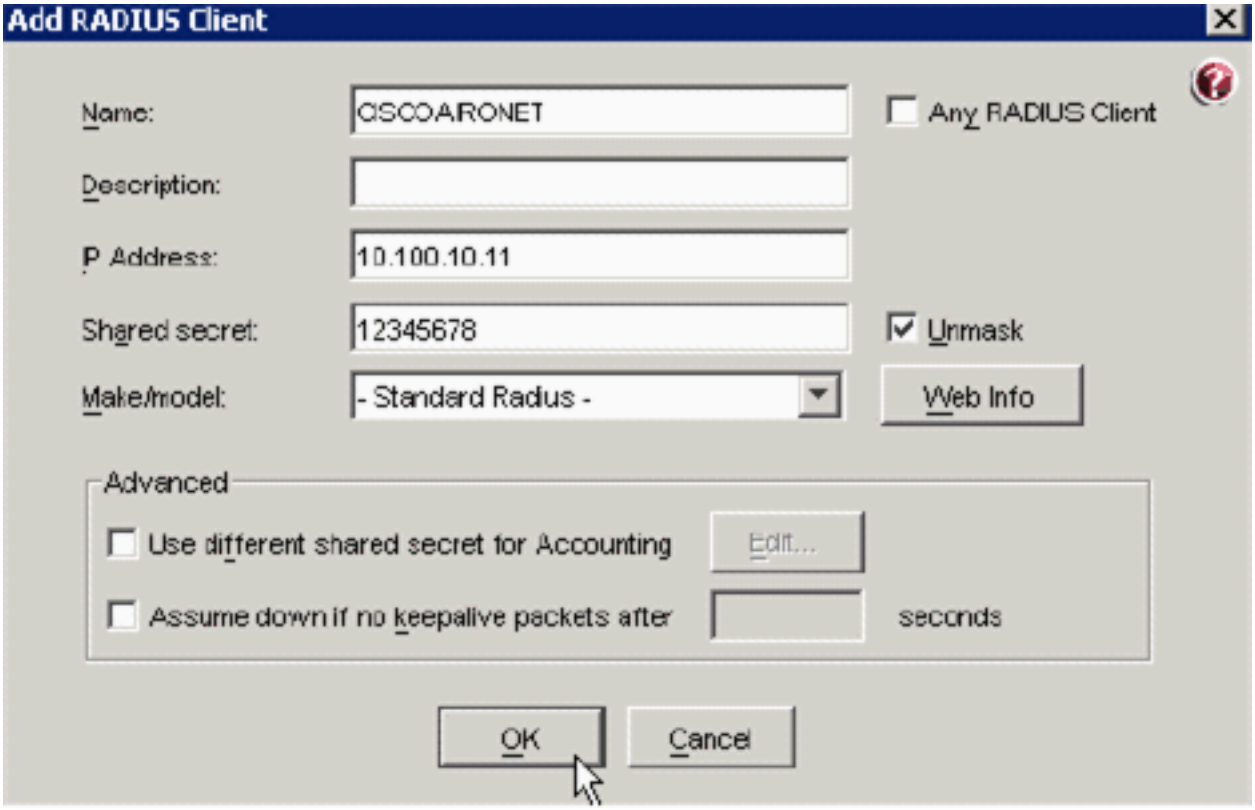


Uma janela Administração nova abre.

6. Neste indicador, os **clientes RADIUS** seletos, clicam então **adicionam**.



7. Incorpore a informação apropriada para Cisco WLC. O segredo compartilhado deve combinar o segredo compartilhado definido em Cisco WLC.



8. Clique em **OK**.

Configuração de Agente de Autenticação

Esta tabela representa a funcionalidade do agente da autenticação de RSA do 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

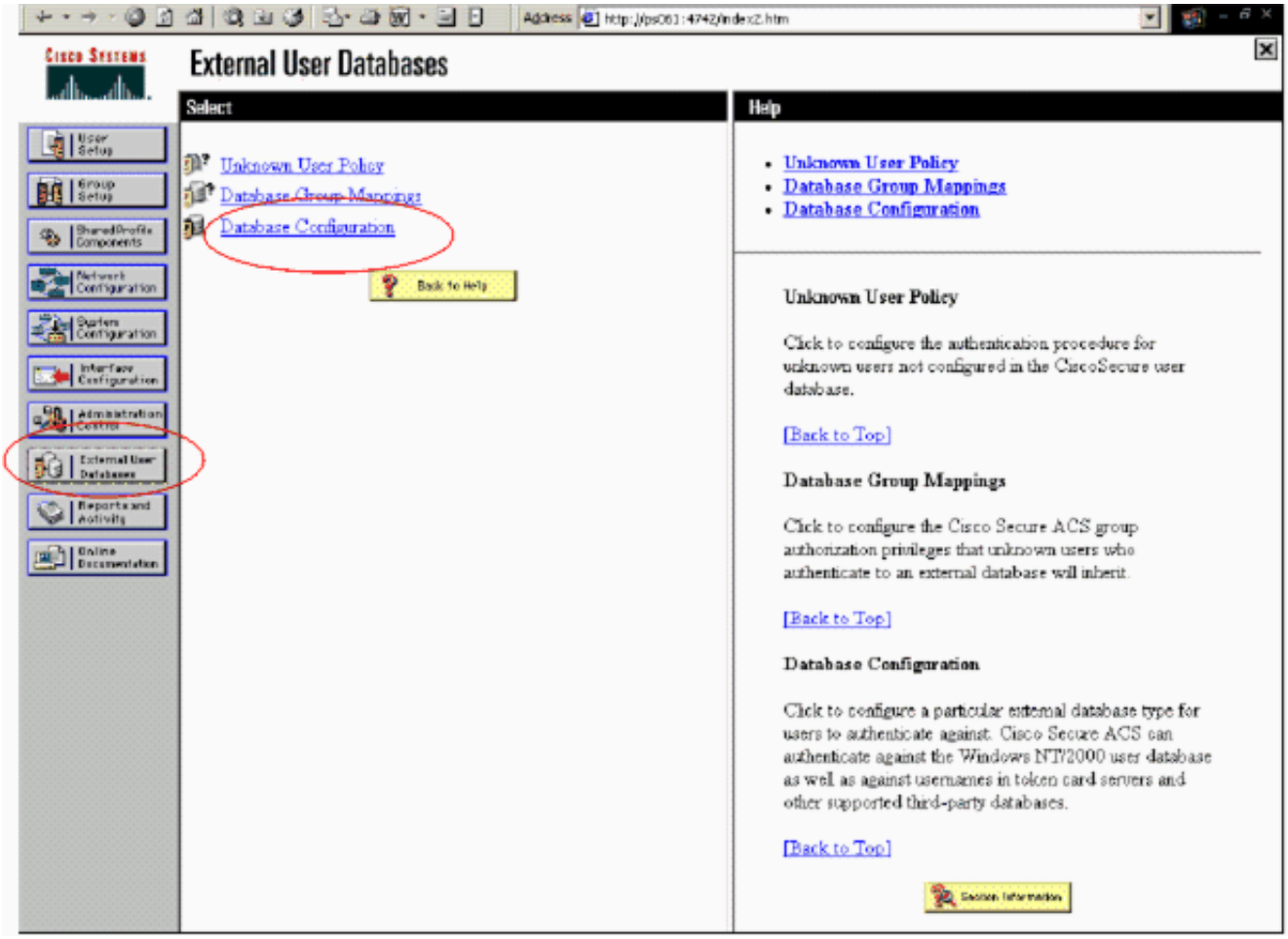
Nota: Veja a documentação do RAIO que esteve incluída com o gerente da autenticação de RSA em como configurar o servidor Radius, se aquele é o servidor Radius que estará usado.

Configurar Cisco ACS

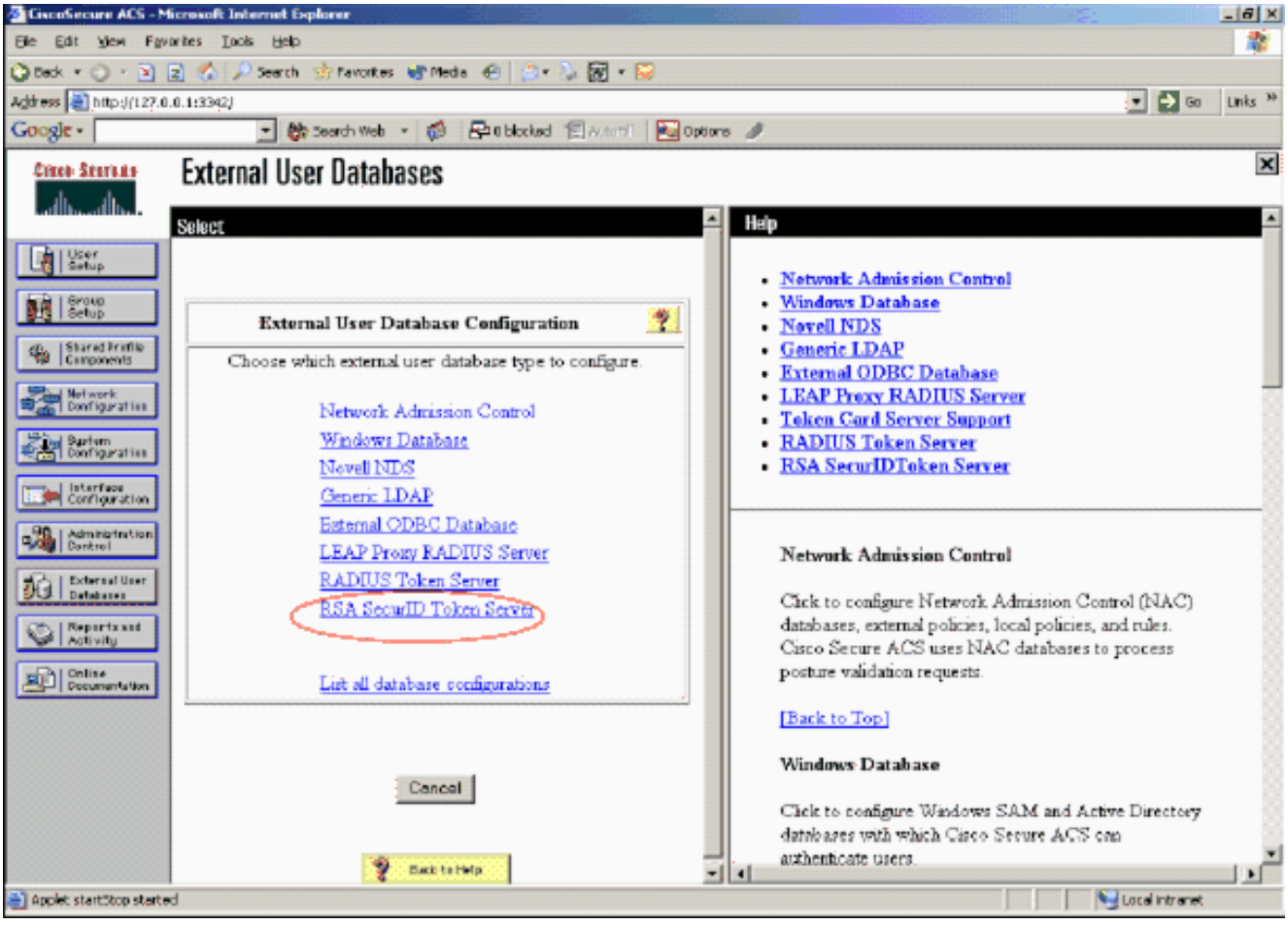
Ative a autenticação securid RSA

Autenticação securid dos apoios RSA do Cisco Secure ACS dos usuários. Termine estas etapas a fim configurar o Cisco Secure ACS para autenticar usuários com gerente 6.1 da autenticação:

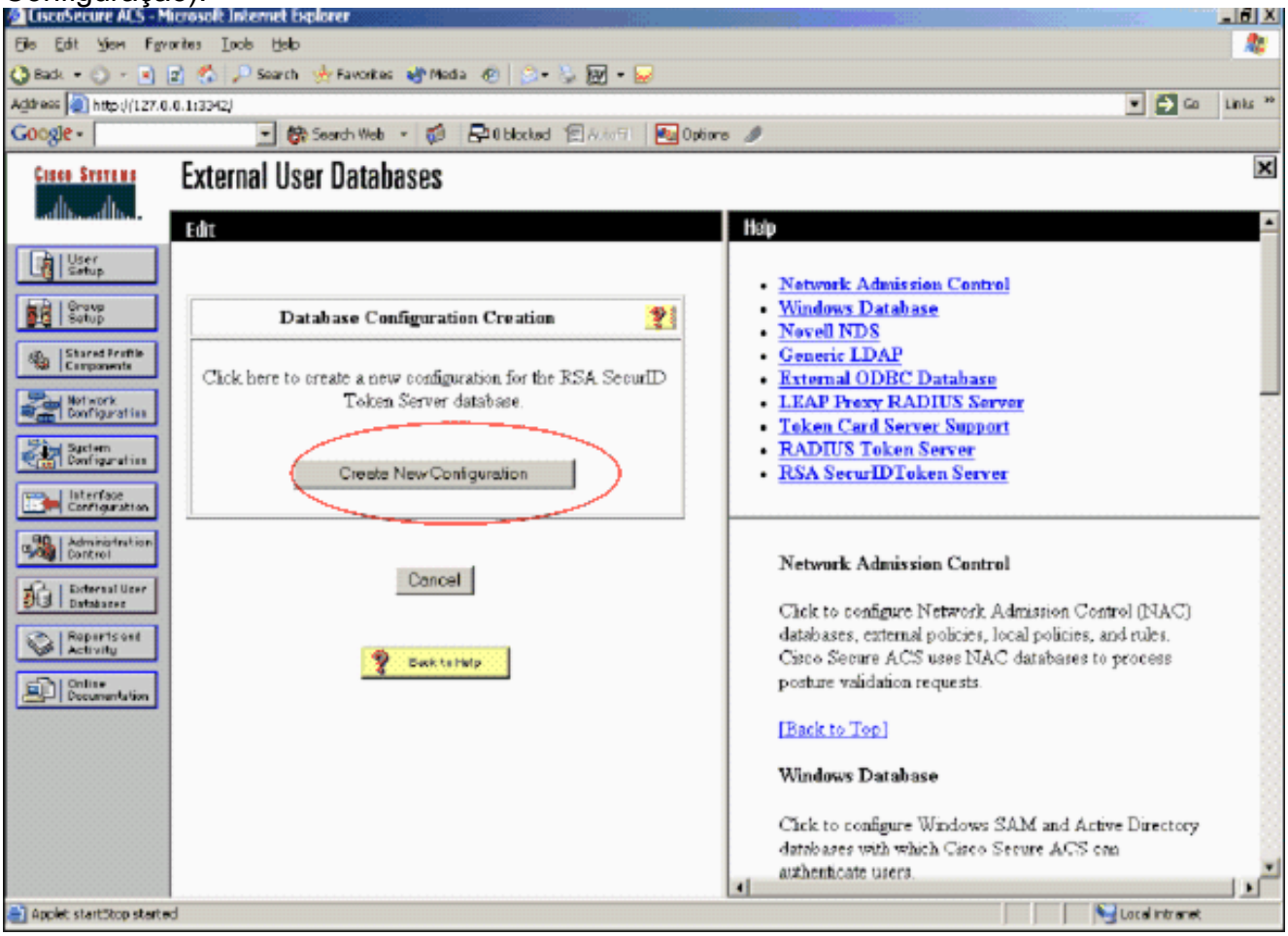
1. Instale o agente 5.6 da autenticação de RSA ou mais atrasado para Windows no mesmo sistema que o server do Cisco Secure ACS.
2. Verifique a Conectividade executando a função da autenticação de teste do Agente de Autenticação.
3. Copie o arquivo aceclnt.dll do **gerente da Segurança \ autenticação de RSA de** c:\Program Files\RSA do server RSA **\ diretório do prog ao diretório de** c:\WINNT\system32 do servidor ACS.
4. Na barra de navegação, clique a **base de dados de usuário externo**. Então, **configuração do base de dados do** clique na página do base de dados externo.



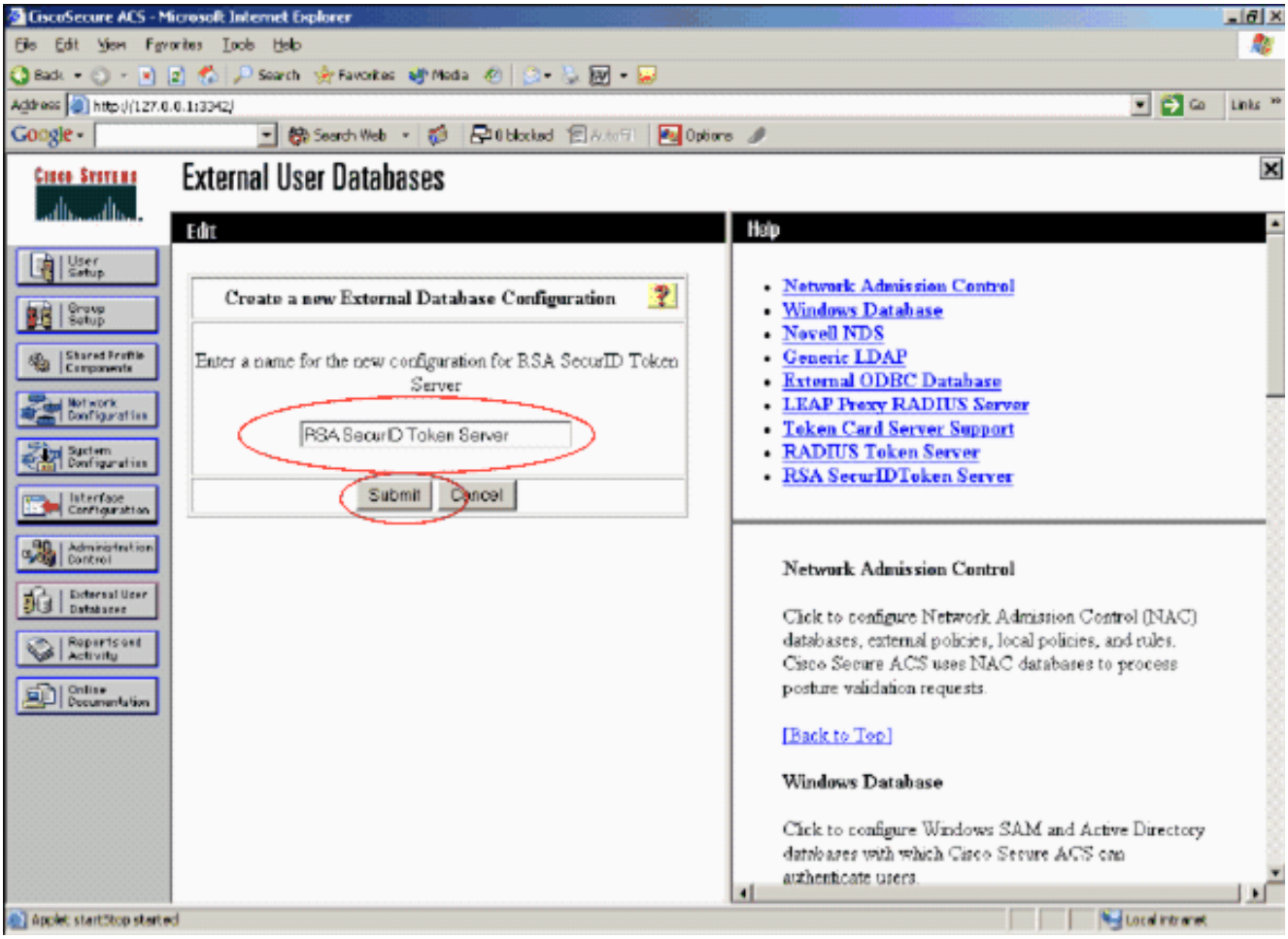
5. Na página da configuração externa de bando de dados de usuário, **servidor de tokens do SecurID do** clique
RSA.



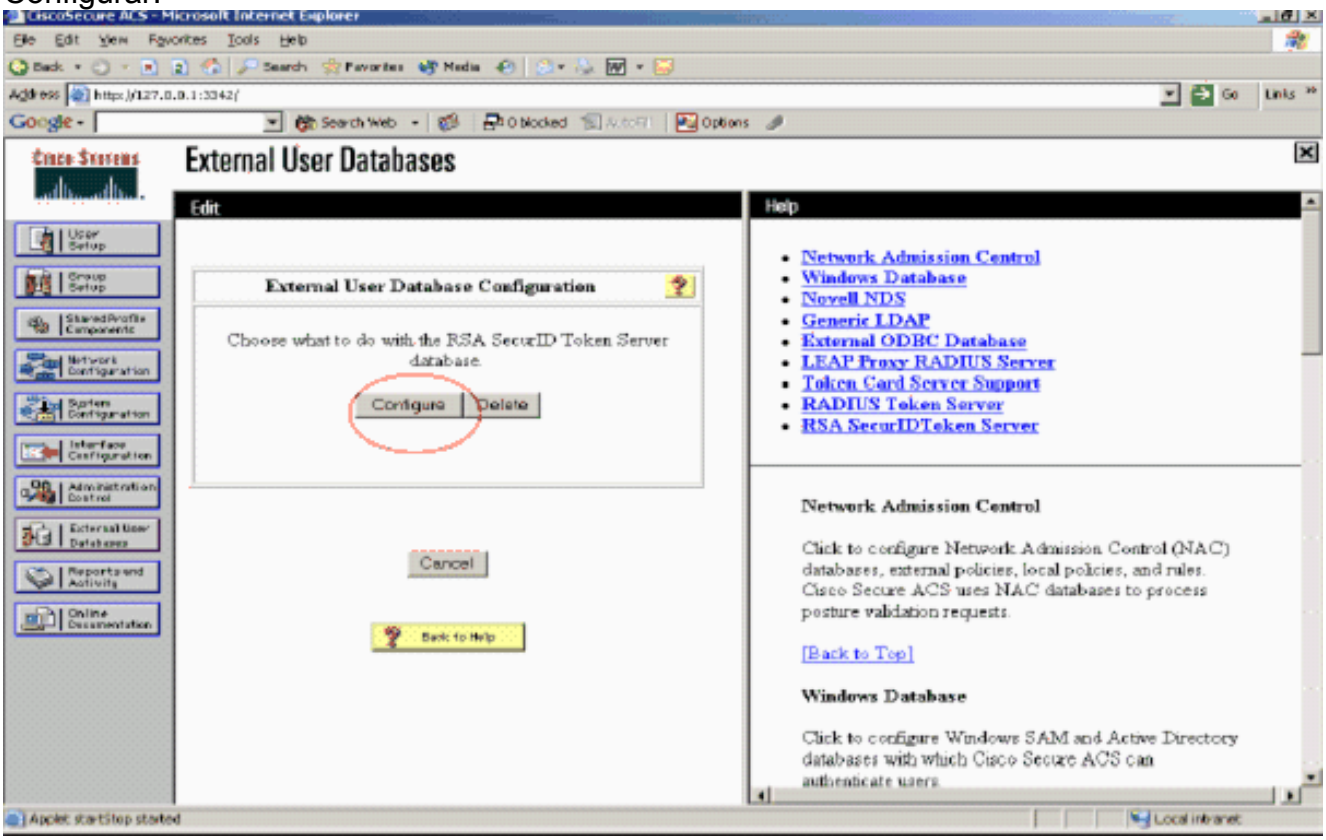
6. Clique em Create New Configuration (Criar Nova Configuração).



7. Dê entrada com um nome, a seguir clique-o **submetem-se**.

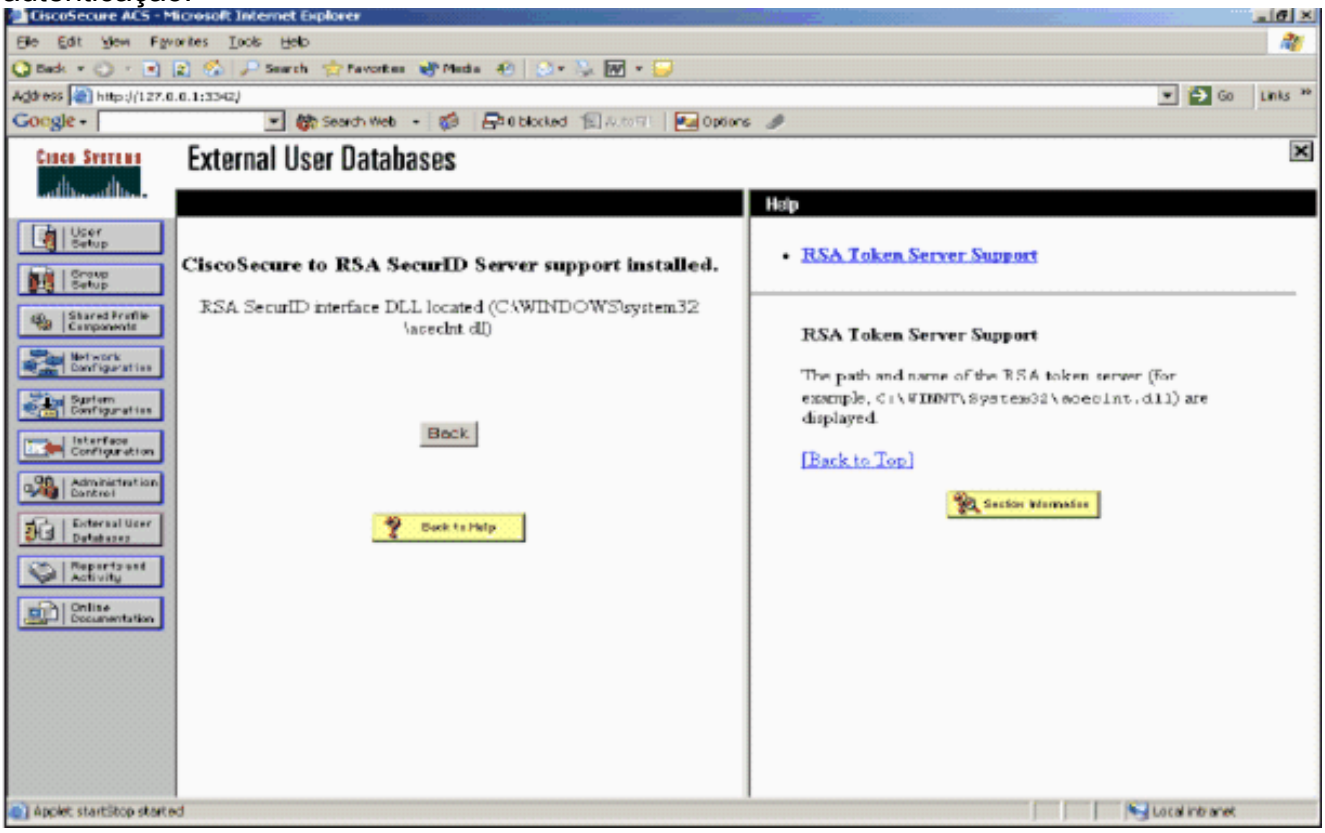


8. Clique em Configurar.



O Cisco Secure ACS indica o nome do servidor de tokens e do trajeto ao autenticador DLL. Esta informação confirma que o Cisco Secure ACS pode contactar o agente da autenticação de RSA. Você pode adicionar a base de dados de usuário externo do SecurID RSA a sua política de usuário desconhecida ou atribuir contas de usuário específicas para usar este

base de dados para
autenticação.

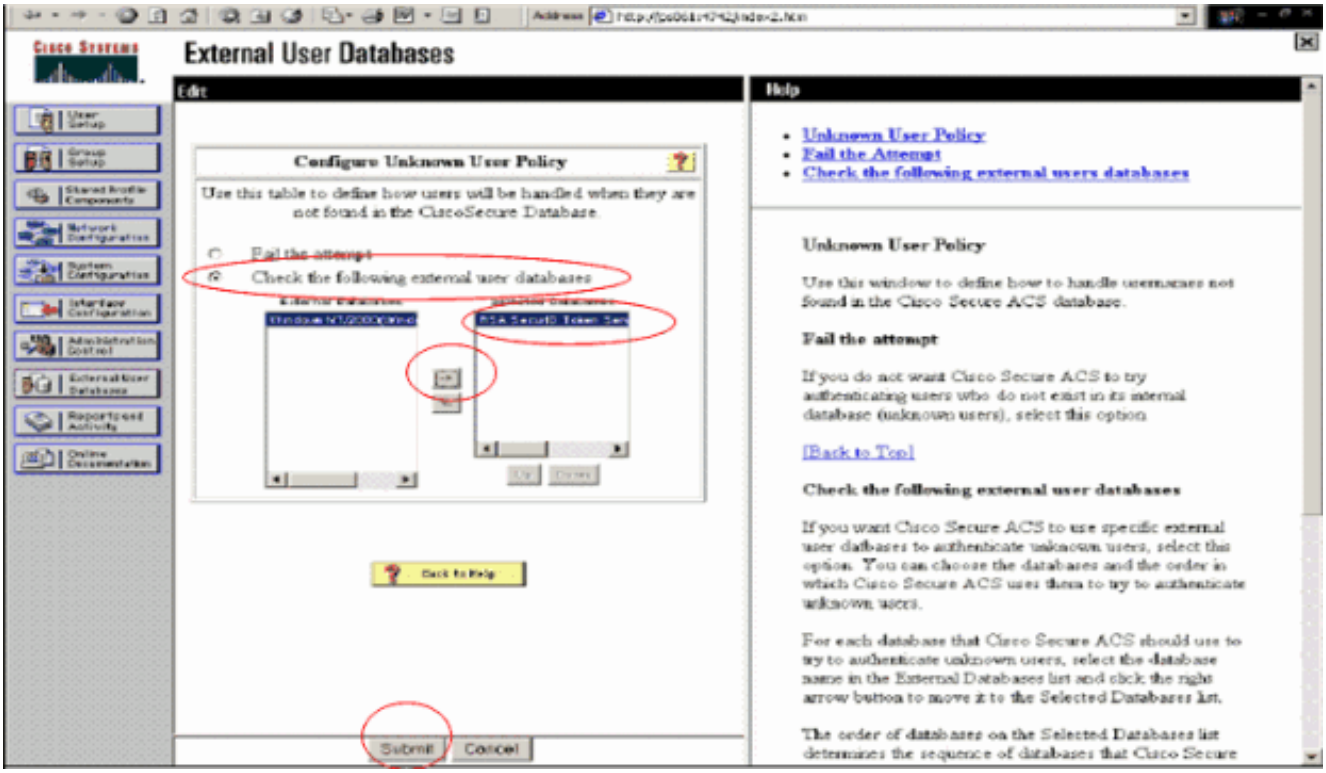


Adicionar/configurar a autenticação securid RSA a sua política de usuário desconhecida

Conclua estes passos:

1. Na barra de navegação ACS, clique a **base de dados de usuário externo** > a **política de usuário**
desconhecida.

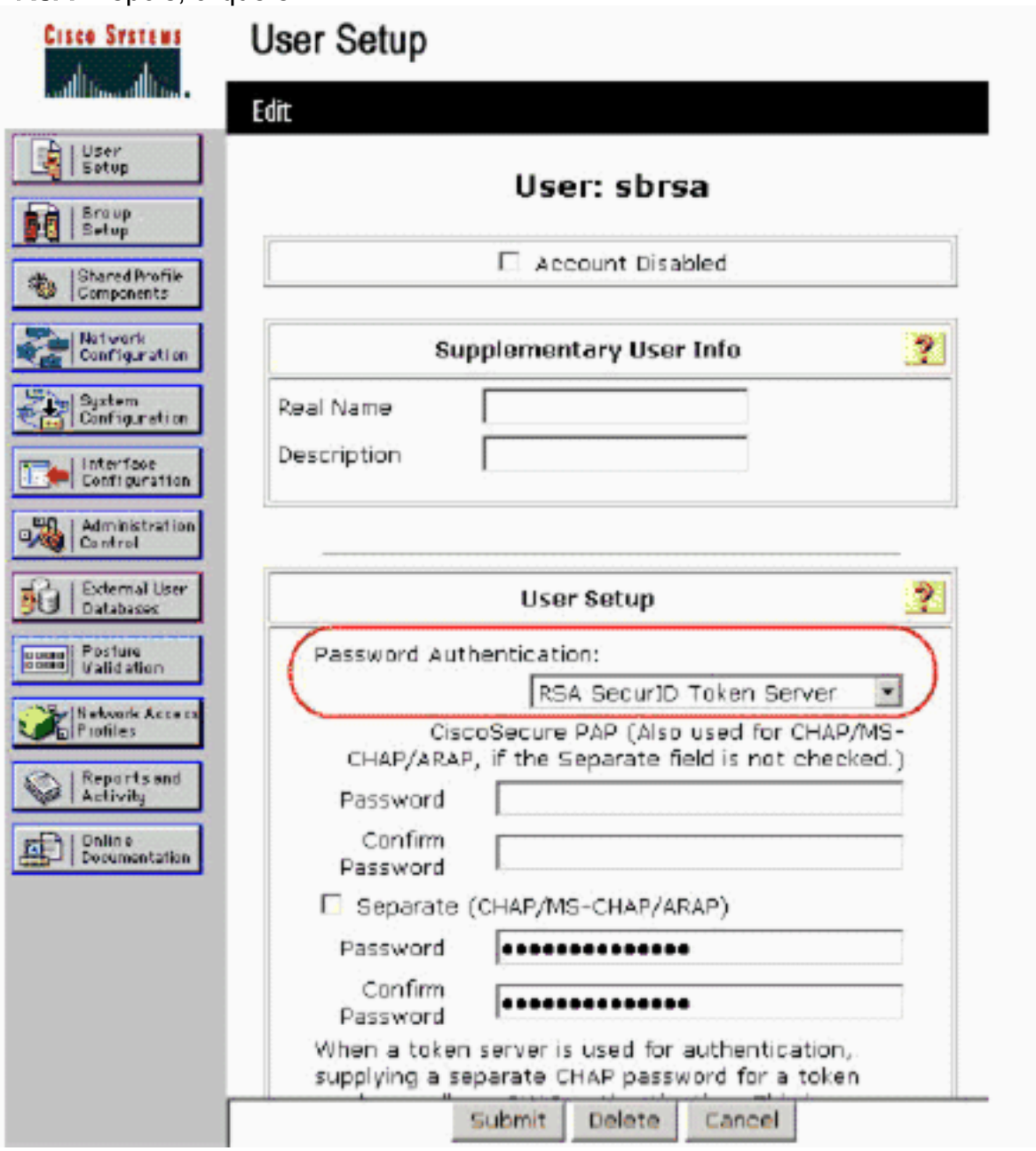
2. Na página da **política de usuário desconhecida**, a **verificação** seleta as **seguintes bases de dados de usuário externo**, destaca o **servidor de tokens do SecurID RSA** e move-o para a caixa dos bases de dados selecionado. Depois, clique em **Submit**.



Adicionar/configurar a autenticação securid RSA para contas de usuário específicas

Conclua estes passos:

1. Clique a **instalação de usuário do** ACS principal Admin GUI. Incorpore o username e o clique **adicionam** (ou selecione um usuário que existente você deseja alterar).
2. Sob a instalação de usuário > a autenticação de senha, escolha o **servidor de tokens do SecurID RSA**. Depois, clique em **Submit**.

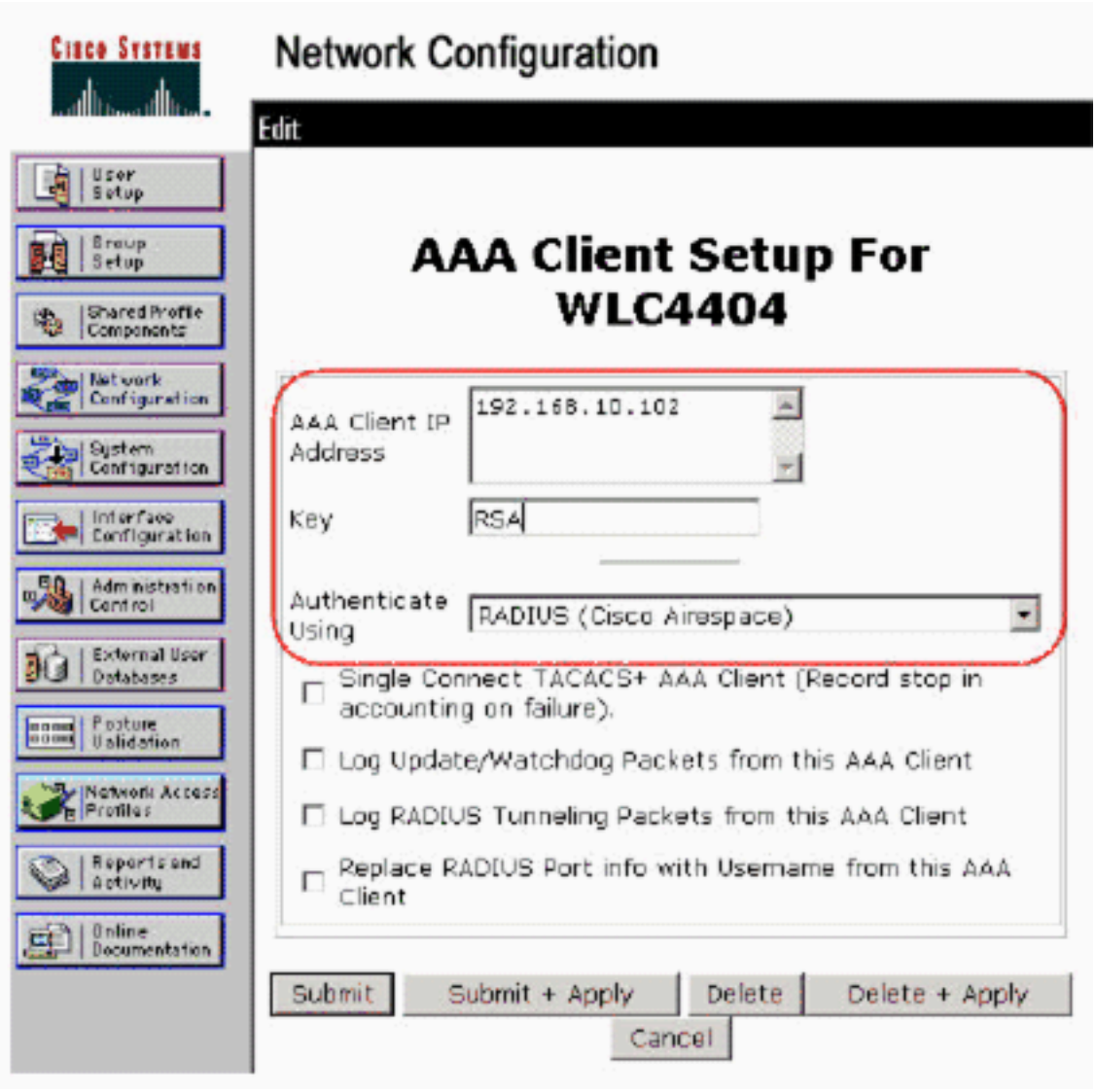


[Adicionar um cliente RADIUS em Cisco ACS]

O servidor ACS Cisco instala precisará os endereços IP de Um ou Mais Servidores Cisco ICM NT do WLC de servir como um NAS para enviar autenticações de PEAP do cliente ao ACS.

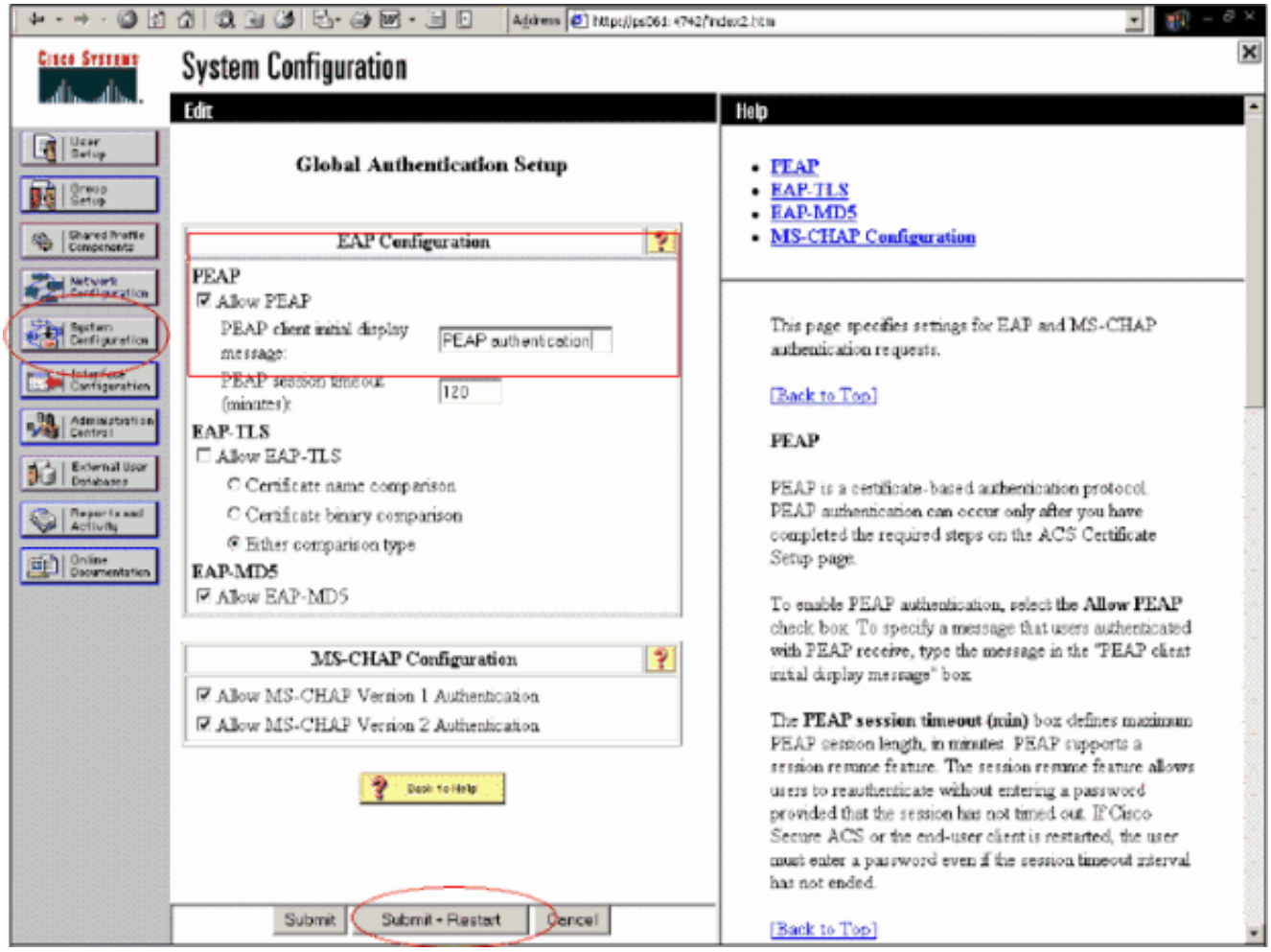
Conclua estes passos:

1. Sob a **configuração de rede**, adicionar/edite o cliente de AAA para o WLC que será usado. Incorpore a chave “secreta” compartilhada (comum ao WLC) que é usada entre o cliente de AAA e o ACS. Seleto **autentique usando-se > RAIO (Cisco Airespace)** para este cliente de AAA. Então, o clique **submete-se + aplica-**



se.

2. Aplique para e instale um certificado de servidor de um Certificate Authority conhecido, confiado tal como o Certificate Authority RSA Keon.Para obter mais informações sobre deste processo, refira a documentação que envia com Cisco ACS. Se você está usando o gerenciador certificado RSA, você pode ver o guia de execução RSA Keon Aironet para a ajuda adicional. Você deve com sucesso terminar esta tarefa antes que você continue.**Nota:** Os certificados auto-assinados podem igualmente ser usados. Refira a documentação do Cisco Secure ACS em como usar estes.
3. Sob a **instalação da configuração de sistema > da autenticação global**, verifique a caixa de seleção para ver se há a **autenticação de PEAP**
Allow.



Configurar a configuração do controlador de LAN do Cisco Wireless para o 802.1x

Conclua estes passos:

1. Conecte à interface da linha de comando do WLC para configurar o controlador assim que pode ser configurado para conectar ao Cisco Secure ACS o server.
2. Inscreva o **comando ip-address do AUTH do raio da configuração do** WLC configurar um servidor Radius para a autenticação.**Nota:** Quando você testa com o servidor Radius do gerente da autenticação de RSA, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius do gerente da autenticação de RSA. Quando você testa com o servidor ACS Cisco, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do server do Cisco Secure ACS.
3. Inscreva o **comando port do AUTH do raio da configuração do** WLC especificar a porta UDP para a autenticação. As portas 1645 ou 1812 são ativas à revelia no gerente e no servidor ACS Cisco da autenticação de RSA.
4. Inscreva o **comando secreto do AUTH do raio da configuração do** WLC configurar o segredo compartilhado no WLC. Isto deve combinar o segredo compartilhado criado nos servidores Radius para este cliente RADIUS.
5. Inscreva o **comando enable do AUTH do raio da configuração do** WLC permitir a autenticação. Quando desejado, inscreva o **comando disable do AUTH do raio da configuração** desabilitar a autenticação. Note que a autenticação está desabilitada à revelia.
6. Selecione a opção de segurança apropriada da camada 2 para o WLAN desejado no WLC.
7. Use as **estatísticas do AUTH do raio da mostra** e **mostre comandos summary do raio** verificar que os ajustes do RAIO estão configurados corretamente.**Nota:** Os temporizadores

padrão para o Pedido-intervalo EAP são baixos e puderam precisar de ser alterado. Isto pode ser feito usando o comando **avançado configuração do** *<seconds> do pedido*-**intervalo do eap**. Pôde igualmente ajudar à emenda que o intervalo do pedido da identidade baseou nas exigências. Isto pode ser feito usando o comando **avançado configuração do** *<seconds> do identidade-pedido*-**intervalo do eap**.

Configuração de cliente Wireless do 802.11

Para uma explicação detalhada de como configurar seu suplicante wireless do hardware e do cliente, refira a vária Documentação da Cisco.

Problemas conhecidos

Estes são algumas das edições conhecidas com autenticação RSA SecureID:

- Token de software RSA. O modo novo Pin e os modos seguintes de Código Token não são apoiados ao usar este formulário de autenticação com XP2. (FIXADO em consequência de ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip)
- Se sua aplicação ACS é mais velha ou você não tem a correção de programa acima, o cliente não pôde autenticar até que as transições do usuário de “permitiram; Modo novo PIN” “ao permitido”. Você pode realizar este tendo o usuário termina uma autenticação do NON-Sem fio, ou usando o aplicativo RSA da “autenticação de teste”.
- Negue 4 dígitos/pinos alfanuméricos. Se um usuário no modo novo Pin vai contra a política PIN, o processo de autenticação falha, e o usuário é inconsciente de como ou de porque. Tipicamente, se um usuário vai contra a política, serão enviados a uma mensagem que o PIN esteve rejeitado e para ser alertado outra vez ao mostrar ao usuário outra vez qual a política PIN é (por exemplo, se a política PIN é 5-7 dígitos, contudo o usuário incorpora 4 dígitos).

Informações Relacionadas

- Atribuição do VLAN dinâmico com os WLC baseados no ACS ao exemplo de configuração do mapeamento do grupo do diretório ativo
- Cliente VPN sobre LAN Wireless com Exemplo de Configuração de WLC
- Autenticação em exemplos de configuração dos controladores do Wireless LAN
- Autenticação EAP-FAST com exemplo de configuração dos controladores e do servidor de raio externo do Wireless LAN
- Tipos do autenticação wireless em ISR fixo com o exemplo da configuração de SDM
- Tipos do autenticação wireless em um exemplo de configuração fixo ISR
- Cisco protegeu o protocolo extensible authentication
- Autenticação de EAP com servidor RADIUS
- Suporte Técnico e Documentação - Cisco Systems