>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

本文档说明如何设置和配置支持思科轻量接入点协议(LWAPP)的AP和无线局域网控制器(WLC)，以及要在RSA SecurID身份验证的WLAN环境中使用的思科安全访问控制服务器(ACS)。有关RSA SecurID特定实施指南，请访问www.rsasecured.com。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解 WLC 和如何配置 WLC 基本参数.
- 了解如何使用Aironet桌面实用程序(ADU)配置思科无线客户端的配置文件。
- 了解 Cisco Secure ACS 的功能.
- 了解LWAPP的基本知识。
- 基本了解Microsoft Windows Active Directory(AD)服务以及域控制器和DNS概念。**注意：**在尝试此配置之前，请确保ACS和RSA身份验证管理器服务器位于同一域中，且其系统时钟完全同步。如果使用Microsoft Windows AD服务，请参阅Microsoft文档以在同一域中配置ACS和RSA

Manager服务器。有关信息，请参阅配置Active Directory和Windows用户数据库。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- RSA身份验证管理器6.1
- 用于Microsoft Windows的RSA身份验证代理6.1
- 思科安全ACS 4.0(1)内部版本27**注意：**包含的RADIUS服务器可用来取代Cisco ACS。有关如何配置服务器，请参阅RSA身份验证管理器随附的RADIUS文档。
- 版本4.0（版本4.0.155.0）的Cisco WLC和轻量接入点

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

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

RSA SecurID系统是一个双因素用户身份验证解决方案。RSA SecurID身份验证器与RSA身份验证管理器和RSA身份验证代理配合使用时，需要用户使用双因素身份验证机制来识别自己。

一个是RSA SecurID代码，该代码是每60秒在RSA SecureID身份验证器设备上生成的随机数。另一个是个人识别码(PIN)。

RSA SecurID身份验证器的使用与输入密码一样简单。为每个最终用户分配一个RSA SecurID身份验证器，该身份验证器生成一次性使用代码。登录时，用户只需输入此号码和要成功验证的加密PIN。另外， RSA SecurID硬件令牌通常预编程为在收到令牌后能完全正常工作。

此Flash演示说明如何使用RSA secureID身份验证器设备：RSA演示。

通过RSA SecurID就绪计划，Cisco WLC和Cisco Secure ACS服务器开箱即可支持RSA SecurID身份验证。RSA身份验证代理软件拦截来自用户（或用户组）的访问请求（无论是本地还是远程），并将其定向到RSA身份验证管理器程序进行身份验证。

RSA Authentication Manager软件是RSA SecurID解决方案的管理组件。它用于验证身份验证请求并集中管理企业网络的身份验证策略。它与RSA SecurID身份验证器和RSA身份验证代理软件配合使用。

在本文档中，通过在Cisco ACS服务器上安装代理软件，将其用作RSA身份验证代理。WLC是网络接入服务器(NAS)（AAA客户端），它反过来将客户端身份验证转发到ACS。本文档演示了使用受保护可扩展身份验证协议(PEAP)客户端身份验证的概念和设置。

要了解PEAP身份验证，请参阅思科保护的可扩展身份验证协议。

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
- 身份验证代理配置

代理主机配置

使用Cisco Secure ACS作为RADIUS服务器

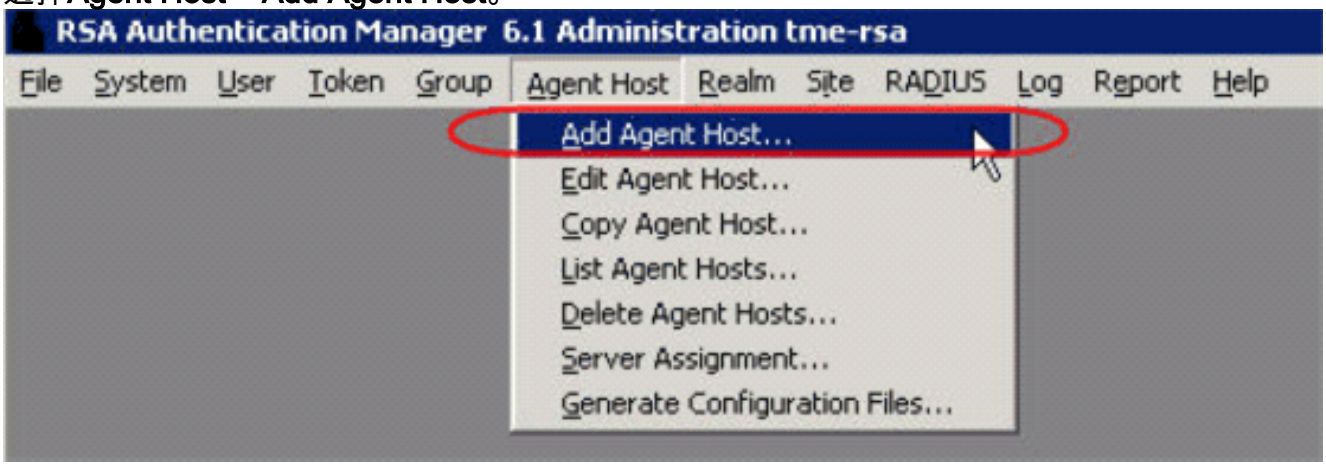
为了促进Cisco Secure ACS与RSA Authentication Manager/RSA SecurID设备之间的通信，必须将代理主机记录添加到RSA Authentication Manager数据库。代理主机记录标识其数据库中的思科安全ACS，并包含有关通信和加密的信息。

要创建代理主机记录，您需要以下信息：

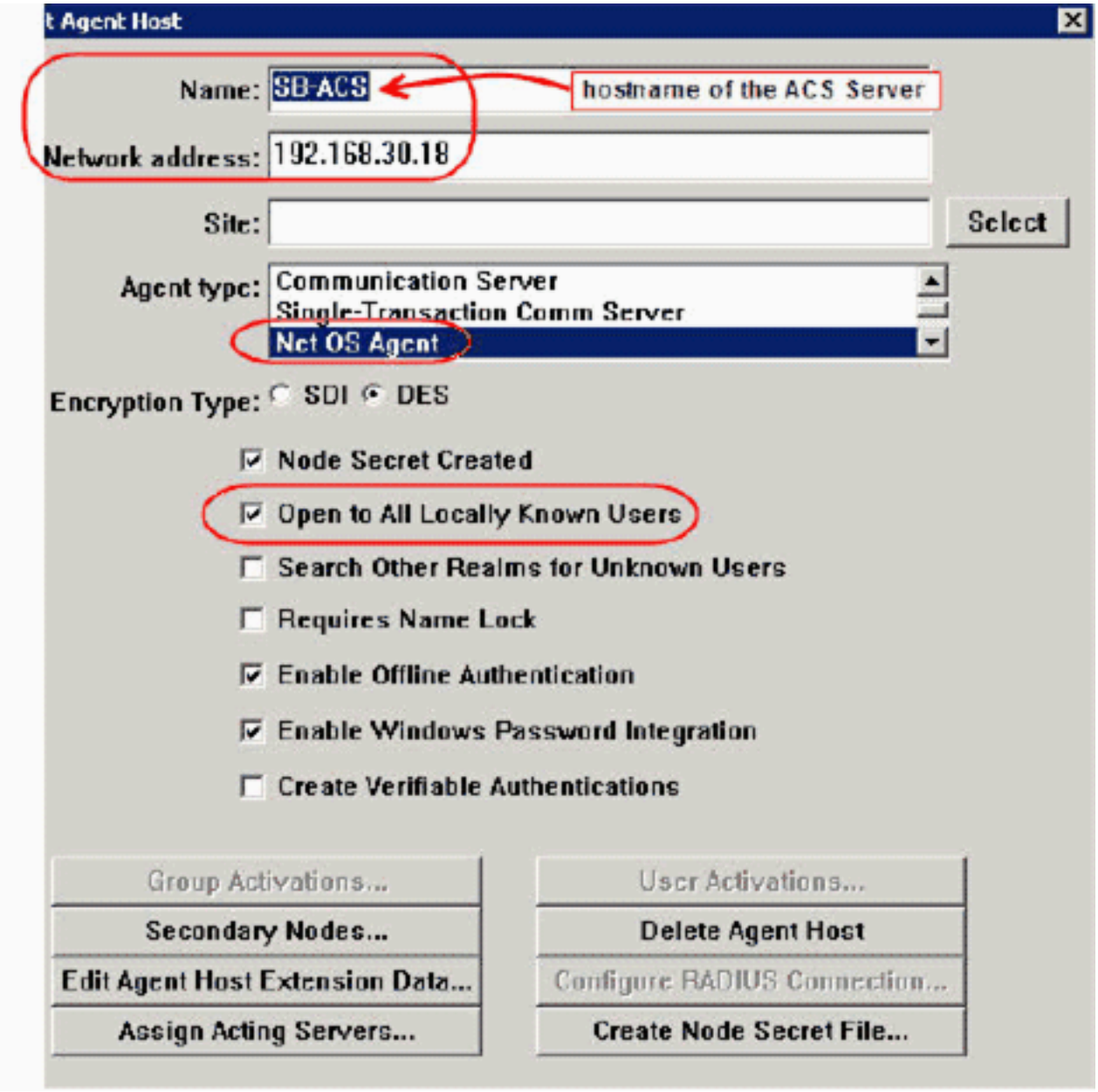
- Cisco ACS服务器的主机名
- Cisco ACS服务器所有网络接口的IP地址

请完成以下步骤：

1. 打开RSA Authentication Manager主机模式应用程序。
2. 选择**Agent Host > Add Agent Host**。



您看见此窗口



:

3. 输入Cisco ACS服务器名称和网络地址的相应信息。为“代理**类型**”选择“NetOS”，并选中“Open to All Locally Known Users”**复选框。**
4. Click **OK**.

使用RSA Authentication Manager 6.1 RADIUS服务器

为了便于Cisco WLC和RSA身份验证管理器之间的通信，必须将代理主机记录添加到RSA身份验证管理器数据库和RADIUS服务器数据库。代理主机记录标识其数据库中的Cisco WLC，并包含有关通信和加密的信息。

要创建代理主机记录，您需要以下信息：

- WLC的主机名
- WLC的管理IP地址
- RADIUS密钥，必须与思科WLC上的RADIUS密钥匹配

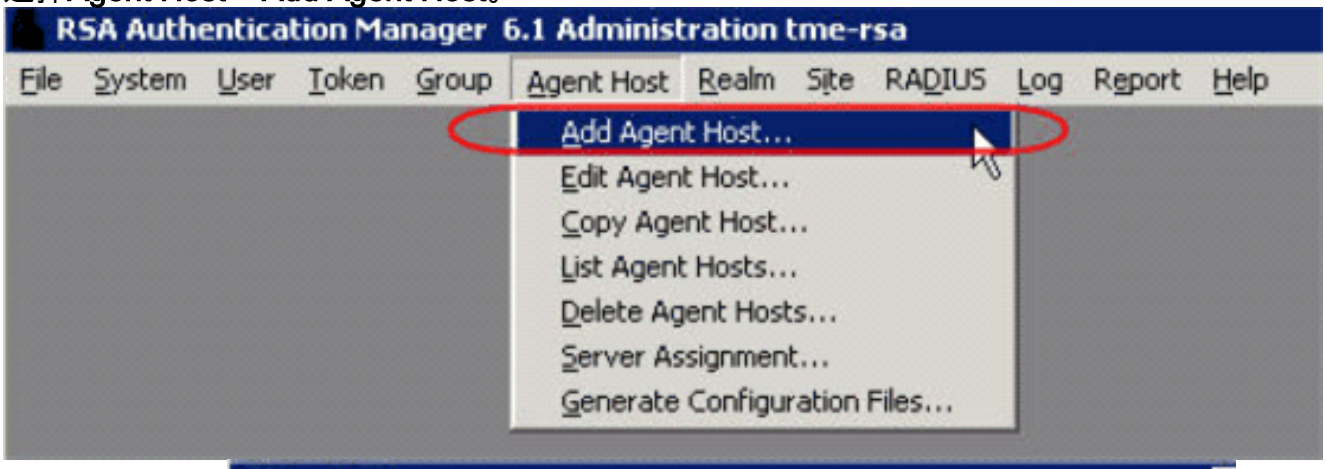
添加代理主机记录时，WLC的角色配置为通信服务器。RSA身份验证管理器使用此设置来确定与WLC的通信将如何进行。

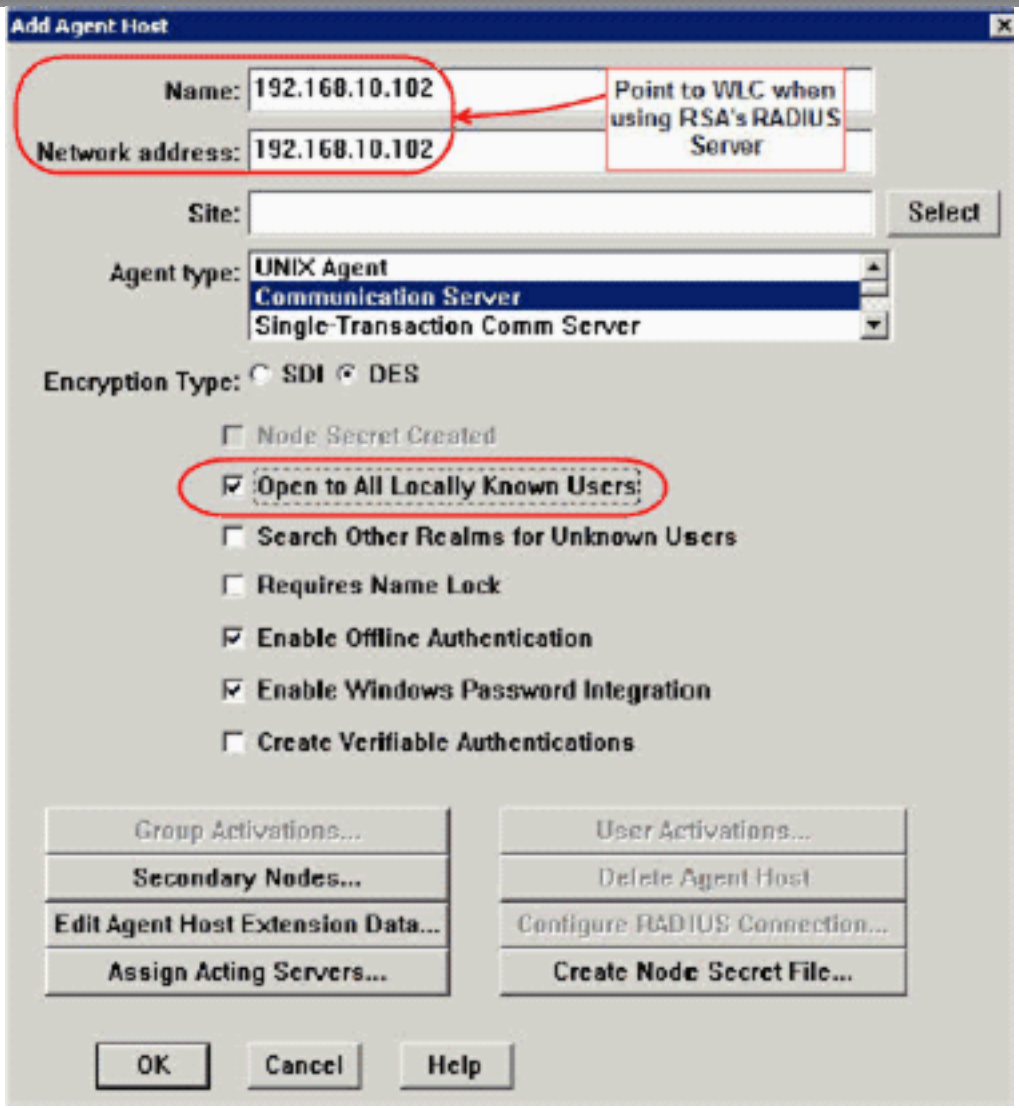
注意：RSA Authentication Manager/RSA SecurID设备中的主机名必须解析为本地网络上的有效

IP地址。

请完成以下步骤：

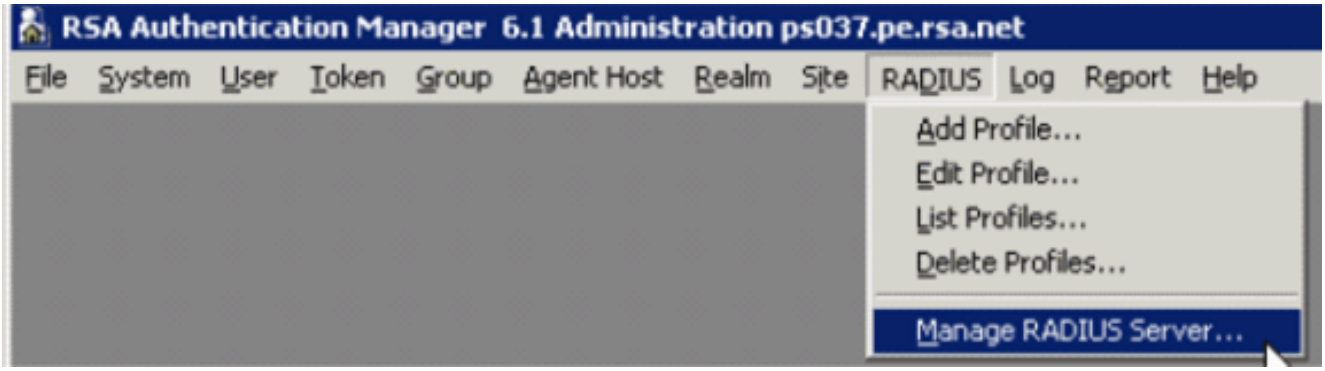
1. 打开RSA Authentication Manager主机模式应用程序。
2. 选择**Agent Host > Add Agent Host**。





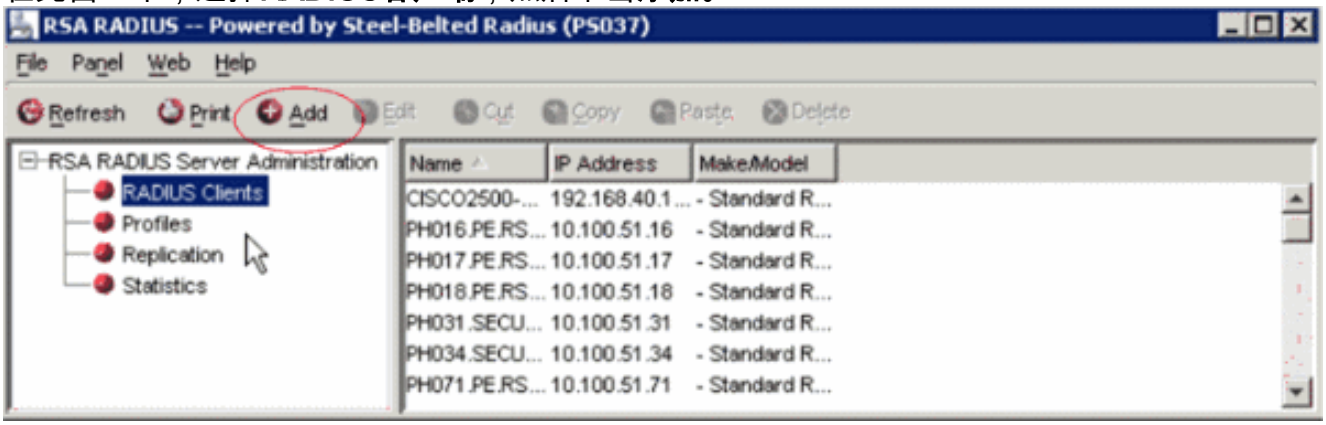
您看见此窗口：

3. 输入WLC主机名（可解析的FQDN，如有必要）和网络地址的适当信息。为代理类**型选择Communication Server**，并选中Open to All Locally Known Users**复选框。**
4. Click **OK**.
5. 从菜单中，选择**RADIUS > Manage RADIUS Server**。

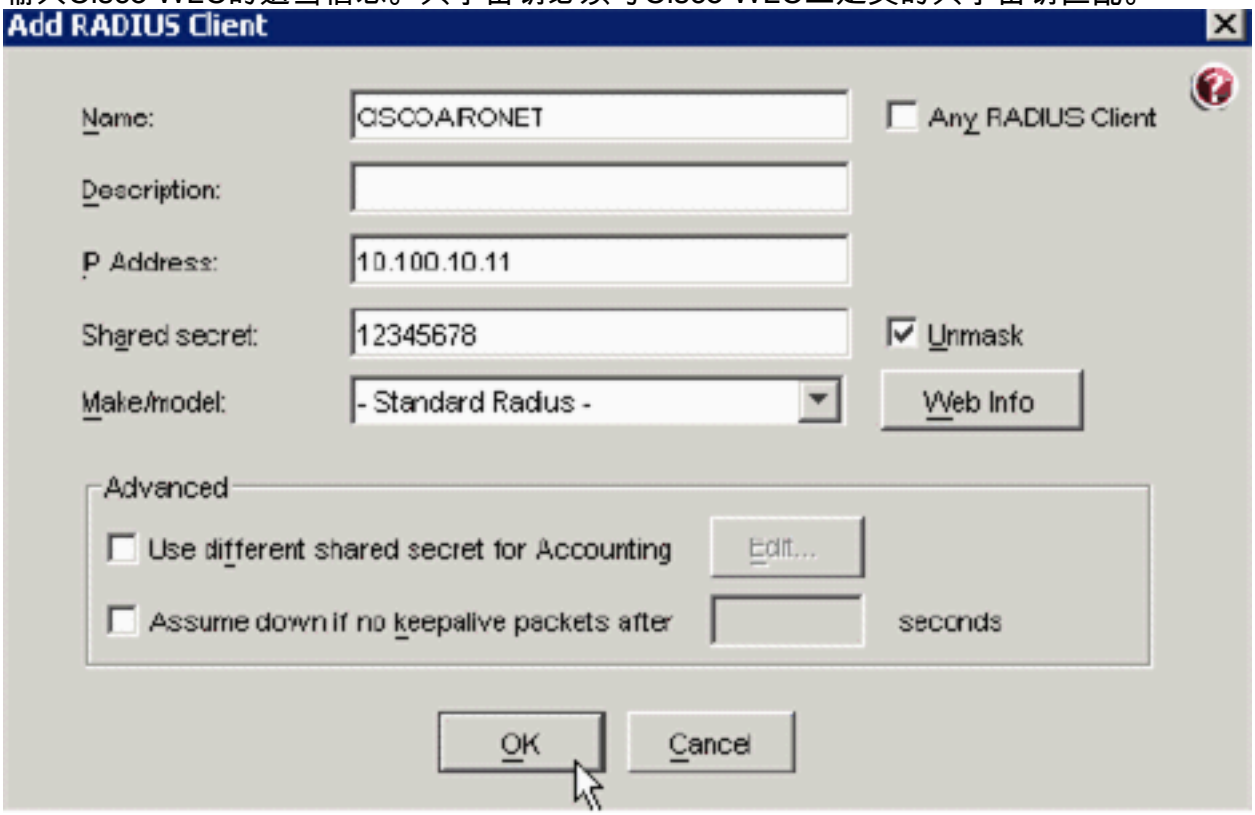


将打开新的管理窗口。

6. 在此窗口中，选择**RADIUS客户端**，然后单击**添加**。



7. 输入Cisco WLC的适当信息。共享密钥必须与Cisco WLC上定义的共享密钥匹配。



8. Click **OK**.

身份验证代理配置

下表表示ACS的RSA身份验证代理功能：

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

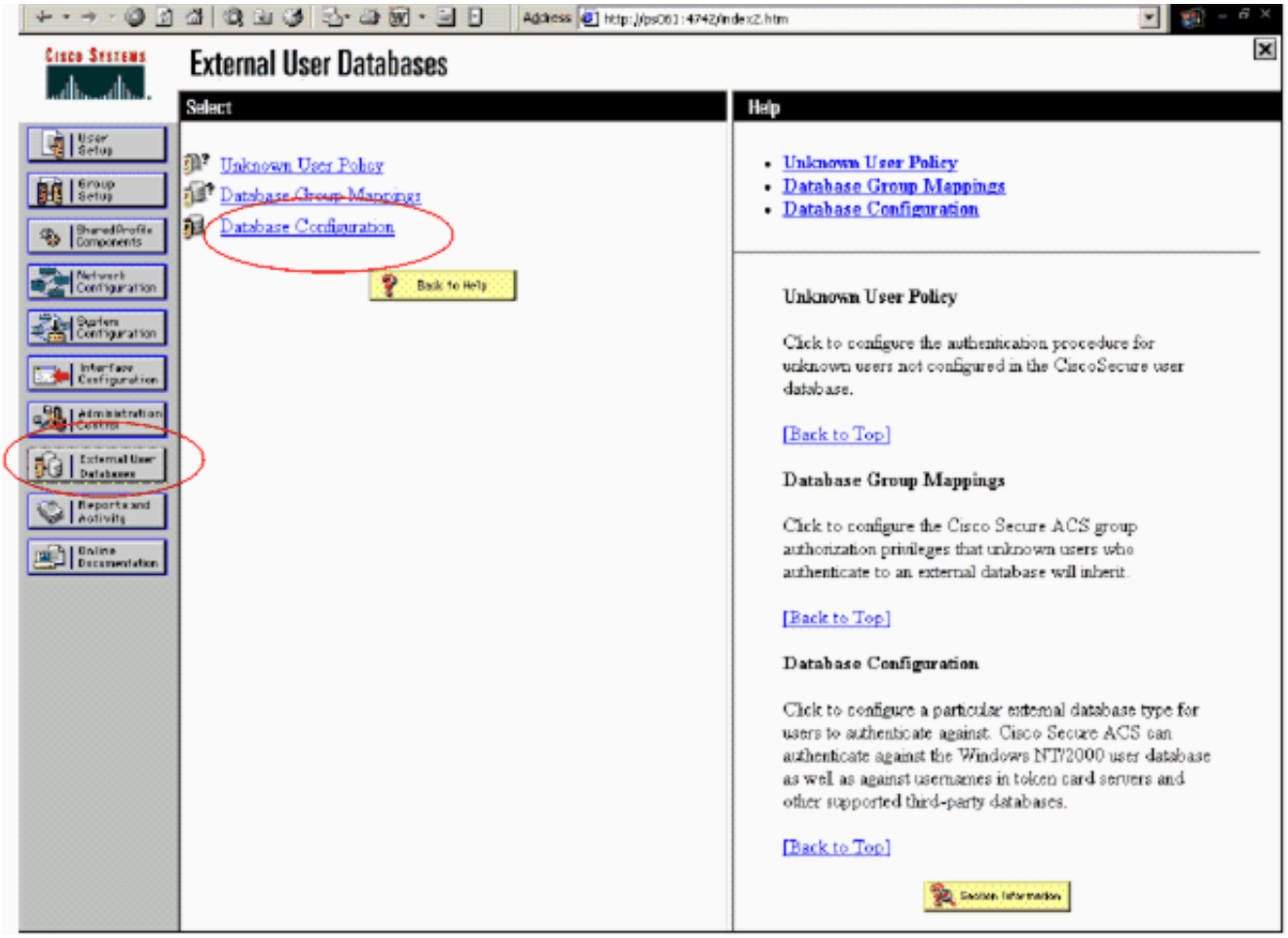
注意：如果RADIUS服务器将要使用，请参阅RSA身份验证管理器随附的RADIUS文档，了解如何配置RADIUS服务器。

配置Cisco ACS

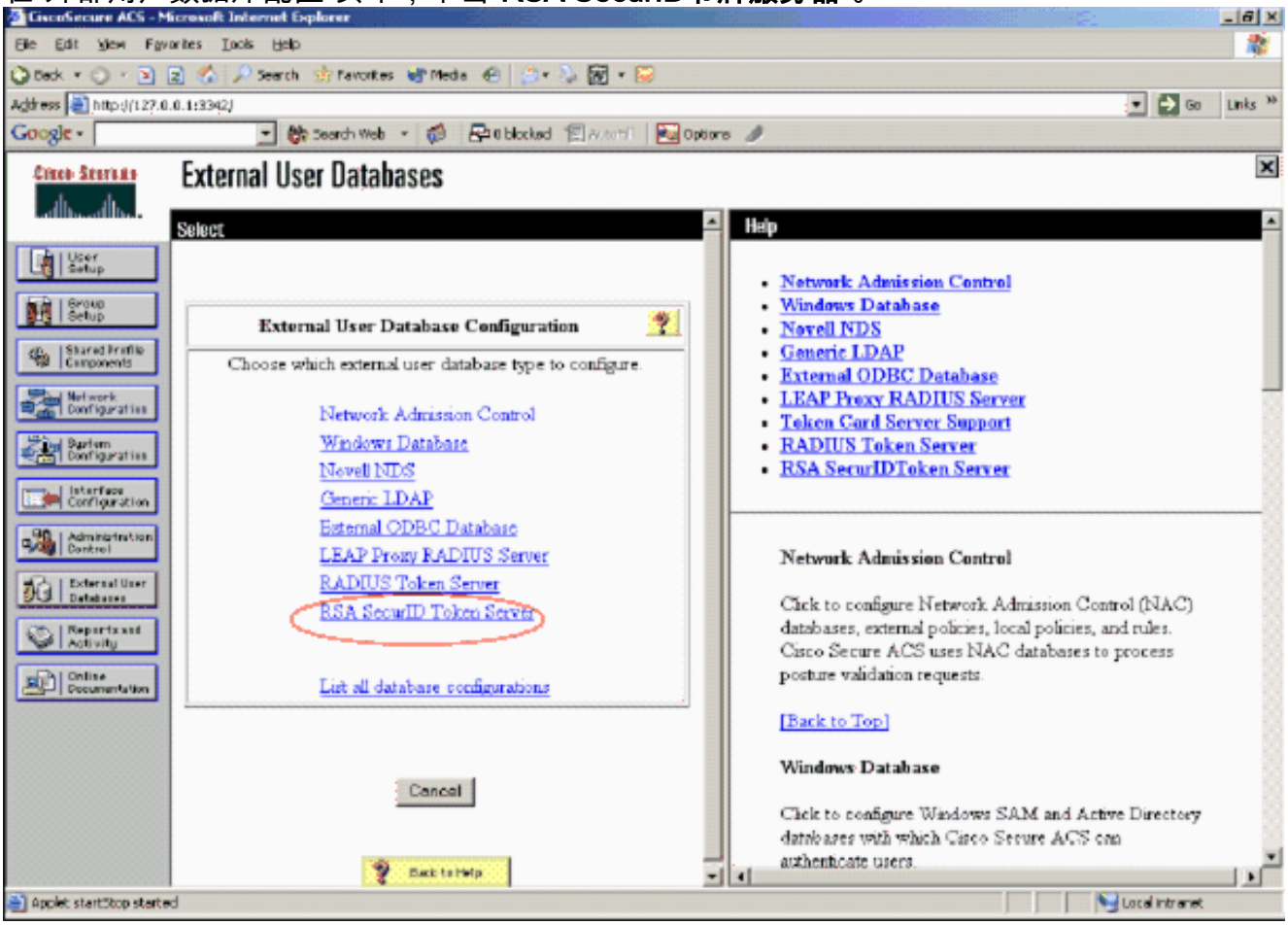
激活RSA SecurID身份验证

Cisco Secure ACS支持用户的RSA SecurID身份验证。要配置Cisco Secure ACS以使用Authentication Manager 6.1对用户进行身份验证，请完成以下步骤：

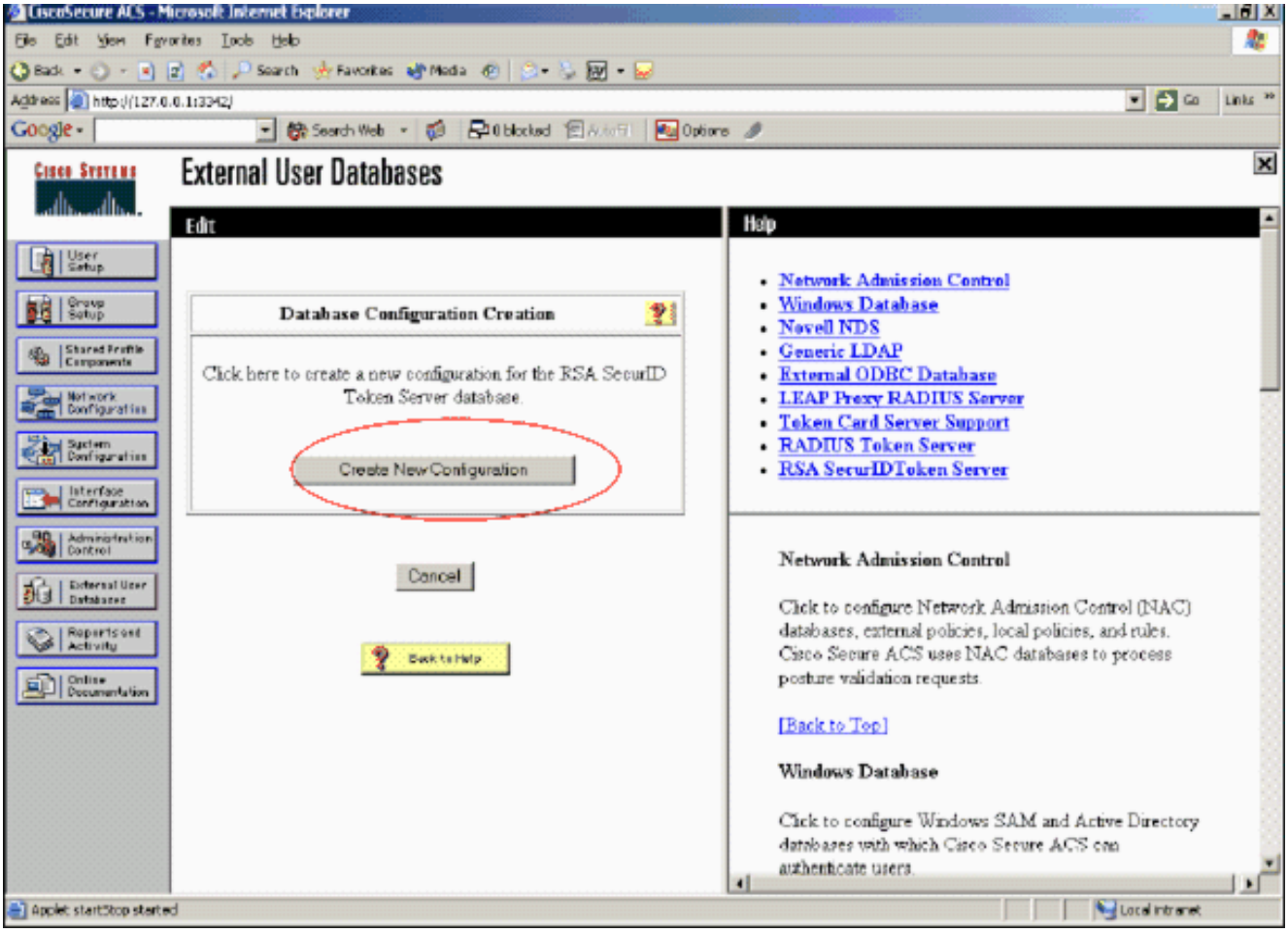
1. 在与Cisco Secure ACS服务器相同的系统上安装Windows的RSA Authentication Agent 5.6或更高版本。
2. 通过运行身份验证代理的测试身份验证功能来验证连接。
3. 将aceclnt.dll文件从RSA服务器**c:\Program Files\RSA Security\RSA Authentication Manager\prog目**录复制到ACS服务器的c:\WINNT\system32**目**录。
4. 在导航栏中，单击“外部**用户数据库”**。然后，单击“外**部数据**库”页中的“数据库配置”。



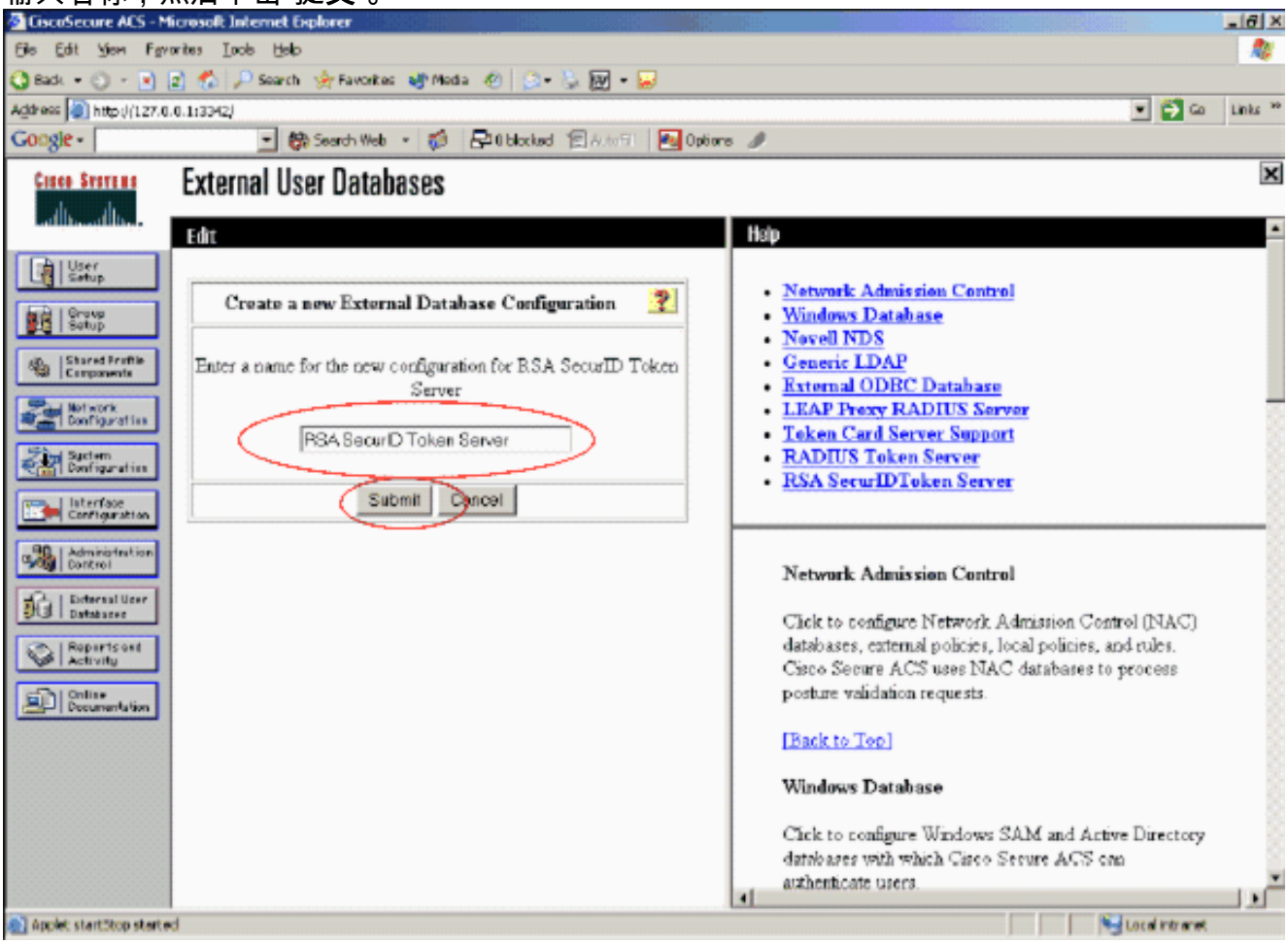
5. 在“外部用户数据库配置”页中，单击**“RSA SecurID令牌服务器”**。



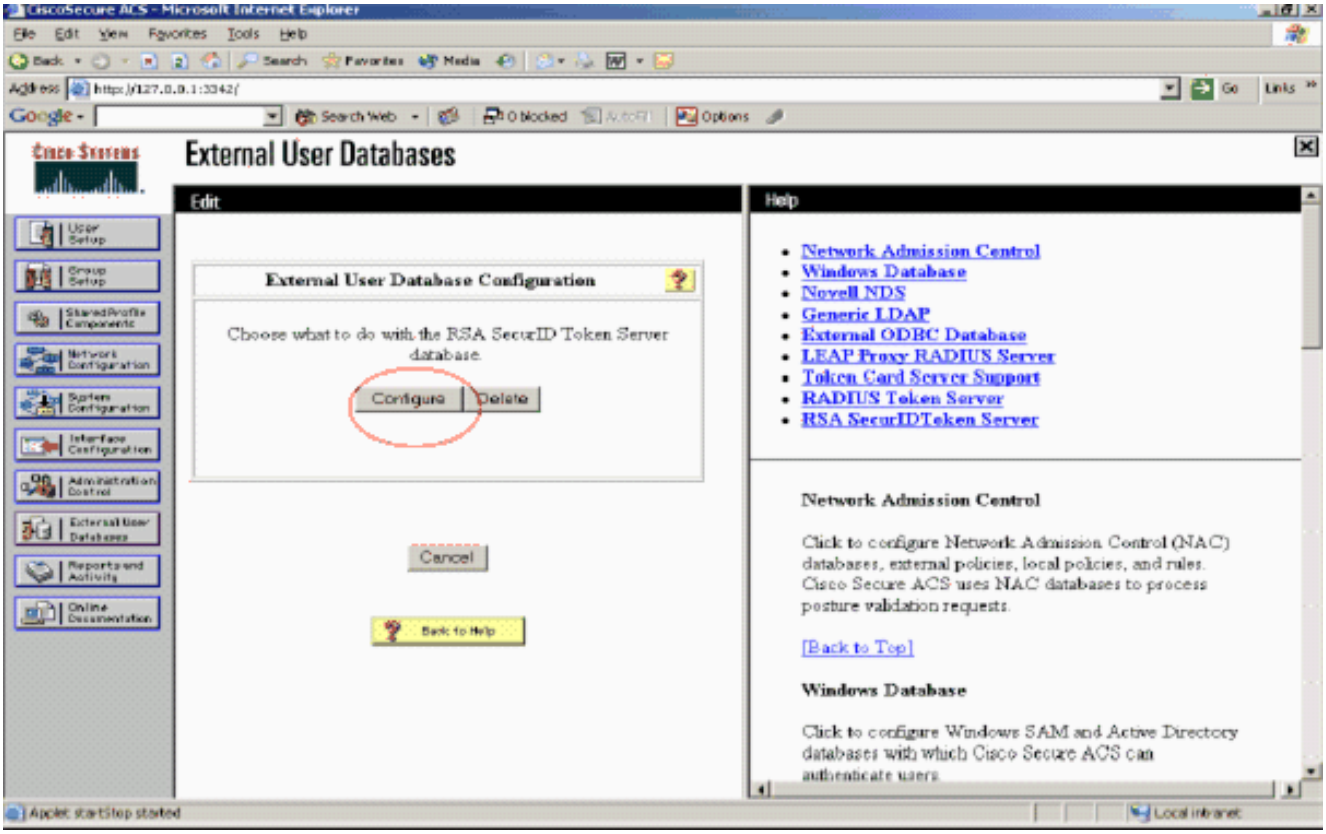
6. 单击“**创建新配置**”。



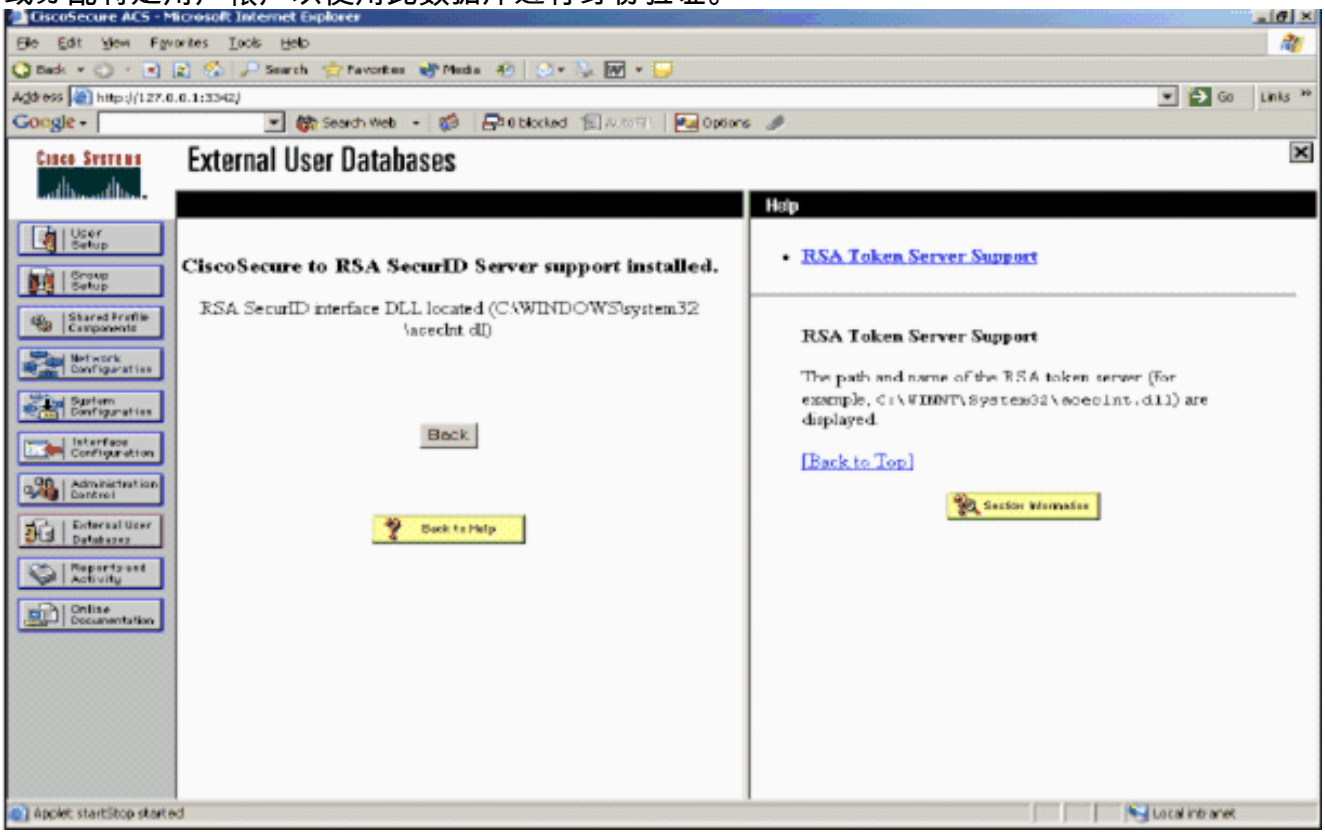
7. 输入名称，然后单击“提交”。



8. 单击 Configure。



Cisco Secure ACS显示令牌服务器的名称和身份验证器DLL的路径。此信息确认Cisco Secure ACS可以联系RSA身份验证代理。您可以将RSA SecurID外部用户数据库添加到未知用户策略或分配特定用户帐户以使用此数据库进行身份验证。

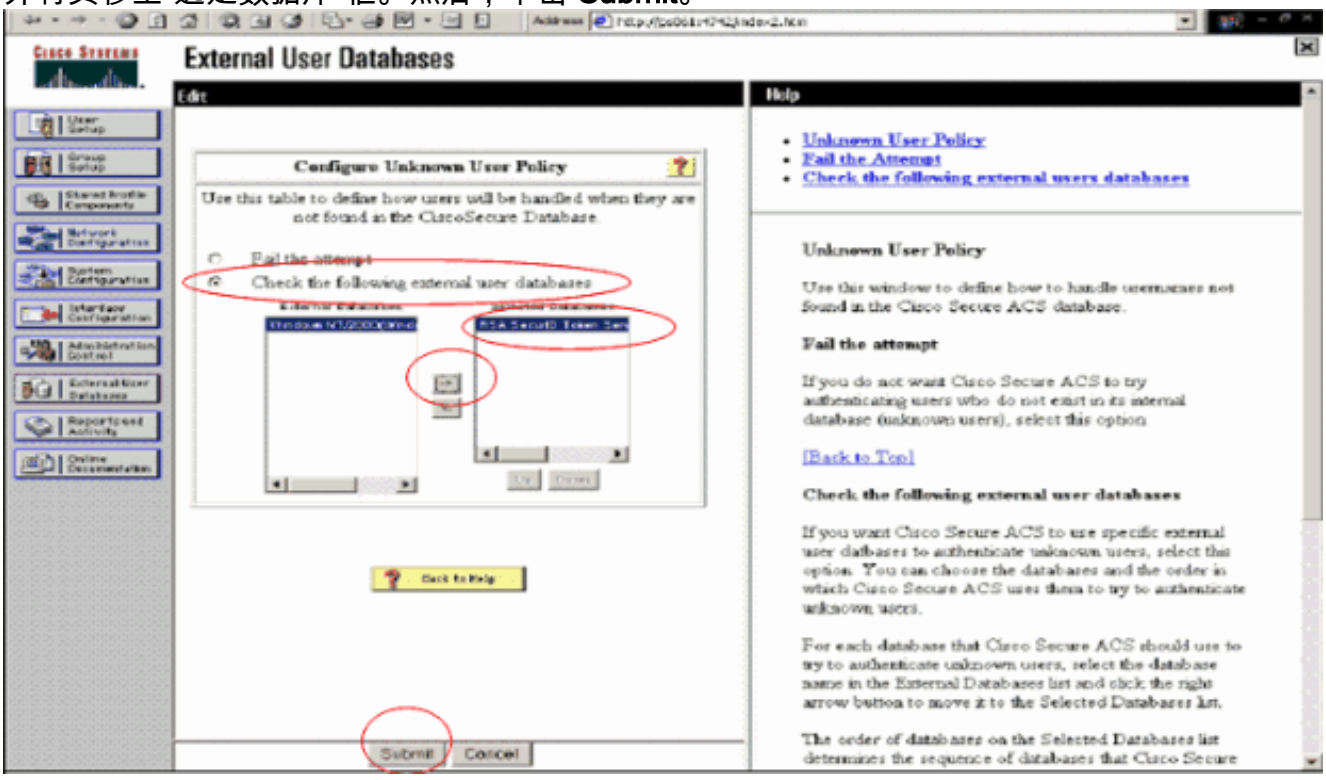


向未知用户策略添加/配置RSA SecurID身份验证

请完成以下步骤：

1. 在ACS导航栏中，单击“外部用**户数据库”>**“未**知用户策略”**。

2. 在“未**知用户策**略”页中，**选择“检查以下外部用户数据库”**，突出**显示RSA SecurID令牌服务器**并将其移至“选定数据库”框。然后，单击 **Submit**。

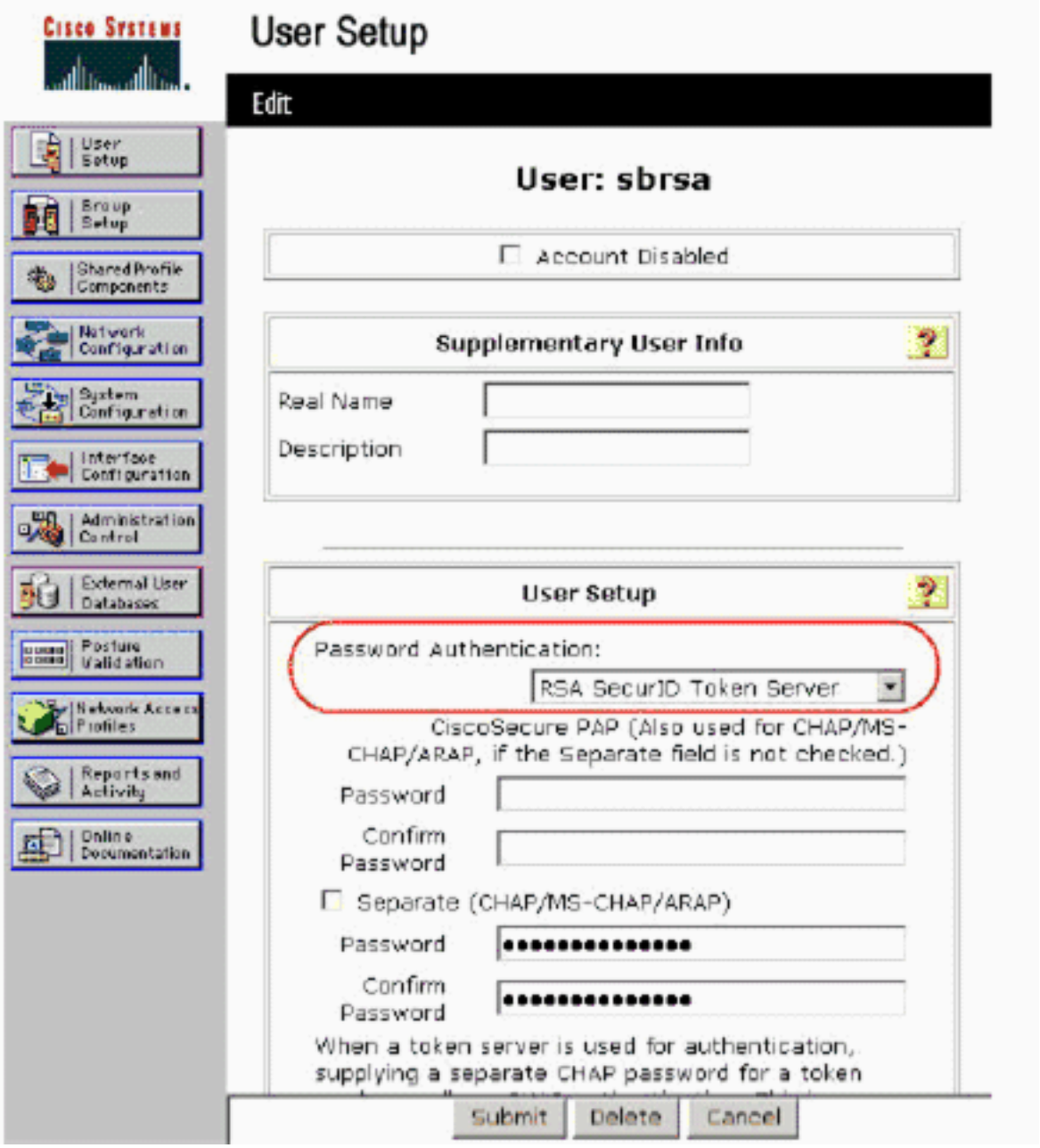


[添加/配置特定用户帐户的RSA SecurID身份验证]

请完成以下步骤：

1. 从主ACS Admin GUI中单击**User Setup**。输入用户名并单击**Add**（或选择要修改的现有用户）。

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

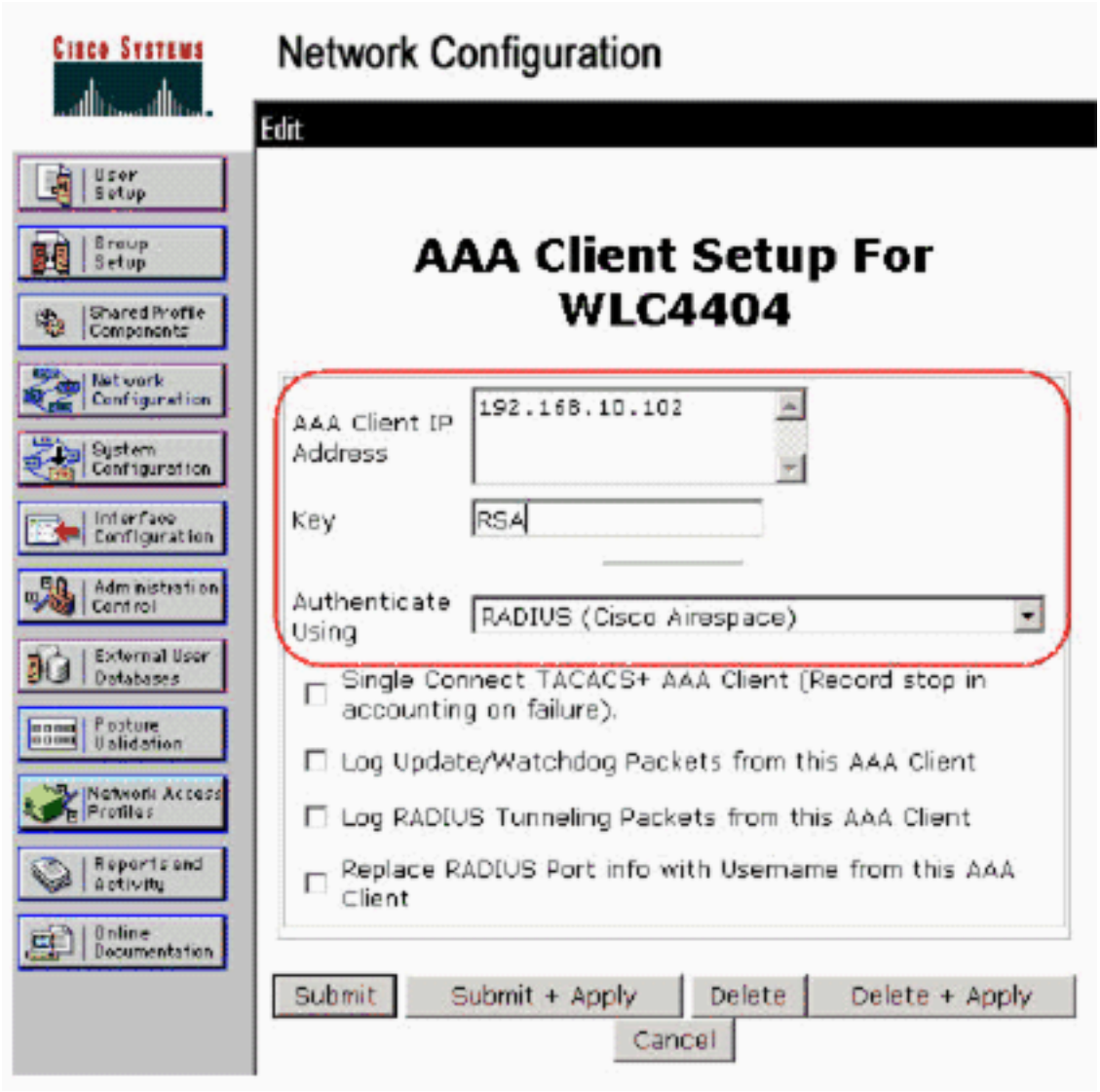


在Cisco ACS中添加RADIUS客户端

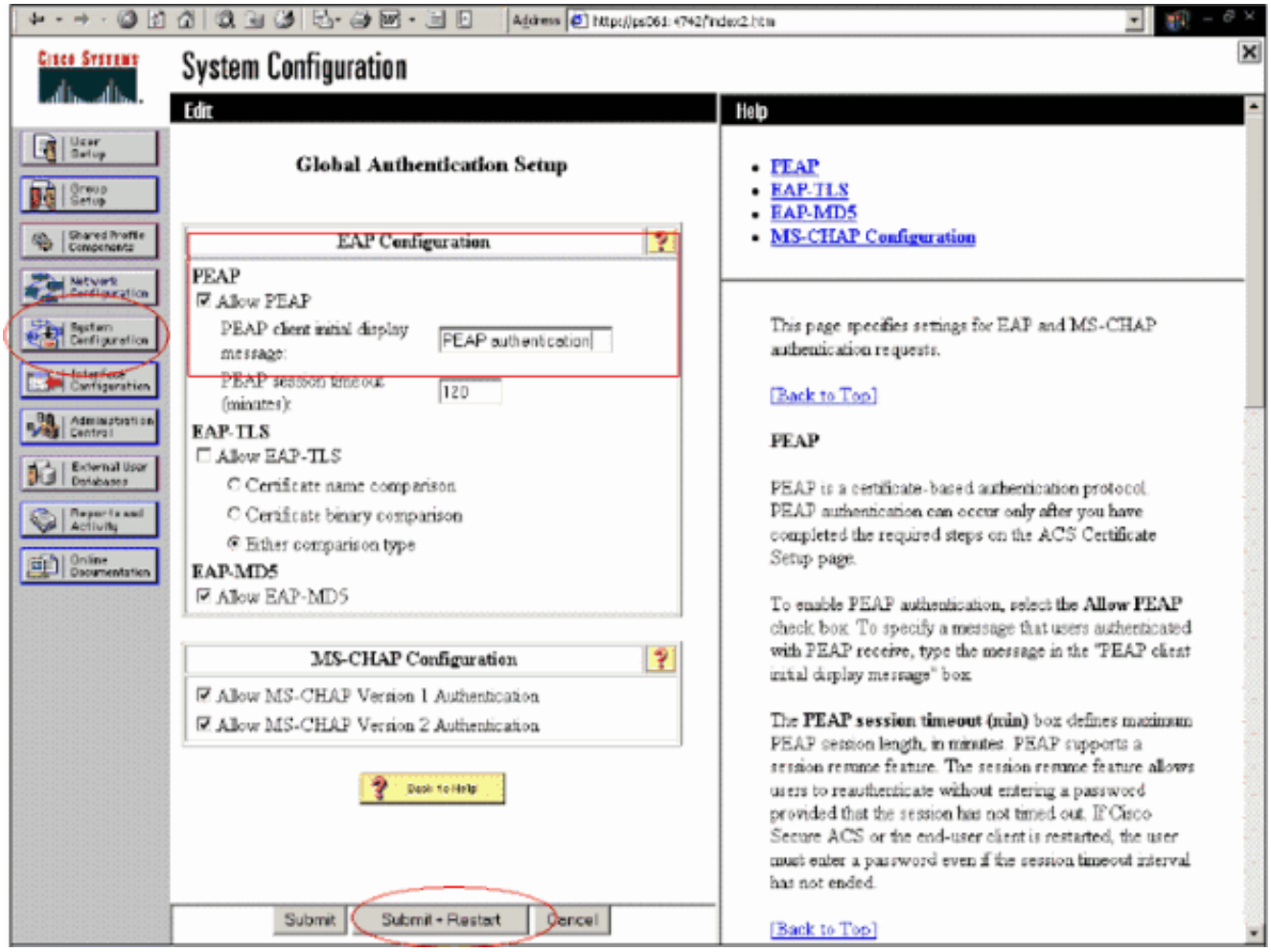
Cisco ACS服务器安装需要WLC的IP地址作为NAS，以将客户端PEAP身份验证转发到ACS。

请完成以下步骤：

1. 在**网络配置**下，为将要使用的WLC添加/编辑AAA客户端。输入AAA客户端和ACS之间使用的“共享密钥”（WLC通用）。为此**AAA客户端选择Authenticate Using > RADIUS(Cisco Airespace)**。然后，单击**提交+应用**。



2. 从已知的受信任证书颁发机构（如RSA Keon Certificate Authority）申请并安装服务器证书。有关此流程的详细信息，请参阅Cisco ACS随附的文档。如果您使用的是RSA Certificate Manager，则可以查看RSA Keon Aironet实施指南以获取其他帮助。您必须成功完成此任务，才能继续。**注意：**也可以使用自签名证书。有关如何使用这些ACS的信息，请参阅Cisco Secure ACS文档。
3. 在“**系统配置”>“全局身份验证设置”**下，选中“允许PEAP身份**验证”的**复选框。



为802.1x配置思科无线局域网控制器配置

请完成以下步骤：

1. 连接到WLC的命令行界面以配置控制器，以便可以将其配置为连接到Cisco Secure ACS服务器。
2. 从WLC中输入**config radius auth ip-address**命令，以配置RADIUS服务器进行身份验证。**注意**：使用RSA Authentication Manager RADIUS服务器进行测试时，请输入RSA Authentication Manager的RADIUS服务器的IP地址。使用Cisco ACS服务器测试时，输入Cisco Secure ACS服务器的IP地址。
3. 从WLC输入**config radius auth port**命令以指定用于身份验证的UDP端口。默认情况下，端口1645或1812在RSA身份验证管理器和思科ACS服务器中都处于活动状态。
4. 从WLC输入**config radius auth secret**命令，以在WLC上配置共享密钥。这必须与在RADIUS服务器中为此RADIUS客户端创建的共享密钥匹配。
5. 从WLC中输入**config radius auth enable**命令以启用身份验证。如果需要，请输入**config radius auth disable**命令以禁用身份验证。请注意，默认情况下禁用身份验证。
6. 在WLC上为所需WLAN选择适当的第2层安全选项。
7. 使用**show radius auth statistics**和**show radius summary命令**验证RADIUS设置是否已正确配置。**注意**：EAP请求超时的默认计时器较低，可能需要修改。这可以使用config advanced eap request-timeout**<seconds>命令来*完成***操作。它还有助于根据要求调整身份请求超时。这可以使用config advanced eap identity-request-timeout**<seconds>命令来*完成*。**

802.11无线客户端配置

有关如何配置无线硬件和客户端请求方的详细说明，请参阅各种思科文档。

已知问题

以下是RSA SecureID身份验证的一些众所周知的问题：

- RSA软件令牌。在XP2上使用这种身份验证形式时，不支持新的引脚模式和下一个令牌代码模式。(ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip的结果为FIXED)
- 如果您的ACS实施较旧或您没有上述补丁，则在用户从“已启用；新PIN模式”转换到“已启用”之前，客户端将无法进行身份验证。您可以通过让用户完成非无线身份验证或使用“测试身份验证”RSA应用程序来完成此操作。
- 拒绝4位/字母数字PIN。如果处于新PIN模式的用户违反PIN策略，则身份验证过程会失败，并且用户不知道如何操作或为什么。通常，如果用户违反策略，他们将收到一条消息，表明PIN被拒绝，并在再次向用户显示PIN策略是什么时再次收到提示（例如，如果PIN策略是5-7位，但用户输入4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
- 思科保护的可扩展身份验证协议
- 使用 RADIUS 服务器执行 EAP 身份验证
- 技术支持和文档 - Cisco Systems