>RSA SecurID就绪与无线局域网控制器和Cisco安全ACS配置示例

目录

简介

本文解释如何设立和配置思科轻量级接入点用于RSA SecurID验证的WLAN环境(ACS)的协议(LWAPP) -有能力AP和无线局域网控制器(WLCs)，以及思科安全访问控制服务器。RSA SecurID特定实施指南可以在www.rsasecured.com找到。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- WLCs知识和如何配置WLC基本参数。
- 使用Aironet Desktop软件(ADU)，关于怎样的知识配置Cisco无线客户端的配置文件。
- 有Cisco Secure ACS功能知识。
- 有LWAPP基础知识。
- 有Microsoft Windows激活目录(AD)服务、以及域控制器和DNS概念基本的了解。**注意：** 在您尝试此配置前，请保证ACS和RSA验证管理器服务器在同一个域，并且他们的系统时钟正确地同步。如果使用Microsoft Windows AD服务，参考Microsoft文档配置在同一个域的ACS和

RSA管理器服务器。参考请配置活动目录和Windows用户数据库相关信息的。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- RSA验证管理器6.1
- RSA Microsoft Windows的验证代理程序6.1
- Cisco Secure ACS 4.0(1)构建27**注意：** 包括的RADIUS服务器可以在Cisco ACS位置使用。请参阅包括与关于怎样的RSA验证管理器配置服务器的RADIUS文档。
- 思科WLCs和轻量级接入点版本的4.0 (版本4.0.155.0)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

RSA SecurID系统是二要素用户认证解决方案。使用二要素验证机制，使用与RSA验证管理器和RSA验证代理程序一道， RSA SecurID验证器要求用户识别。

一个是RSA SecurID代码，随机数生成在RSA SecureID验证器设备的每60秒。其他是Personal identification number (PIN)。

RSA SecurID证明人是一样方便操作象输入密码。生成一时间使用代码的每最终用户分配RSA SecurID验证器。当注册时，用户输入此编号和PIN顺利地验证的机密。一个已添加好处， RSA SecurID硬件令牌通常被预编程序功能完备的在收据。

此闪存演示解释如何使用RSA secureID验证器设备：RSA演示。

通过RSA SecurID就绪程序、思科WLCs和Cisco Secure ACS服务器支持RSA SecurID验证权利箱外。RSA验证代理软件截住访问请求，本地或远程，从用户的用户(或组)和是否处理他们对RSA验证管理器程序验证的。

RSA验证管理器软件是RSA SecurID解决方案的管理组件。它用于验证认证请求和在中央管理企业网络的验证策略。它与RSA SecurID证明人和RSA验证代理软件一道工作。

在本文中， Cisco ACS服务器使用作为RSA验证代理程序通过安装对此的代理软件。WLC是反过来寄客户端验证给ACS的网络接入服务器(NAS) (AAA客户端)。使用Protected Extensible Authentication Protocol (PEAP)客户端验证，本文展示概念和设置。

为了得知PEAP验证，参考思科保护的可扩展的认证协议。

配置

本部分提供有关如何配置本文档所述功能的信息。

本文档使用以下配置：

- 代理主机配置
- 验证代理配置

代理主机配置

使用Cisco Secure ACS作为RADIUS服务器

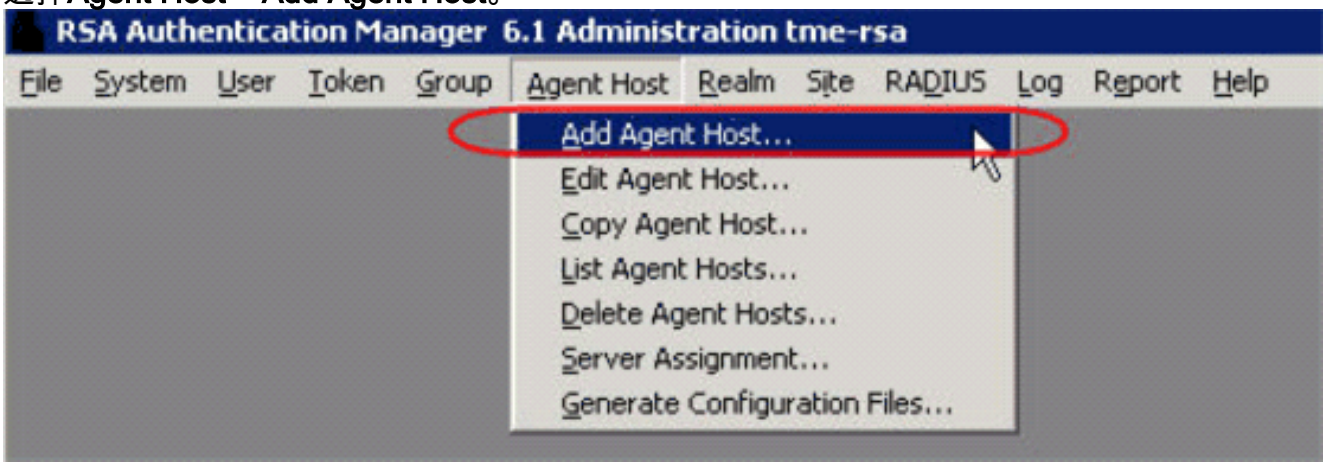
为了实现Cisco Secure ACS和RSA验证管理器/RSA SecurID设备之间的通信，必须添加代理主机记录到RSA验证管理器数据库。代理主机记录识别在其数据库内的Cisco Secure ACS并且包含关于通信和加密的信息。

为了创建代理主机记录，您需要此信息：

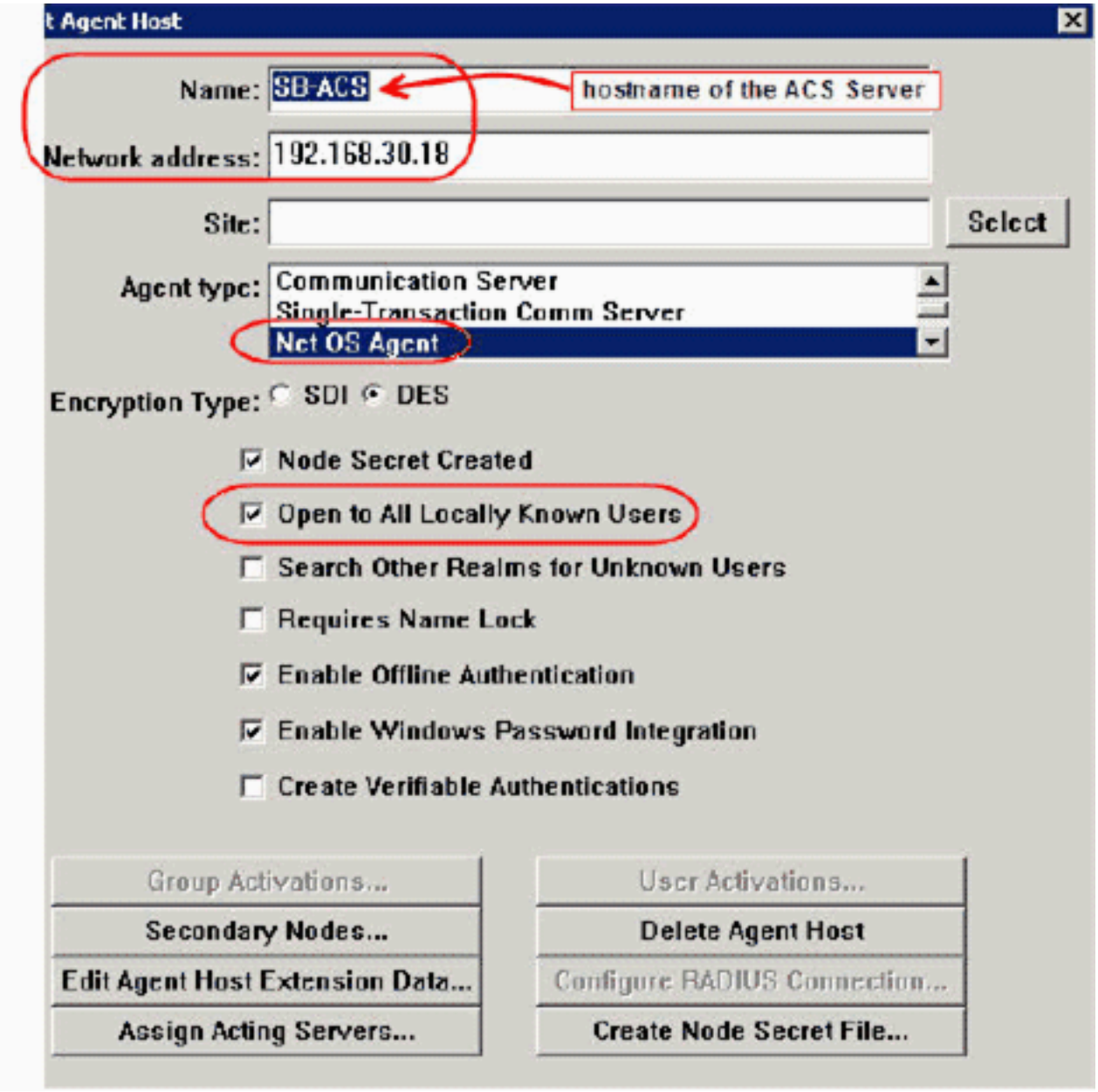
- Cisco ACS服务器的主机名
- Cisco ACS服务器的所有网络接口的IP地址

完成这些步骤：

1. 打开RSA验证管理器主机模式应用程序。
2. 选择**Agent Host > Add Agent Host**。



您看见此窗口



:

3. 进入Cisco ACS服务器名称和网络地址的相应的信息。选择代理程序类型的**NetOS**并且检查复选框**对所有本地已知用户的Open**。
4. 单击 **Ok**。

使用RSA验证管理器6.1 RADIUS服务器

为了实现思科WLC和RSA验证管理器之间的通信，必须添加代理主机记录到RSA验证管理器数据库和RADIUS服务器数据库。代理主机记录识别在其数据库内的思科WLC并且包含关于通信和加密的信息。

为了创建代理主机记录，您需要此信息：

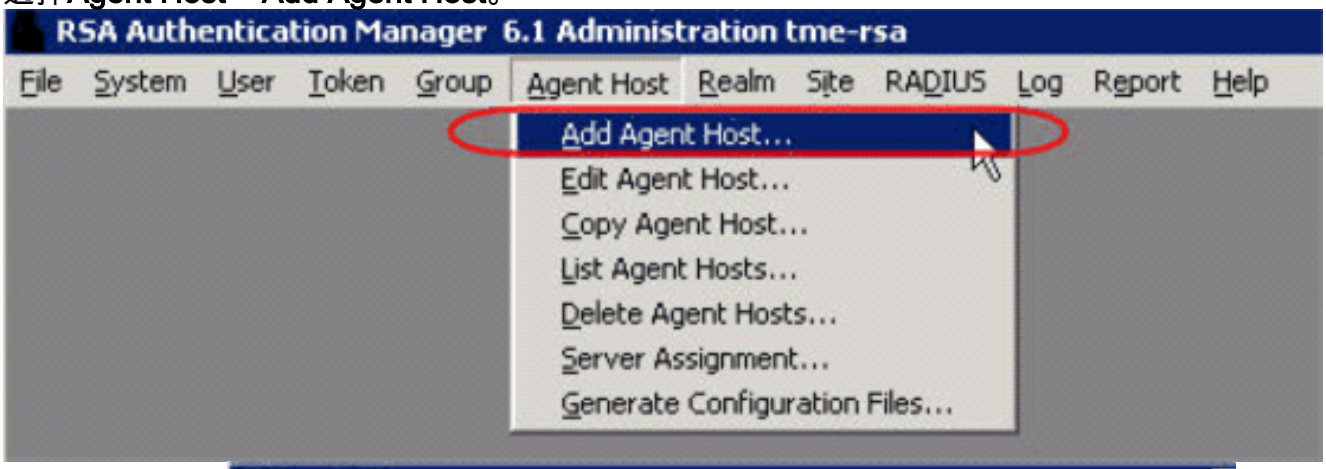
- WLC's主机名
- WLC的管理IP地址
- RADIUS机密，必须匹配在思科WLC的RADIUS机密

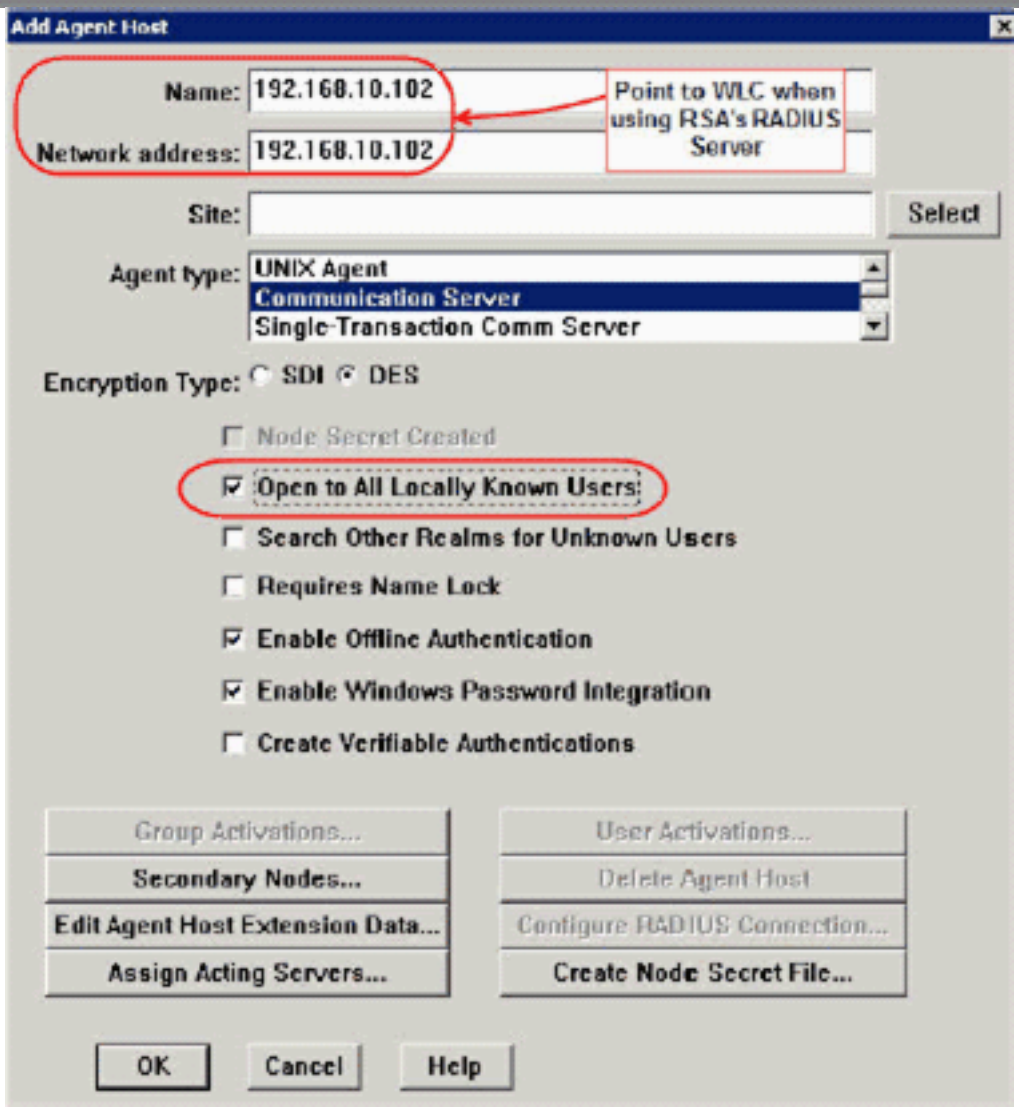
当添加代理主机记录时， WLC's角色配置作为通信服务器。RSA验证管理器用于此设置确定与WLC的通信如何将发生。

注意： 在RSA验证管理器/RSA SecurID设备内的主机名必须解决到在本地网络的有效IP地址。

完成这些步骤：

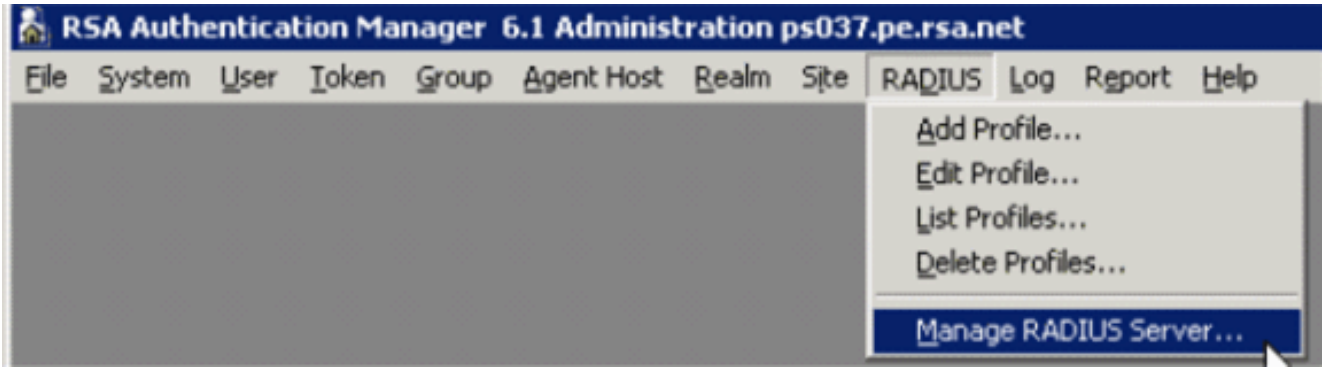
1. 打开RSA验证管理器主机模式应用程序。
2. 选择**Agent Host > Add Agent Host**。





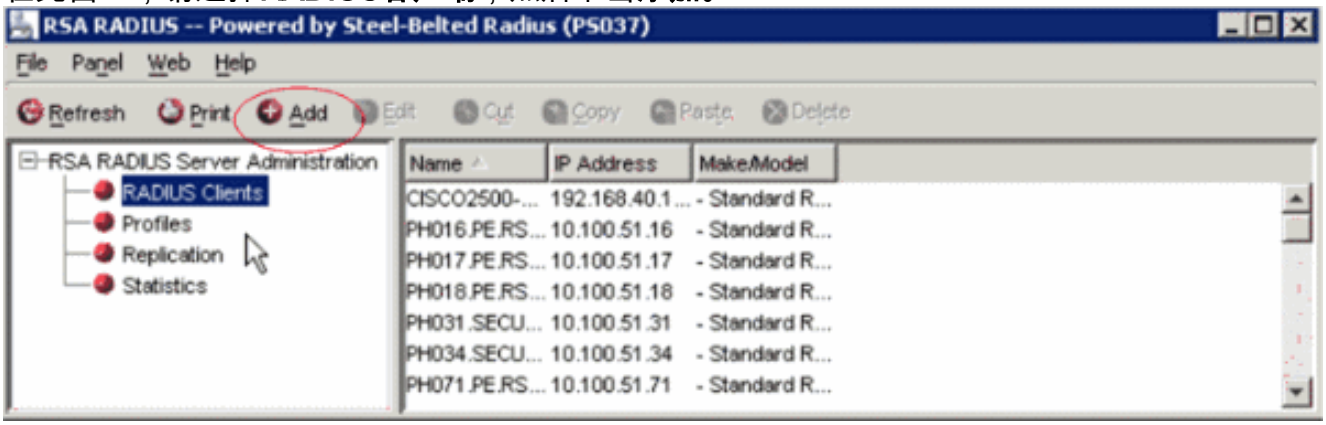
您看见此窗口：

3. 进入WLC主机名(可解决FQDN，如果需要)和网络地址的相应的信息。选择代理程序类型的**通信服务器**并且检查复选框**对所有本地已知用户的Open**。
4. 单击 **Ok**。
5. 从菜单，挑选**RADIUS>管理RADIUS服务器**。

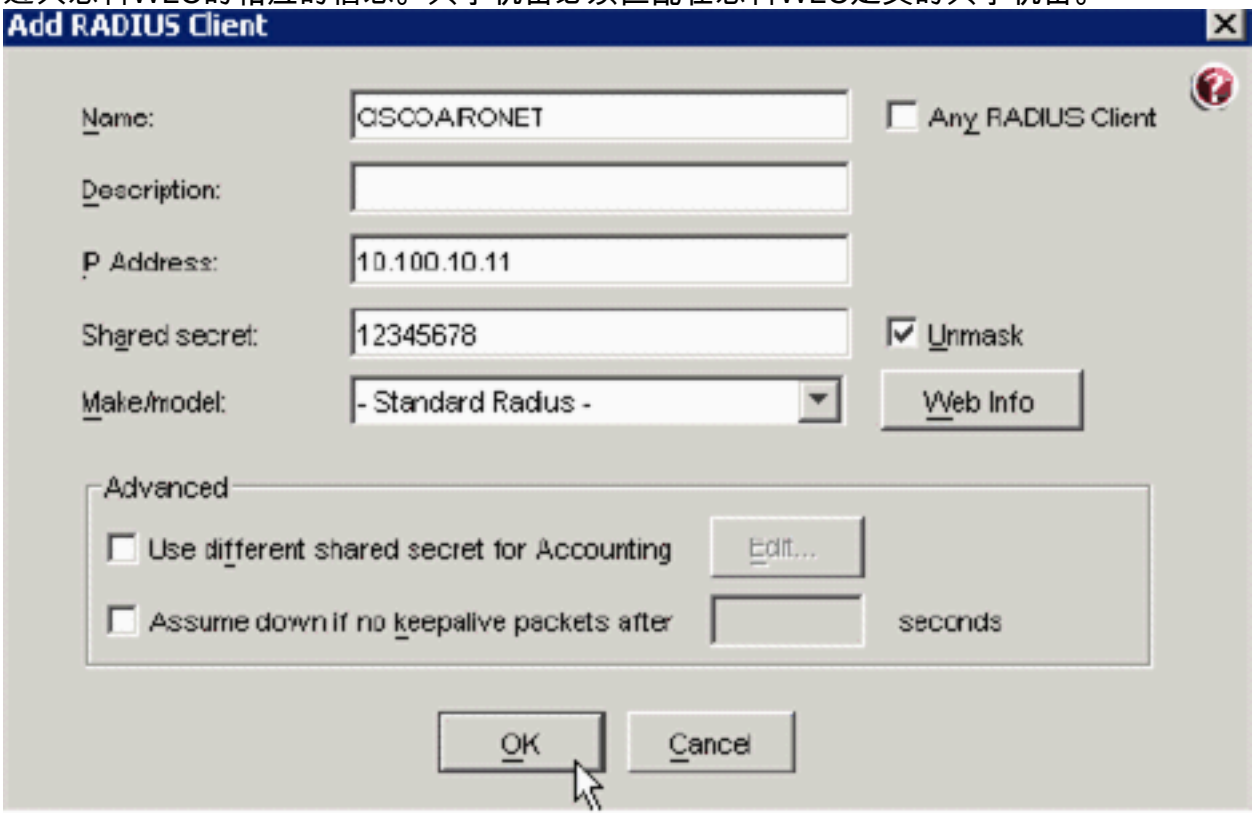


一个新的管理窗口打开。

6. 在此窗口，请选择**RADIUS客户端**，然后单击**添加**。



7. 进入思科WLC的相应的信息。共享机密必须匹配在思科WLC定义的共享机密。



8. 单击 **Ok**。

验证代理配置

此表描述ACS RSA验证代理功能：

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

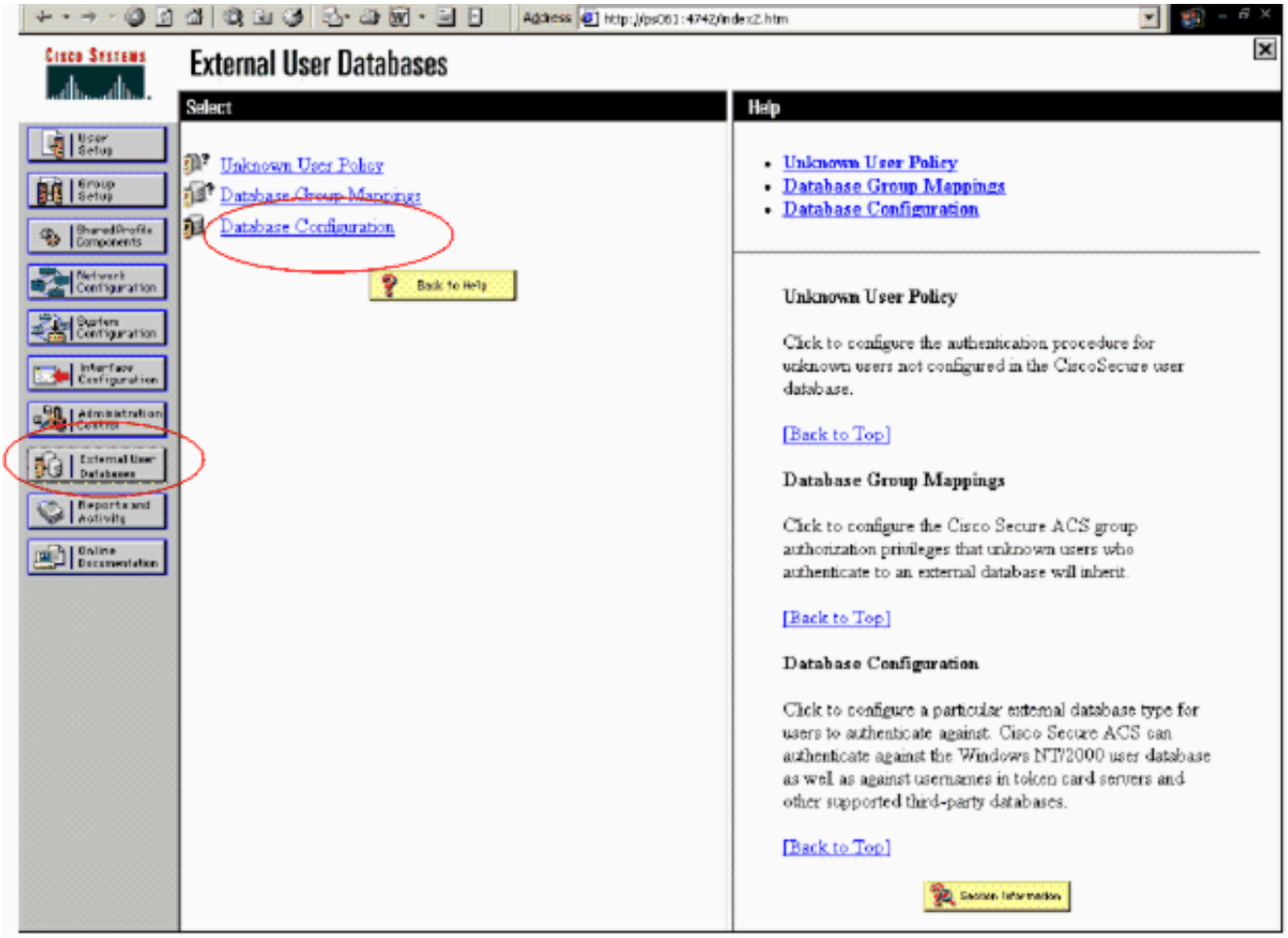
注意： 请参阅包括与关于怎样的RSA验证管理器配置RADIUS服务器的RADIUS文档，如果那是将使用的RADIUS服务器。

配置Cisco ACS

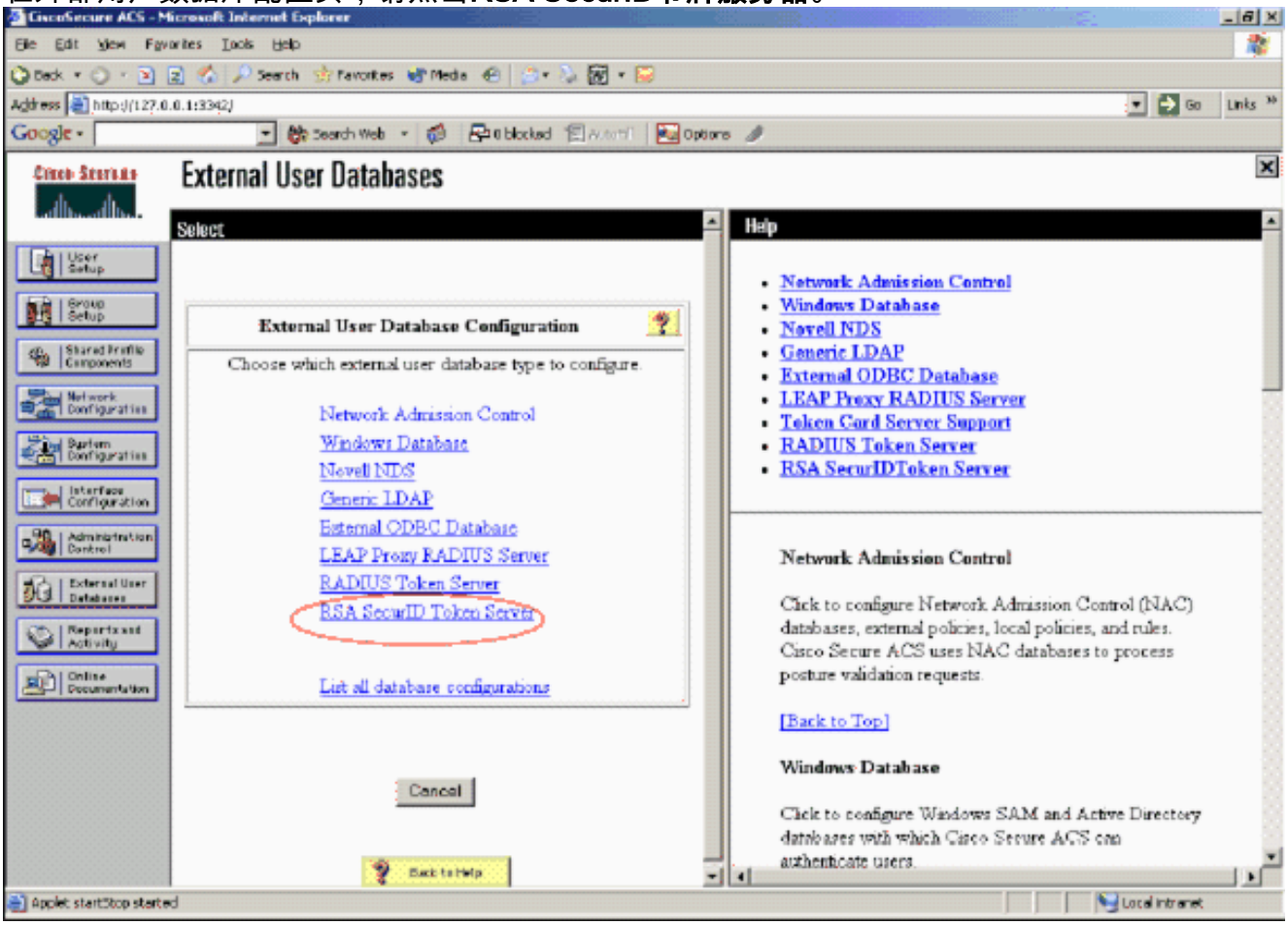
激活RSA SecurID验证

Cisco Secure ACS支持用户RSA SecurID验证。完成这些步骤为了配置Cisco Secure ACS验证有验证管理器的6.1用户：

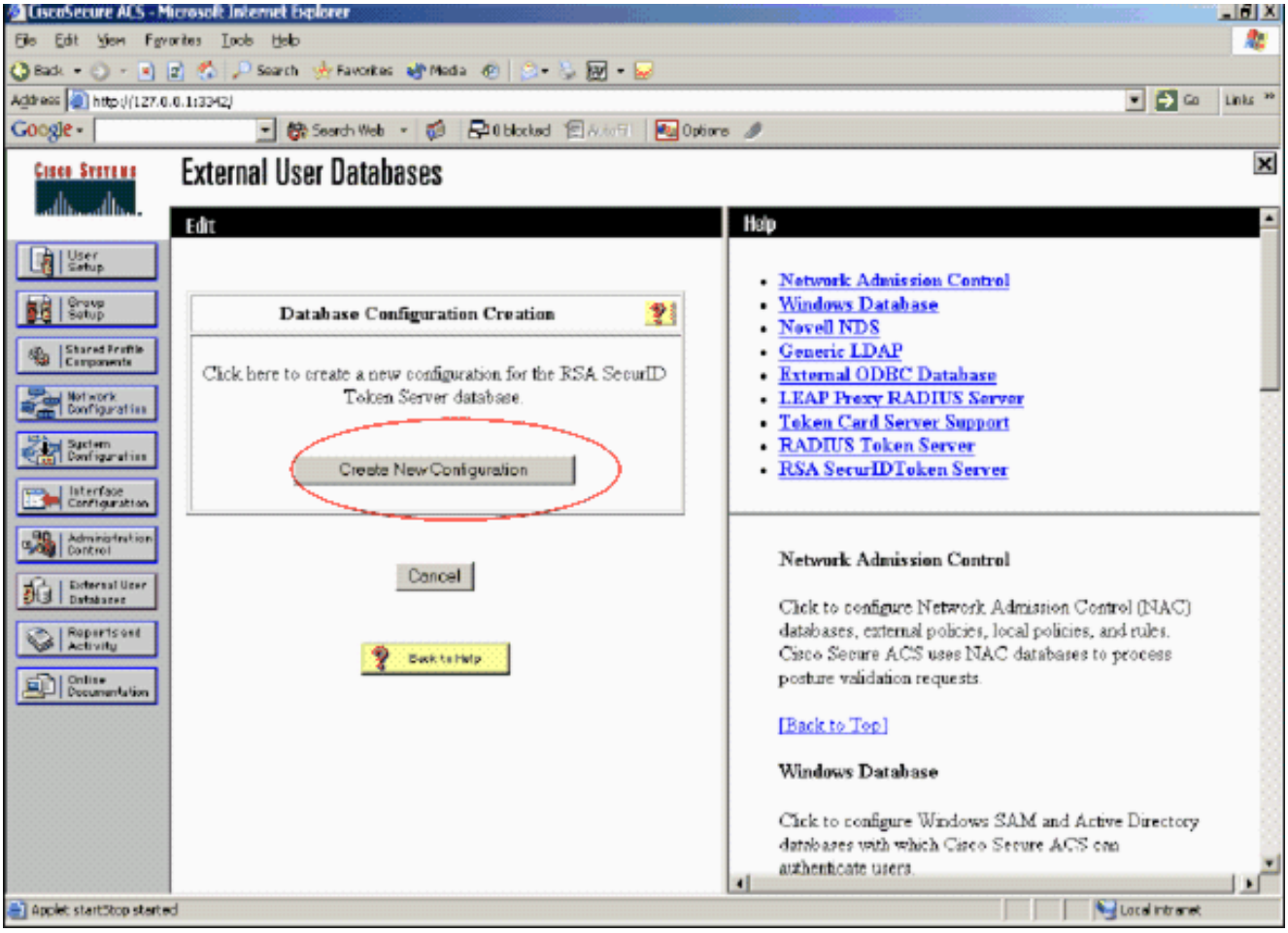
1. 安装RSA验证代理程序5.6或以上在系统的Windows的和Cisco Secure ACS服务器一样。
2. 通过运行验证代理程序的测验验证功能验证连接。
3. 复制acecInt.dll文件从RSA服务器c:\Program Files\RSA**安全\ RSA验证管理器\ prog目录**到ACS服务器的c:\WINNT\system32**目录**。
4. 在导航条，请点击**外部用户数据库**。然后，请点击在外部数据库页的**数据库配置**。



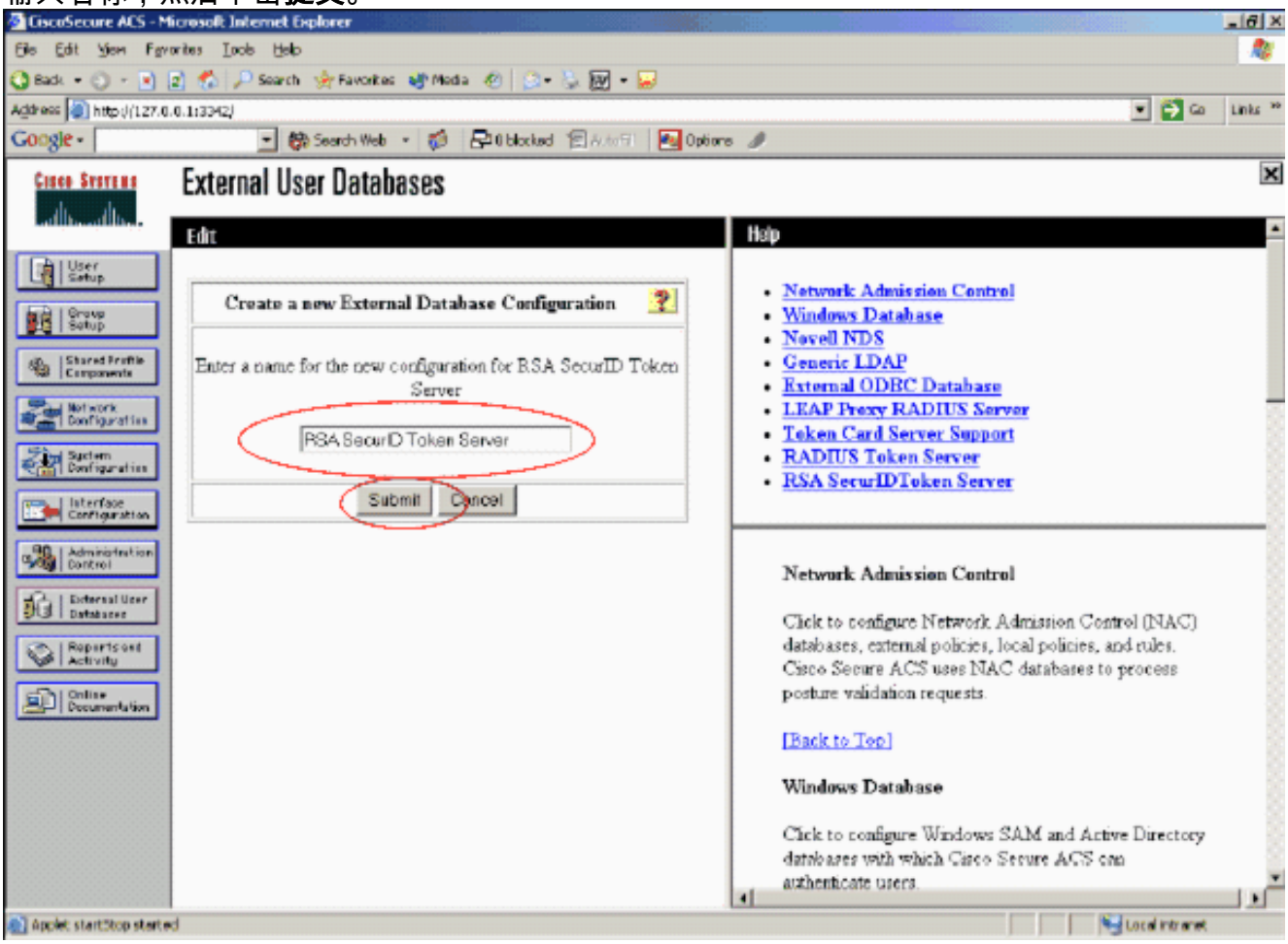
5. 在外部用户数据库配置页，请点击**RSA SecurID令牌服务器**。



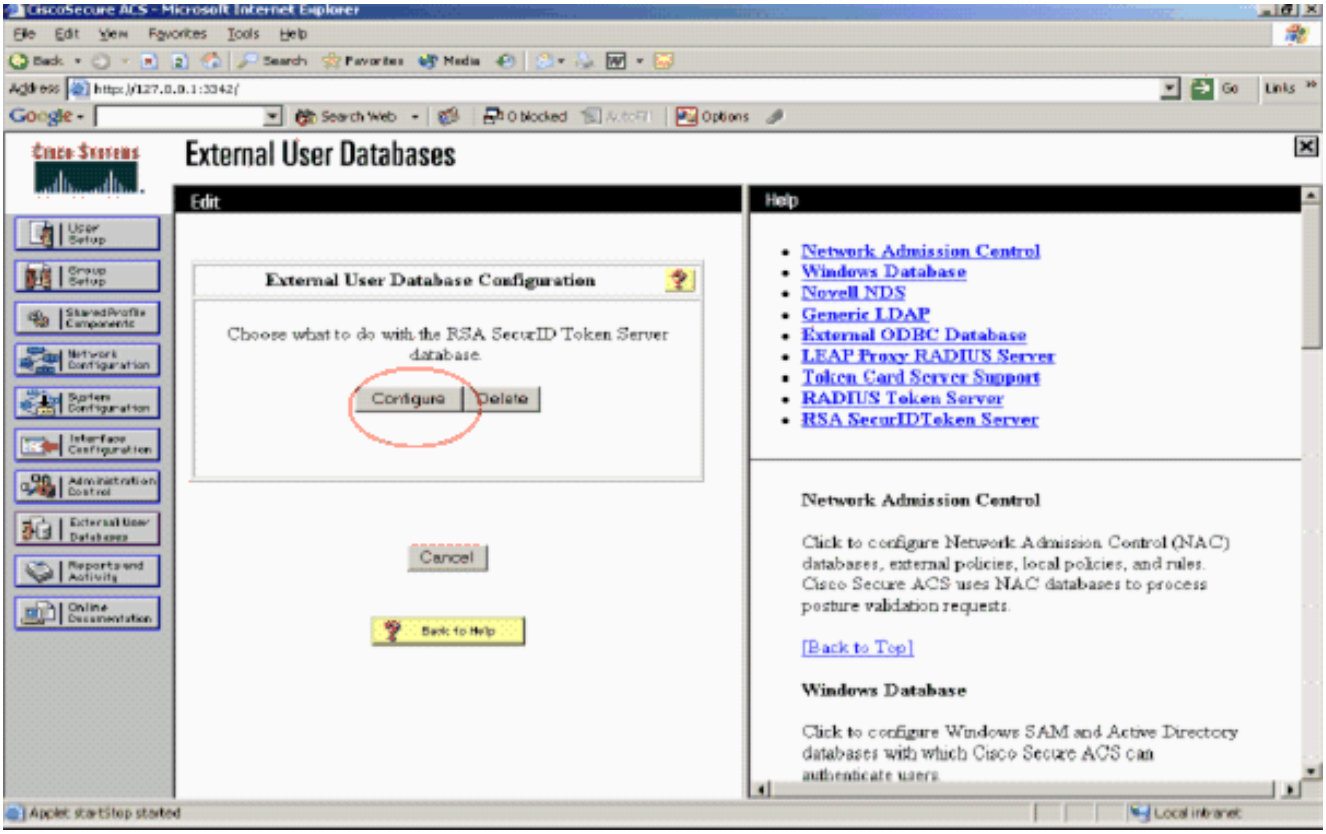
6. 单击**创建新的配置**。



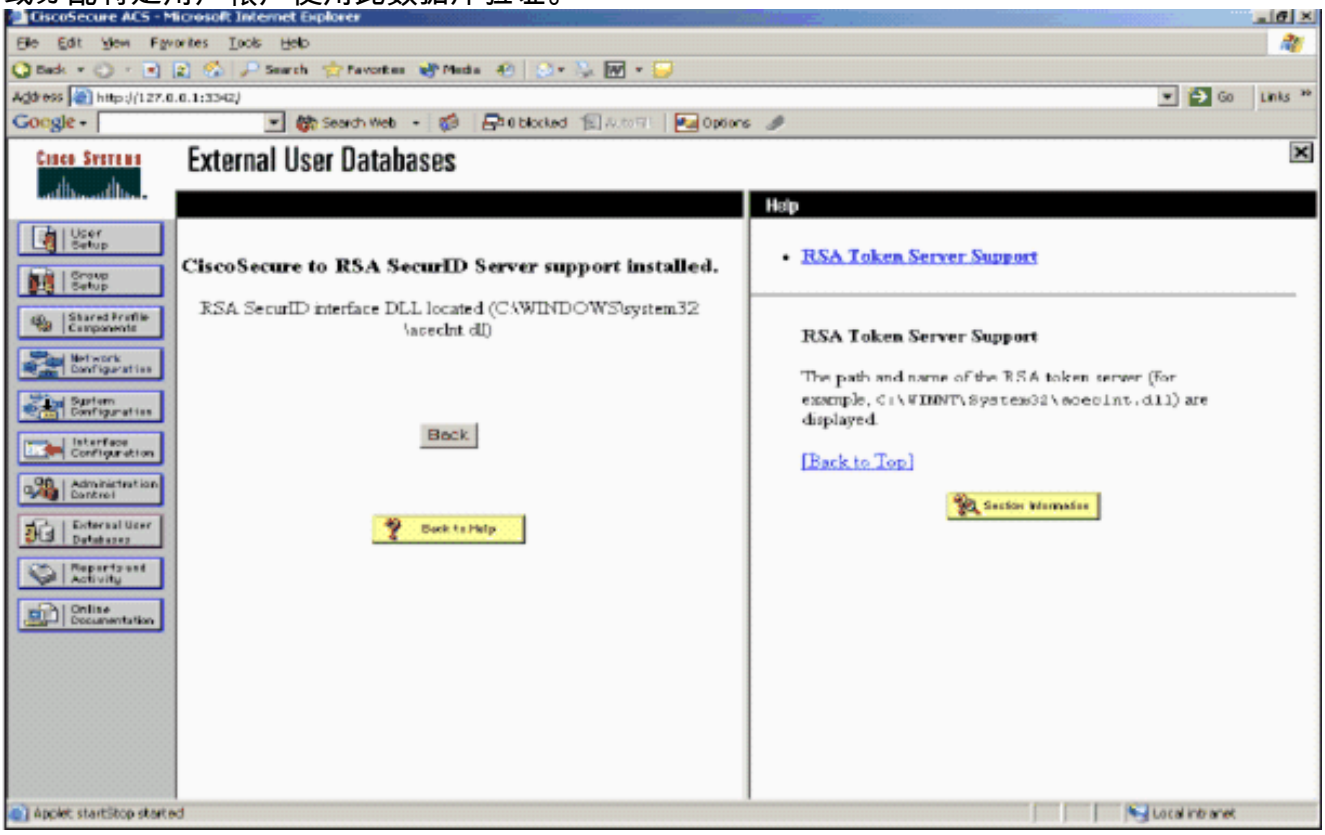
7. 输入名称，然后单击**提交**。



8. 单击 Configure。



Cisco Secure ACS显示令牌服务器和路径的名称对验证器DLL。此信息确认Cisco Secure ACS能与RSA验证代理程序联系。您能添加RSA SecurID外部用户数据库到您的未知用户策略或分配特定用户帐户使用此数据库验证。

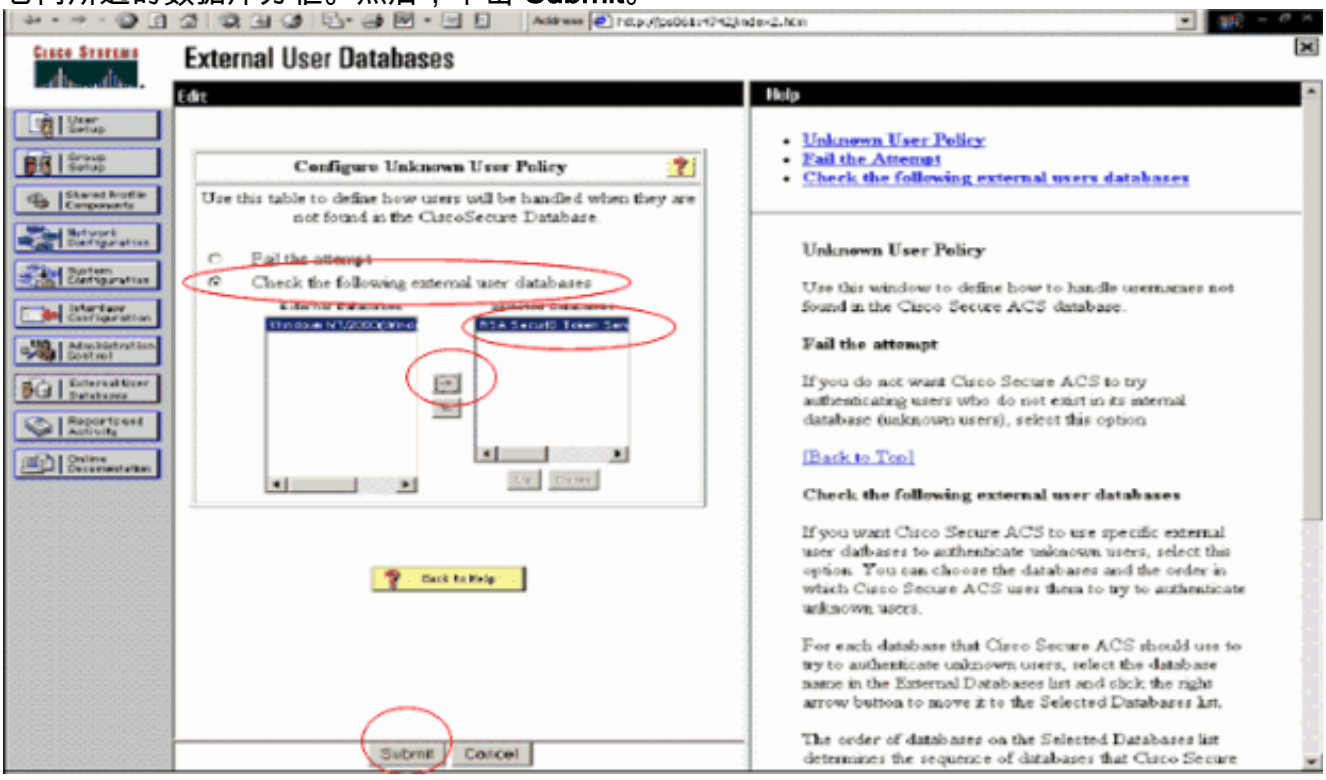


添加/配置RSA SecurID验证对您的未知用户策略

完成这些步骤：

1. 在ACS导航条，请点击**外部用户数据库>未知用户策略**。

2. 在**未知用户策略**页，请选择**检查以下外部用户数据库**，选定**RSA SecurID令牌服务器**并且移动它向所选的数据库方框。然后，单击 **Submit**。

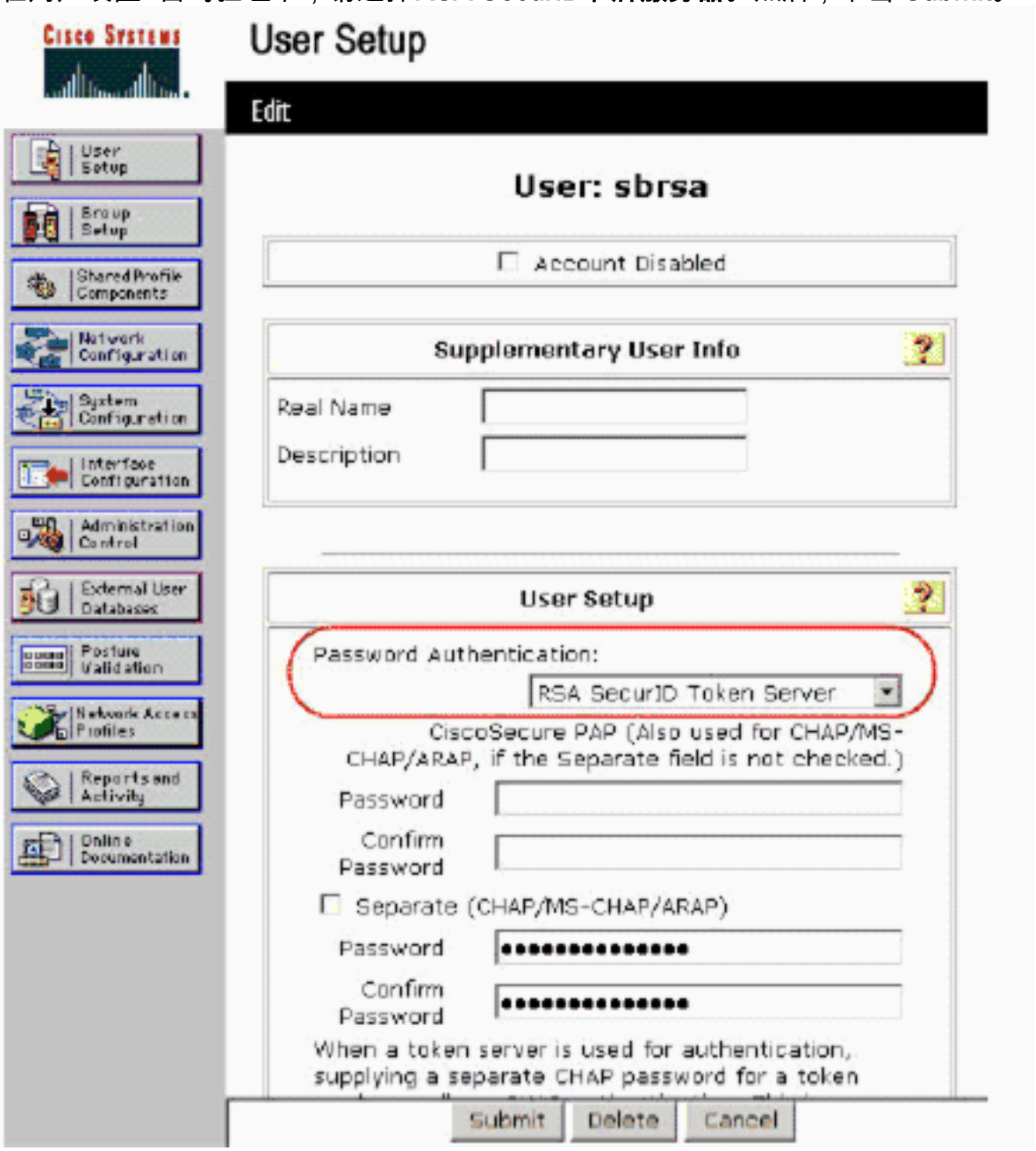


添加/配置特定用户帐户的RSA SecurID验证

完成这些步骤：

1. 点击从主要ACS Admin GUI的**用户设置**。输入用户名并且单击**添加**(或请选择您希望修改)的一个现有用户。

2. 在用户设置>密码验证下，请选择**RSA SecurID令牌服务器**。然后，单击 **Submit**。

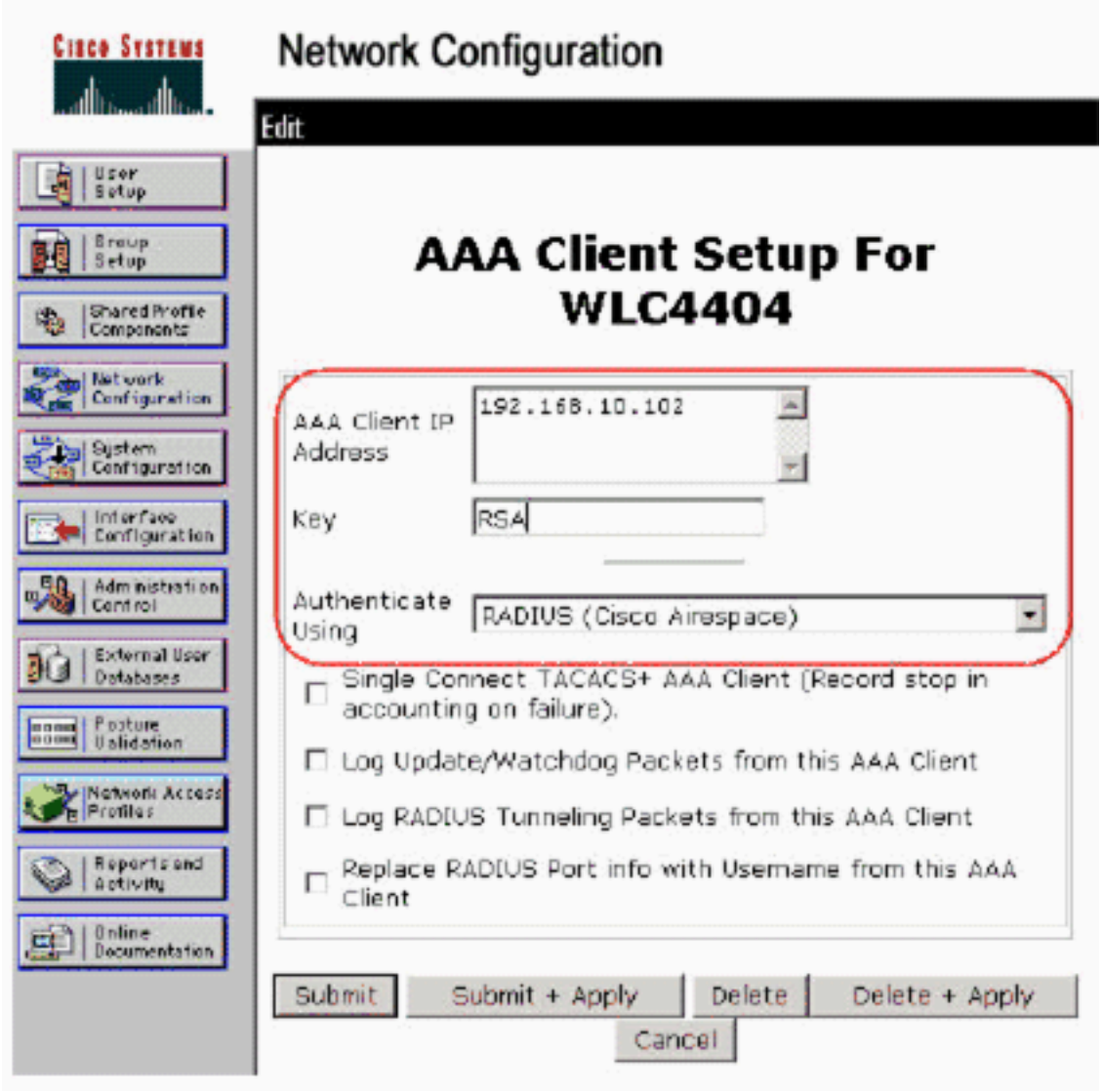


添加Cisco ACS的RADIUS客户端

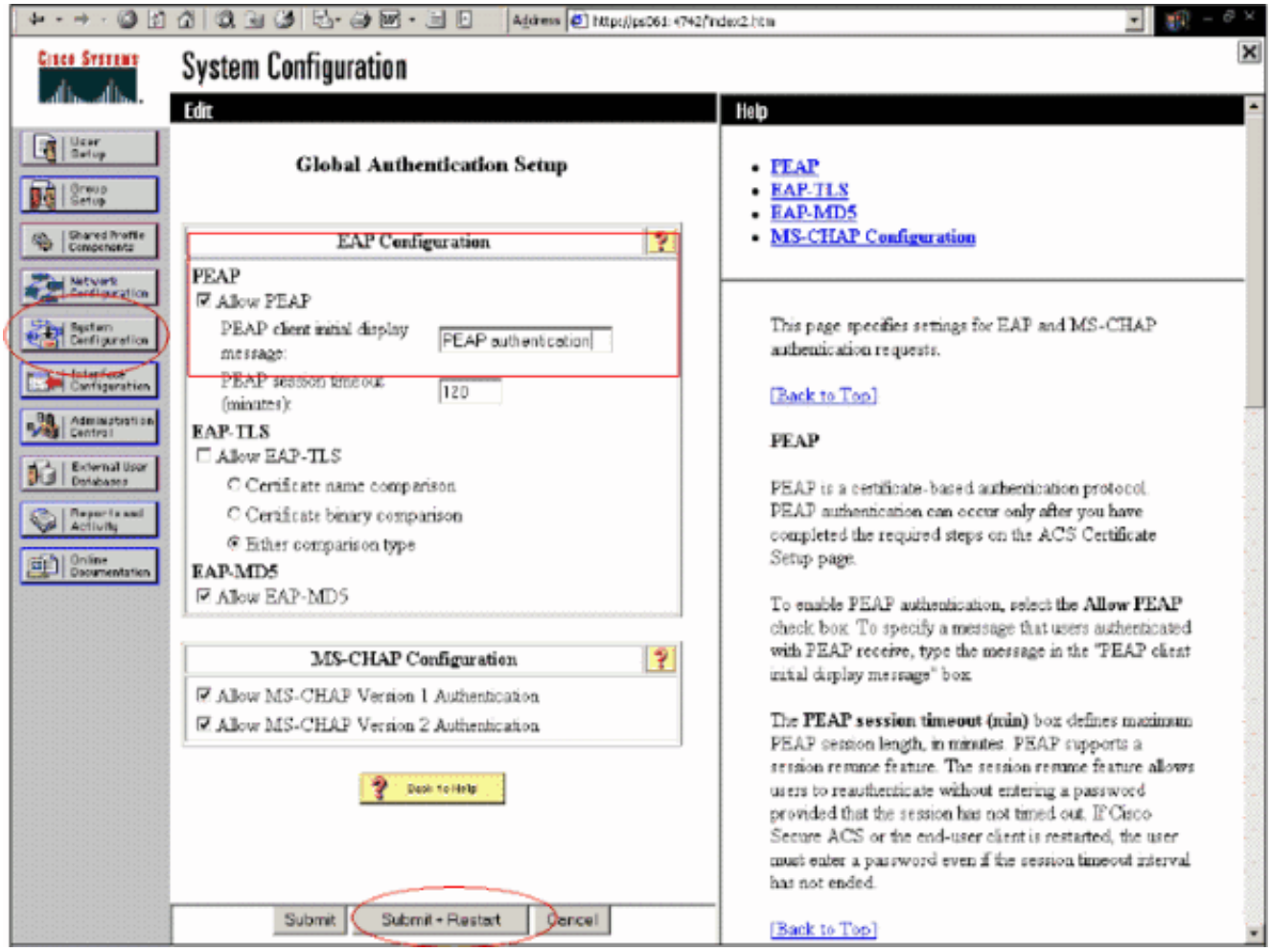
Cisco ACS服务器安装将需要WLC的IP地址为作为转发客户端PEAP认证的NAS服务到ACS。

完成这些步骤：

1. 在**网络配置下**，请添加/编辑将使用的WLC的AAA客户端。输入使用在AAA客户端和ACS之间的“共享机密”锁上(普通对WLC)。选择**验证使用> RADIUS (思科Airespace)**此AAA客户端的。然后，请点击**Submit+Apply**。



2. 申请并且安装从知道的一服务器证书，委托认证机关例如RSA Keon认证机关。关于装备Cisco ACS的此进程的更多信息，参考文档。如果使用RSA认证管理器，您能查看另外的帮助的RSA Keon Aironet实施指南。在您继续前，您必须成功地完成此任务。**注意：** 可能也使用自签名证书。参考关于怎样的Cisco Secure ACS文档使用这些。
3. 在**系统配置下>全局验证设置**，检查复选框**Allow PEAP**验证。



配置802.1x的Cisco无线LAN控制器配置

完成这些步骤：

1. 对配置控制器，因此它的WLC's命令行界面的连接可以配置连接到Cisco Secure ACS服务器。
2. 输入**设置radius验证ip-address命令**从WLC配置验证的一个RADIUS服务器。**注意：** 当您用RSA验证管理器RADIUS服务器时测试，请输入RSA验证管理器的RADIUS服务器的IP地址。当您用Cisco ACS服务器时测试，请输入Cisco Secure ACS服务器的IP地址。
3. 输入**设置radius验证port命令**从WLC指定验证的UDP端口。默认情况下端口1645或1812是活跃的在RSA验证管理器和Cisco ACS服务器。
4. 输入从WLC的**设置radius验证秘密命令**配置在WLC的共享机密。这必须匹配在此RADIUS客户端的RADIUS服务器创建的共享机密。
5. 输入从WLC的**config radius auth enable**命令到启用认证。当希望，请输入**disable命令设置radius的验证**禁用验证。注意默认情况下验证禁用。
6. 选择希望的WLAN的适当的第2层安全选项在WLC。
7. 请使用**show radius auth statistics**和**show radius概略的**命令验证RADIUS设置正确地配置。**注意：** EAP请求超时的默认计时器低，并且也许需要被修改。使用**设置提前的eap请求超时** *<seconds>*命令，这可以执行。它也许也帮助调整根据需求的标识请求超时。使用**设置提前的eap标识请求超时** *<seconds>*命令，这可以执行。

802.11无线客户端配置

对于详细说明如何配置您的无线硬件和客户端请求方，参考多种Cisco Documentation。

已知问题

这些是某些与RSA SecureID验证的著名的问题：

- RSA软件标记。新的Pin模式和下个Tokencode模式，当使用此认证形式以XP2时，不支持。(修复由于ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip)
- 如果您的ACS实施更旧或没有上述补丁程序，客户端不能验证在从“启用的用户转变内; New PIN模式”对“启用”。通过使用“测验验证” RSA应用程序，您能由有完成此用户完成一非无线验证，或者。
- 拒绝4个位/字母数字管脚。如果新的Pin模式的一个用户去PIN策略，认证过程发生故障，并且用户如何为什么是没有察觉的对或。一般，如果用户去策略，他们将发送消息PIN拒绝和再被提示，当再时显示用户什么PIN策略是(例如，如果PIN策略是5-7个位，用户进入4个位)。

相关信息

- 使用 WLC 基于 ACS 对 Active Directory 组映射执行动态 VLAN 分配配置示例
- 具有WLC的无线局域网上的客户端VPN配置示例
- 无线局域网控制器认证的配置示例
- 包含无线局域网控制器和外部 RADIUS 服务器的 EAP-FAST 身份验证配置示例
- 通过 SDM 的固定 ISR 上的无线认证类型配置示例
- 固定 ISR 上的无线认证类型配置示例
- 思科保护可扩展的认证协议
- 使用 RADIUS 服务器执行 EAP 身份验证
- 技术支持和文档 - Cisco Systems