使用 EAP-FAST 身份验证的 Cisco 安全服务客户端

目录

简介

本文档介绍如何使用无线 LAN 控制器、Microsoft Windows 2000® 软件和 Cisco 安全访问控制服务器 (ACS) 4.0 通过 EAP-FAST 来配置 Cisco 安全服务客户端 (CSSC)。本文档简要介绍 EAP-FAST 体系结构，并且提供部署和配置示例。CSSC 是一种客户端软件组件，可向基础架构提供用户凭据通信，以便在网络上对用户进行身份验证并向其分配适当的访问权限。

如本文档所述，CSSC 解决方案具有以下优点：

- 在授予对 WLAN/LAN 的访问权限之前，通过可扩展身份验证协议 (EAP) 对每个用户（或设备）进行身份验证
- 通过服务器、验证器和客户端组件，实现端到端的 WLAN 安全解决方案

- 适用于有线和无线身份验证的通用解决方案
- 动态，取决于在身份验证过程派生的用户加密密钥
- 不需要公钥基础架构 (PKI) 或证书（证书验证是可选的）
- 访问策略分配和/或支持 NAC 的 EAP 框架

注意： 有关安全的无线部署的信息，请参阅 Cisco SAFE 无线蓝图。

802.1x 身份验证框架已成为 802.11i（无线局域网安全）标准的一部分，可在 802.11 无线局域网中启用基于第 2 层的身份验证、授权和记账功能。如今，有几种 EAP 协议可用于在有线和无线网络中进行部署。部署的常见 EAP 协议包括 LEAP、PEAP 和 EAP-TLS。除了这些协议外，Cisco 还定义和实施了通过安全隧道 (EAP-FAST) 协议的 EAP 灵活身份验证，作为一种基于标准的 EAP 协议，可部署在有线和无线局域网中。EAP-FAST 协议规范在 IETF 网站上公开提供。

与其他一些 EAP 协议一样，EAP-FAST 是一种客户端/服务器安全体系结构，可在 TLS 隧道中对 EAP 事务进行加密。在这方面，EAP-FAST 与 PEAP 或 EAP-TTLS 类似。但是 EAP-FAST 建立隧道时基于每个用户唯一的强共享密钥，而 PEAP/EAP-TTLS 则不同，后者使用服务器 X.509 证书来保护身份验证会话。这些共享密钥称为保护访问凭据 (PAC)，可以自动（自动或带内配置）或手动（手动或带外配置）分配到客户端设备。由于基于共享密钥的握手比基于 PKI 基础架构的握手更为高效，因此在提供受保护的身份验证交换的 EAP 中，EAP-FAST 速度最快而占用的处理器较少。EAP-FAST 还可以简化部署，因为它不要求无线局域网客户端或 RADIUS 基础架构提供证书，而且还融入了内置的配置机制。

下面是 EAP-FAST 协议的一些主要功能：

- 使用 Windows 用户名/密码实现单一登录 (SSO)
- 可执行登录脚本
- 无需第三方请求方即可实现 Wi-Fi 保护访问 (WPA)（仅限 Windows 2000 和 XP）
- 部署简单，无需 PKI 基础架构
- Windows 密码老化（即，支持基于服务器的密码过期）
- 与 Cisco Trust Agent 集成，可通过适当的客户端软件实现网络准入控制

先决条件

需求

假设安装者已经掌握基本的 Windows 2003 安装和 Cisco WLC 安装知识，因为本文档仅涵盖有助于开展测试的特定配置。

Cisco的初始安装和配置信息4400系列控制器，是指:快速入门指南：Cisco 4400 Series Wireless LAN Controllers。有关 Cisco 2000 系列控制器的初始安装和配置信息，请参阅快速入门指南：Cisco 2000 系列无线局域网控制器。

开始之前，请先安装 Microsoft Windows Server 2000 以及最新的 Service Pack 软件。安装控制器和轻量接入点 (LAP) 并确保配置了最新的软件更新。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行 4.0.155.5 的 Cisco 2006 或 4400 系列控制器
- Cisco 1242 LWAPP AP

- Windows 2000，装有 Active Directory
- Cisco Catalyst 3750G 交换机
- Windows XP，装有 CB21AG 适配器卡和 Cisco 安全服务客户端 4.05 版

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

设计参数

数据库

当您部署 WLAN 网络并寻找身份验证协议时，通常希望使用用户/计算机身份验证的当前数据库。可以使用的典型数据库包括：Windows Active Directory、LDAP 或一次性密码 (OTP) 数据库（即，RSA 或 SecureID）。所有这些数据库都与 EAP-FAST 协议兼容，但是当您规划部署时，必须考虑一些兼容性要求。最初将 PAC 文件部署到客户端时，是通过匿名自动配置、经过身份验证的配置（通过当前客户端 X.509 证书）或手动配置来实现的。对于本文档，考虑使用匿名自动配置和手动配置。

自动 PAC 配置方式使用经过身份验证的 Diffie-Hellman 密钥协商协议 (ADHP) 来建立安全隧道。安全隧道可以通过匿名或通过服务器身份验证机制的方式来建立。在已建立的隧道连接内，MS-CHAPv2 用于对客户端进行身份验证，并且在身份验证成功后，用于向客户端分配 PAC 文件。在成功配置 PAC 之后，该 PAC 文件可用于启动新的 EAP-FAST 身份验证会话，以便获得安全的网络访问。

自动 PAC 配置方式与正在使用的数据库密切相关，其原因在于自动配置机制依赖于 MSCHAPv2，因此用于对用户进行身份验证的数据库必须与此密码格式兼容。如果与 EAP-FAST 配合使用的数据库不支持 MSCHAPv2 格式（例如 OTP、Novell 或 LDAP），则必须使用其他机制（即，手动配置或经过身份验证的配置）来部署用户 PAC 文件。本文档提供了使用 Windows 用户数据库进行自动配置的示例。

加密

EAP-FAST 身份验证不要求使用特定的 WLAN 加密类型。要使用的 WLAN 加密类型取决于客户端 NIC 卡的功能。建议使用 WPA2 (AES-CCM) 或 WPA (TKIP) 加密，具体取决于特定部署中的 NIC 卡功能。请注意，Cisco WLAN 解决方案允许在一个公用的 SSID 上同时存在 WPA2 和 WPA 客户端设备。

如果客户端设备不支持 WPA2 或 WPA，可以使用动态 WEP 密钥来部署 802.1X 身份验证，但是由于众所周知的 WEP 密钥攻击，建议不要使用这种 WLAN 加密机制。如果必须支持仅限 WEP 的客户端，建议使用会话超时时间间隔，从而要求客户端经常派生新的 WEP 密钥。对于典型的 WLAN 数据传输速率，建议的会话时间间隔是 30 分钟。

单一登录和计算机凭据

单一登录是指用户只需登录一次或输入一次身份验证凭据，就能访问多个应用程序或多个设备。对于本文档，单一登录是指使用凭据登录到一台 PC，从而在 WLAN 上通过身份验证。

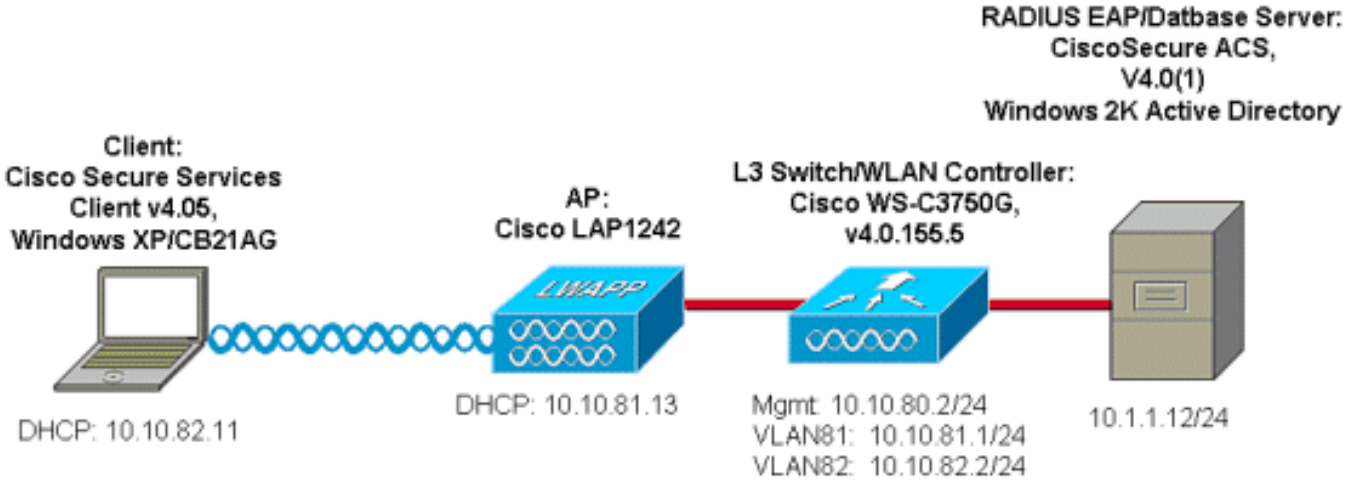
使用 Cisco 安全服务客户端，可以使用某个用户的登录凭据，在 WLAN 网络上通过身份验证。如果必须先在网络上对 PC 进行身份验证，然后才能由用户登录该 PC，则必须使用存储的用户凭据或

绑定到计算机配置文件的凭据。如果需要在 PC 启动时（而不是在用户登录时）运行登录脚本或映射驱动器，则这些方法都很有帮助。

网络图

下面是本文档中使用的网络图。在此网络中，使用了四个子网。请注意，不必将这些设备分段到不同的网络中，但是这么做可以为实际网络的集成提供最高的灵活性。Catalyst 3750G 集成无线局域网控制器在一个公用的机箱中提供以太网供电 (POE) 交换机端口、L3 交换和 WLAN 控制器功能。

1. 网络 10.1.1.0 是 ACS 所在的服务器网络。
2. 网络 10.10.80.0 是由 WLAN 控制器使用的管理网络。
3. 网络 10.10.81.0 是 AP 所在的网络。
4. 网络 10.10.82.0 用于 WLAN 客户端。



配置访问控制服务器 (ACS)

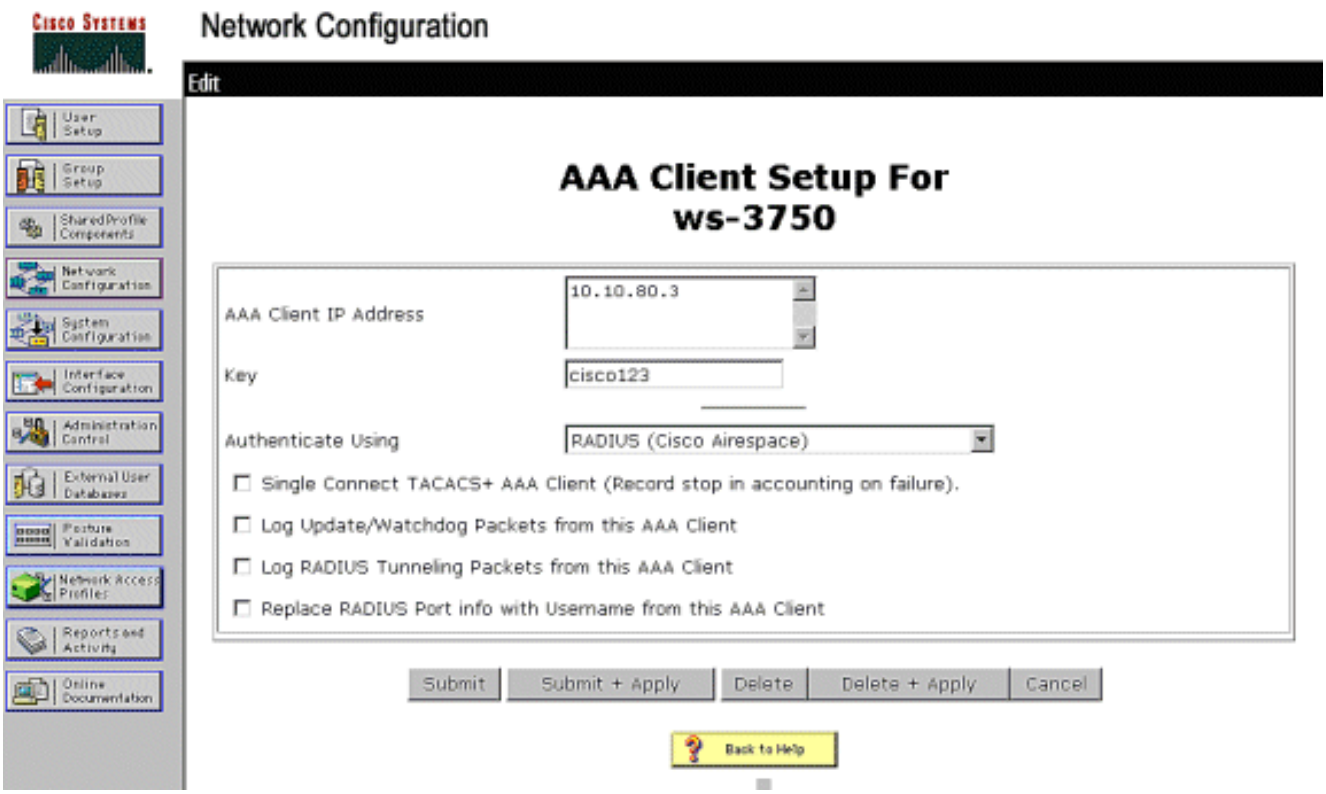
本部分提供有关如何配置本文档所述功能的信息。

注意： 有关本文档所用命令的详细信息，请使用命令查找工具（仅限注册用户）。

在 ACS 中添加接入点作为 AAA 客户端 (NAS)

本部分介绍如何使用 Windows Active Directory 作为外部数据库，通过带内 PAC 配置方式为 EAP-FAST 配置 ACS。

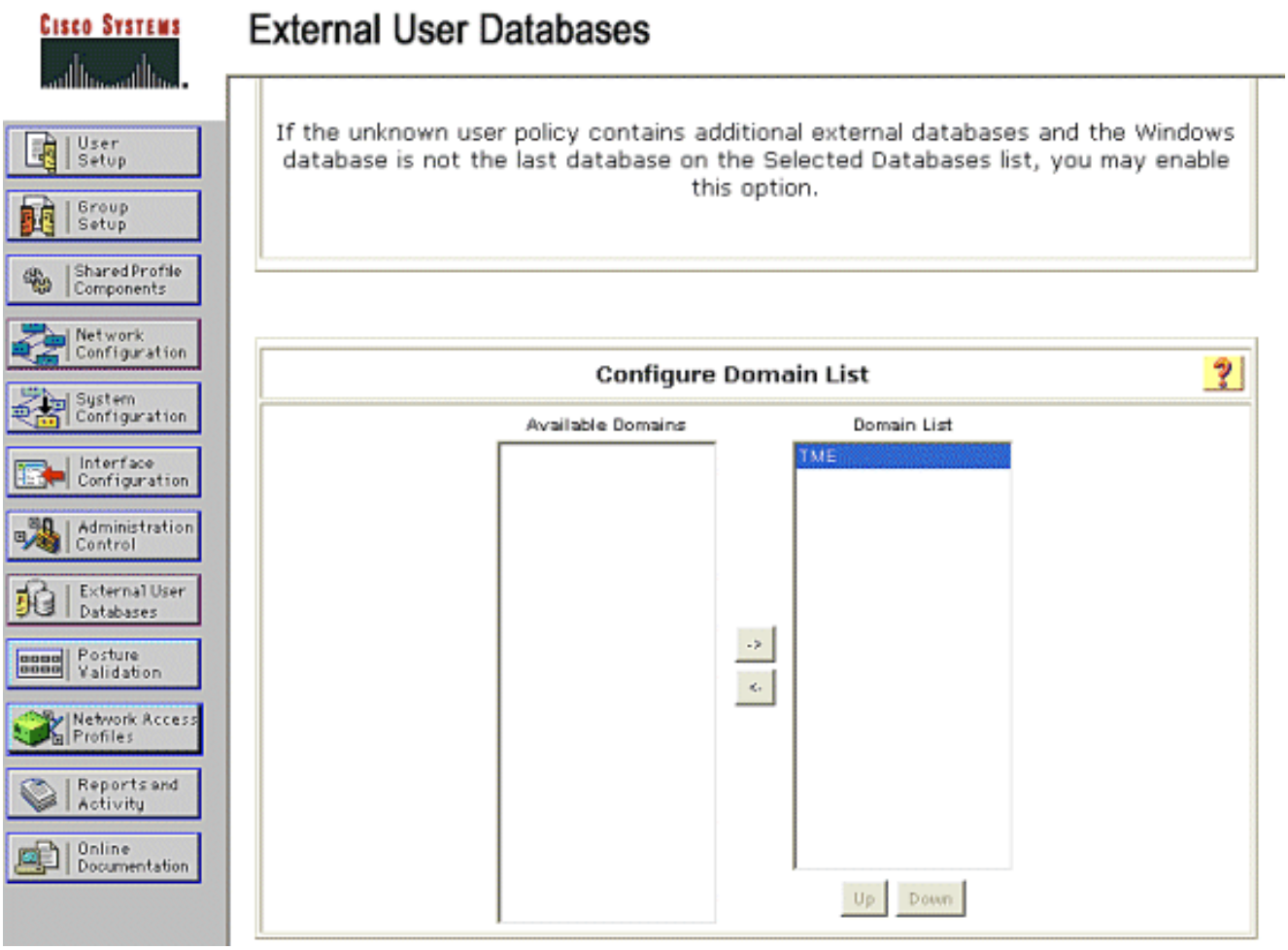
1. 登录到 **ACS > Network Configuration**，然后单击“Add Entry”。
2. 填写 WLAN 控制器名称、IP 地址、共享密钥，然后在“Authenticate Using”下，选择“RADIUS (Cisco Airespace)”，此身份验证方法还包括 RADIUS IETF 属性。**注意：** 如果启用了网络设备组 (NDG)，请先选择适当的 NDG，然后再向其中添加 WLAN 控制器。有关 NDG 的详细信息，请参阅 ACS 配置指南。
3. 单击 **Submit+ Restart**。



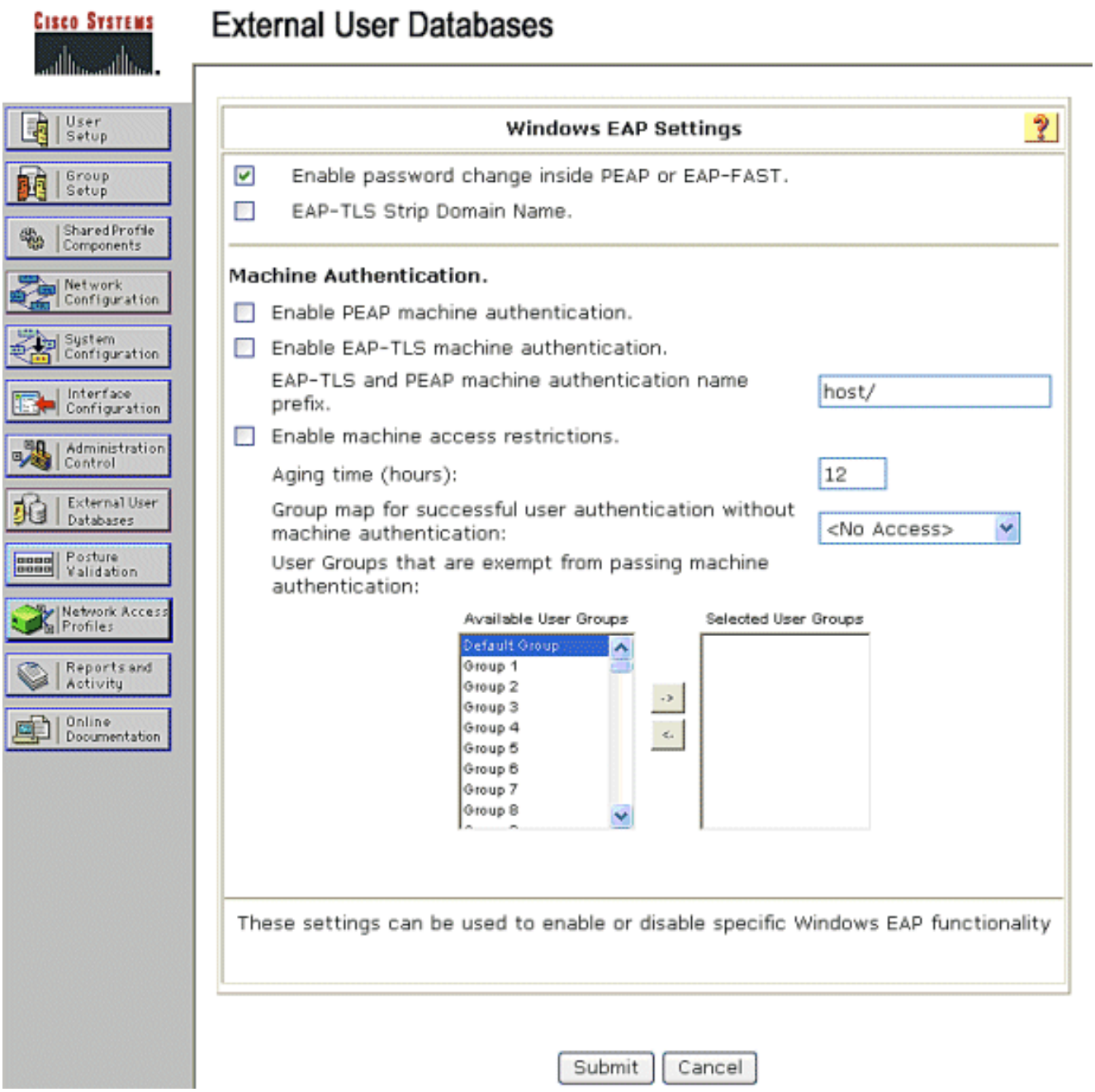
配置 ACS 以便查询外部数据库

本部分介绍如何配置 ACS 以便查询外部数据库。

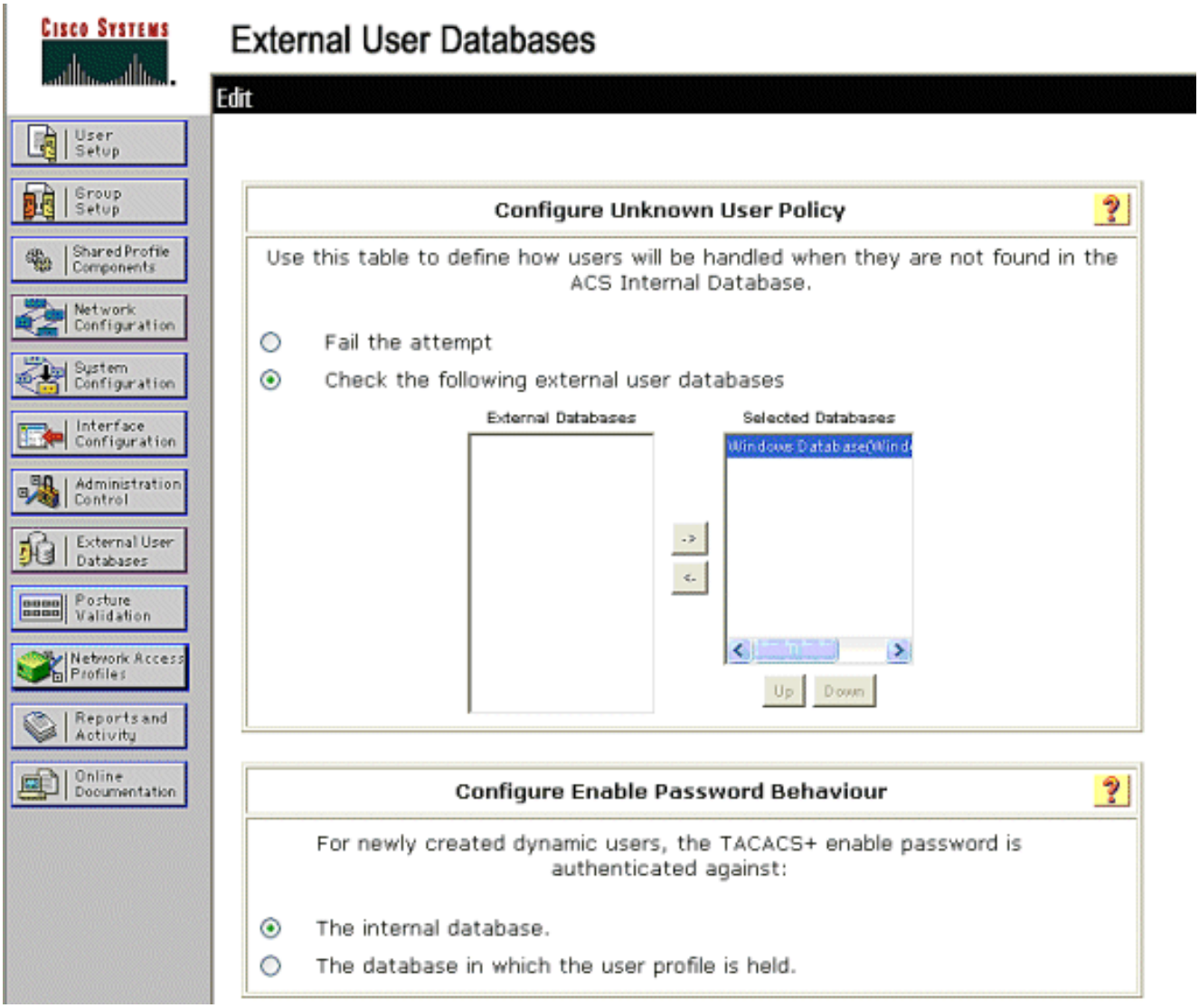
1. 单击 **External User Database > Database Configuration > Windows Database > Configure**。
2. 在“Configure Domain List”下，将 **Domains** 从“Available Domains”移到“Domain List”中。**注意**：运行 ACS 的服务器必须了解这些域，ACS 应用程序才能检测这些域，并将这些域用于身份验证。



3. 在“Windows EAP Settings”下，配置选项，允许在 PEAP 或 EAP-FAST 会话中更改密码。有关 EAP-FAST 和 Windows 密码老化的详细信息，请参阅 Cisco Secure ACS 4.1 配置指南。
4. 单击 **submit**。**注意：** 您也可以在“Windows User Database Configuration”下为 EAP-FAST 启用“Dialin Permission”特性，以便使用 Windows 外部数据库来控制访问权限。Windows 数据库配置页上有关密码更改的“MS-CHAP Settings”仅适用于非 EAP 的 MS-CHAP 身份验证。要允许通过 EAP-FAST 进行密码更改，必须在“Windows EAP Settings”下启用密码更改。



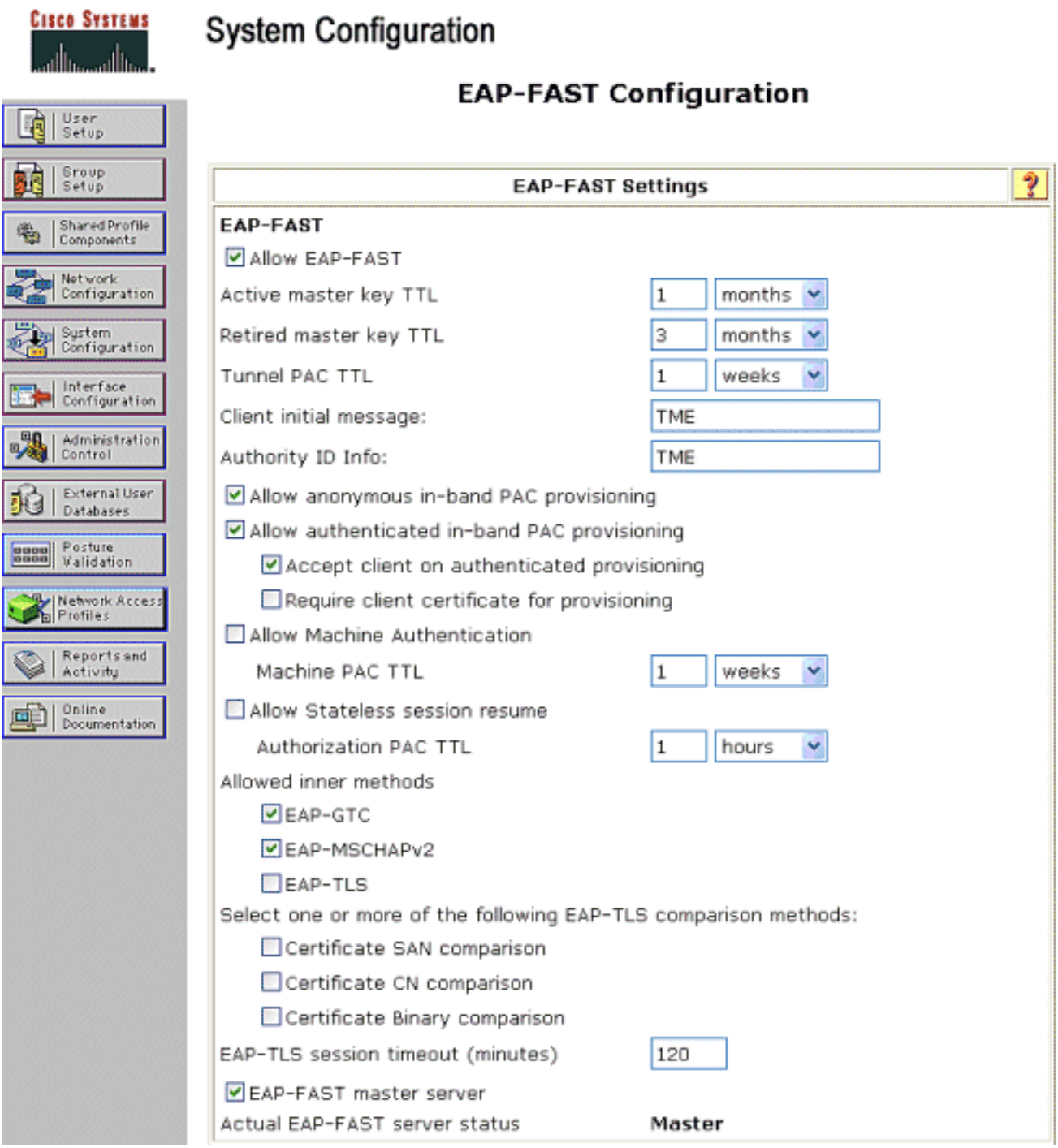
5. 单击 **External User Database > Unknown User Policy**，然后选择“Check the following external user databases”单选按钮。
6. 将“Windows Database”从 **External Databases** 移到“Selected Databases”中。
7. 单击 **submit**。**注意：** 从此时起，ACS 就会查看 Windows DB。如果在 ACS 本地数据库中未找到用户，它会将该用户放到 ACS 默认组中。有关数据库组映射的详细信息，请参阅 ACS 文档。**注意：** 当 ACS 查询 Microsoft Active Directory 数据库来验证用户凭据时，还需要在 Windows 上配置更多访问权限设置。有关详细信息，请参阅 Cisco Secure ACS for Windows Server 安装指南。



在 ACS 上启用 EAP-FAST 支持

本部分介绍如何在 ACS 上启用 EAP-FAST 支持。

1. 转至 **System Configuration > Global Authentication Setup > EAP-FAST Configuration**。
2. 选择 **Allow EAP-FAST**。
3. 建议配置以下选项：Master key TTL/ Retired master key TTL/ PAC TTL。默认情况下，Cisco Secure ACS 中会配置以下设置：主密钥TTL:1月Retired Key TTL：3 个月PAC TTL：1 周
4. 填写 **Authority ID Info** 字段。如果所选的 PAC 颁发机构是控制器，则此文字会显示在某些 EAP-FAST 客户端软件中。**注意：** Cisco 安全服务客户端不会对 PAC 颁发机构使用此描述性的文字。
5. 选择 **Allow in-band PAC provisioning** 字段。此字段为正确启用 EAP-FAST 的客户端启用自动 PAC 配置。此示例使用了自动配置。
6. 选择 **Allowed inner methods**：EAP-GTC 和 EAP-MSCHAP2。这样就同时允许 EAP-FAST v1 和 EAP-FAST v1a 客户端的操作。（Cisco 安全服务客户端支持 EAP-FAST v1a。）如果不必支持 EAP-FAST v1 客户端，则仅需要启用 EAP-MSCHAPv2 作为内部方法。
7. 选中 **EAP-FAST Master Server** 复选项，使此 EAP-FAST 服务器成为主服务器。这使得其他 ACS 服务器能够将此服务器用作主 PAC 颁发机构，从而避免为网络中的每个 ACS 都配置唯一的密钥。有关详细信息，请参阅 ACS 配置指南。
8. 单击 **Submit+Restart**。



Cisco WLAN 控制器

对于本部署指南，使用 Cisco WS3750G 集成无线局域网控制器 (WLC) 与 Cisco AP1240 轻量 AP (LAP) 配合，为 CSSC 测试提供 WLAN 基础架构。该配置适用于任何 Cisco WLAN 控制器。所使用的软件版本是 4.0.155.5。

配置无线局域网控制器

控制器的基本操作和 LAP 注册

使用命令行界面 (CLI) 中的启动配置向导来配置 WLC，以便进行基本操作。此外，也可以使用 GUI 来配置 WLC。本文档介绍用 CLI 中的启动配置向导对 WLC 进行的配置。

首次启动 WLC 之后，它将进入启动配置向导。使用配置向导来配置基本设置。可以通过 CLI 或

GUI 来访问该向导。以下输出展示 CLI 中启动配置向导的示例：

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: ws-3750 Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): ***** Management Interface IP Address:
10.10.80.3 Management Interface Netmask: 255.255.255.0 Management Interface Default Router:
10.10.80.2 Management Interface VLAN Identifier (0 = untagged): Management Interface DHCP Server
IP Address: 10.10.80.2 AP Manager Interface IP Address: 10.10.80.4 AP-Manager is on Management
subnet, using same values AP Manager Interface DHCP Server (172.16.1.1): Virtual Gateway IP
Address: 1.1.1.1 Mobility/RF Group Name: Security Network Name (SSID): Enterprise Allow Static
IP Addresses [YES][no]: yes Configure a RADIUS Server now? [YES][no]: no Warning! The default
WLAN security policy requires a RADIUS server. Please see documentation for more details. Enter
Country Code (enter 'help' for a list of countries) [US]: Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes Enable 802.11g Network [YES][no]: yes Enable Auto-RF
[YES][no]: yes Configuration saved! Resetting system with new configuration.
```

这些参数为基本操作设置 WLC。在此示例配置中，WLC 使用 **10.10.80.3** 作为管理接口 IP 地址，使用 10.10.80.4 作为 AP 管理器接口 IP 地址。

在 WLC 上配置其他任何特性之前，必须在 WLC 上注册 LAP。本文档假设已经在 WLC 上注册了 LAP。有关如何在 WLC 上注册轻量 AP 的信息，请参阅轻量接入点的 WLAN 控制器故障切换配置示例的在 WLC 上注册轻量 AP 部分。对于此配置示例，AP1240 从 WLAN 控制器 (10.10.81.0/24) 部署到单独的子网 (10.10.80.0/24) 中，而 DHCP 选项 43 用于提供控制器发现功能。

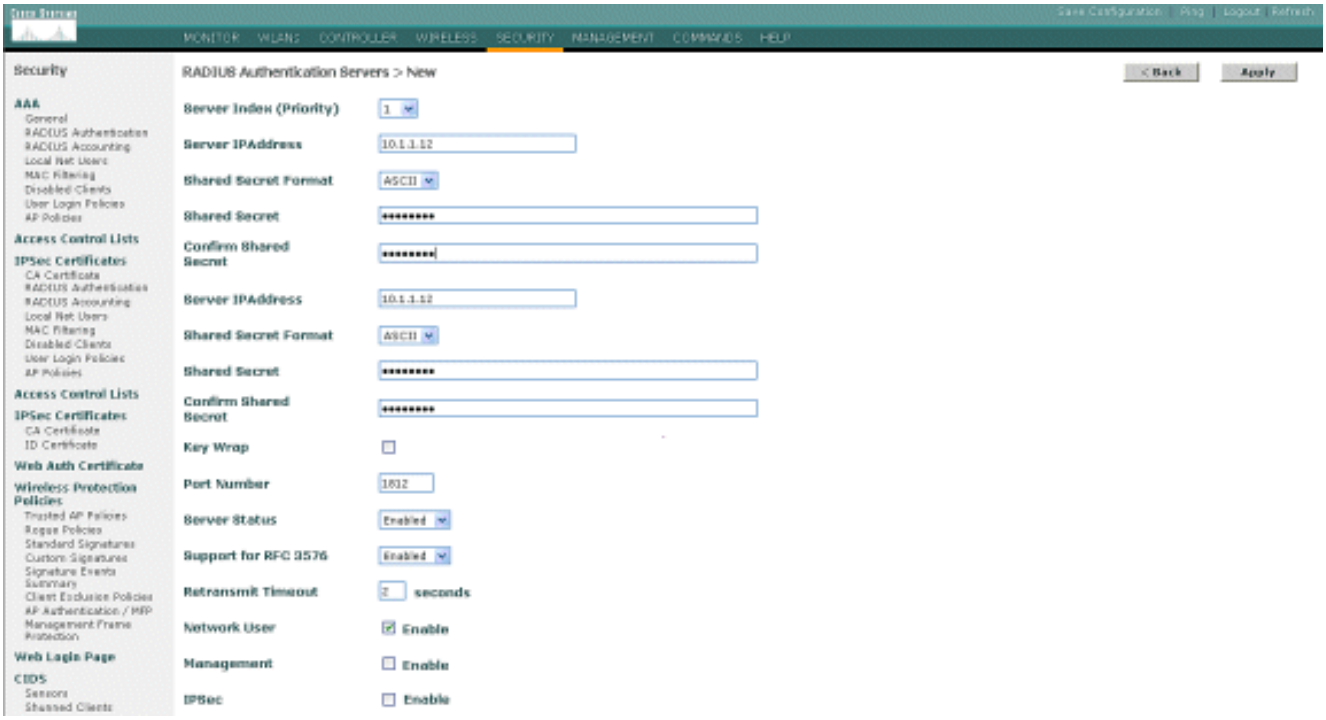
通过 Cisco Secure ACS 执行 RADIUS 身份验证

必须配置 WLC，使其将用户凭据转发给 Cisco Secure ACS 服务器。然后，ACS 服务器验证用户凭据（通过已配置的 Windows 数据库），并向无线客户端提供访问权限。

要配置 WLC，以便与 ACS 服务器进行通信，请完成以下步骤：

1. 在控制器的 GUI 中单击 **Security** 和“RADIUS Authentication”，以显示“RADIUS Authentication Servers”页。然后单击 **New** 以定义 ACS 服务器。

2. 在“RADIUS Authentication Servers > New”页中定义 ACS 服务器参数。这些参数包括 ACS IP 地址、共享密钥、端口号和服务器状态。**注意：** 端口号 1645 或 1812 与 ACS 兼容，可用于 RADIUS 身份验证。“Network User”和“Management”复选框决定基于 RADIUS 的身份验证是否适用于网络用户（例如 WLAN 客户端）和管理（即管理用户）。示例配置使用 Cisco Secure ACS 作为 RADIUS 服务器，其 IP 地址为 10.1.1.12：



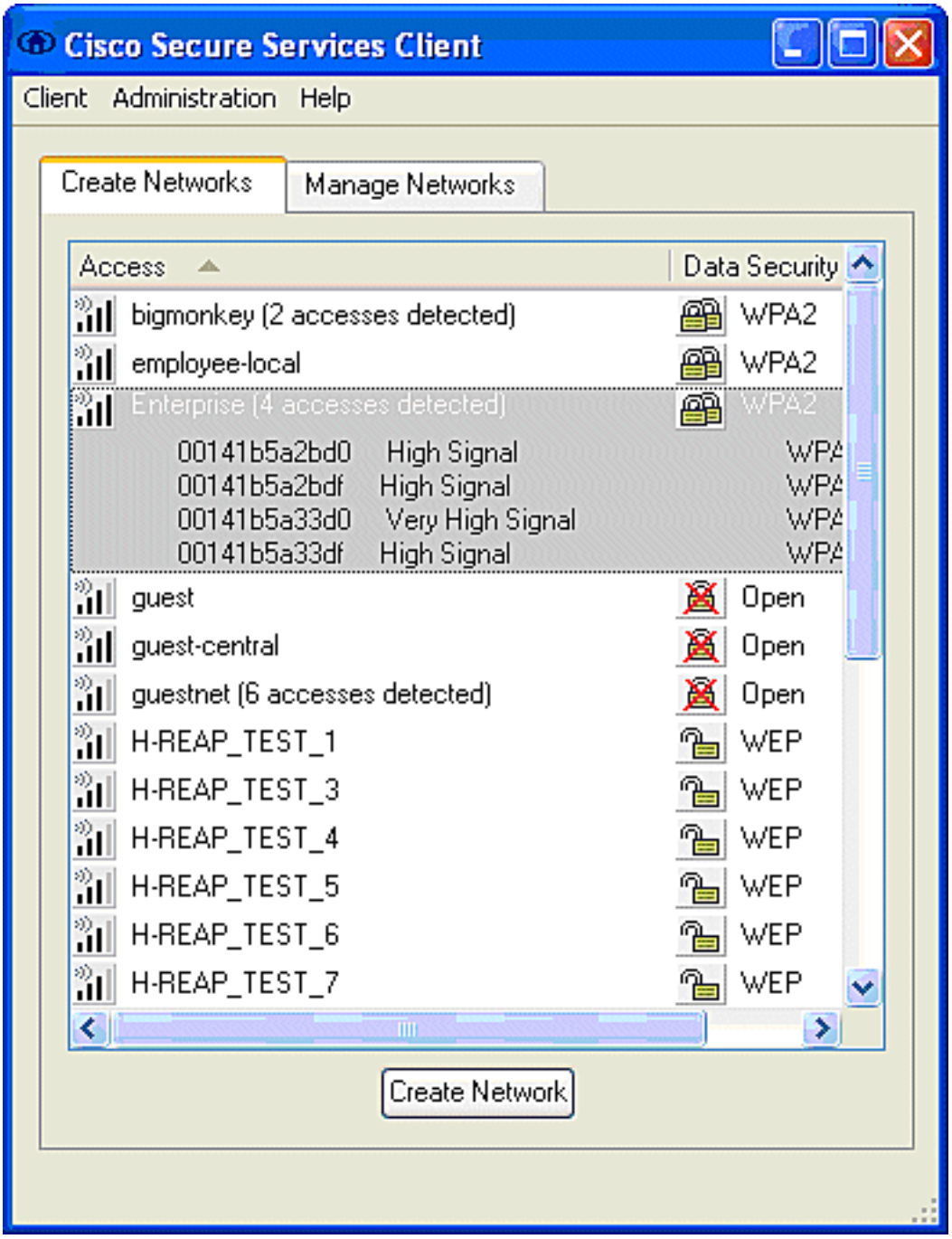
WLAN 参数配置

本部分介绍 Cisco 安全服务客户端的配置。在本示例中，使用 CSSC v4.0.5.4783 与 Cisco CB21AG 客户端适配器配合。在安装 CSSC 软件之前，需确认只安装了 CB21AG 的驱动程序，而无需安装 Aironet Desktop Utility (ADU)。

软件安装并作为服务运行后，它就会扫描并显示可用的网络。

注意： CSSC 会禁用 Windows Zero Config。

注意： 只能看到为广播启用的那些 SSID。



注意： 默认情况下，WLAN 控制器会广播 SSID，使其显示在扫描到的 SSID 的“Create Networks”列表中。要创建网络配置文件，只需单击列表中的 **SSID** (Enterprise) 和“Create Network”单选按钮。

如果 WLAN 基础架构的配置中禁用了广播 SSID，则必须手动添加 SSID；单击“Access Devices”下的 **Add** 单选按钮，然后手动输入适当的 SSID（例如 Enterprise）。为客户端配置“Active”探测行为，即客户端主动探测其配置的 SSID；在“Add Access Device”窗口中输入 SSID 之后，指定 **Actively search for this access device**。

注意： 如果不是首次为配置文件配置 EAP 身份验证设置，则端口设置不允许企业模式 (802.1X)。

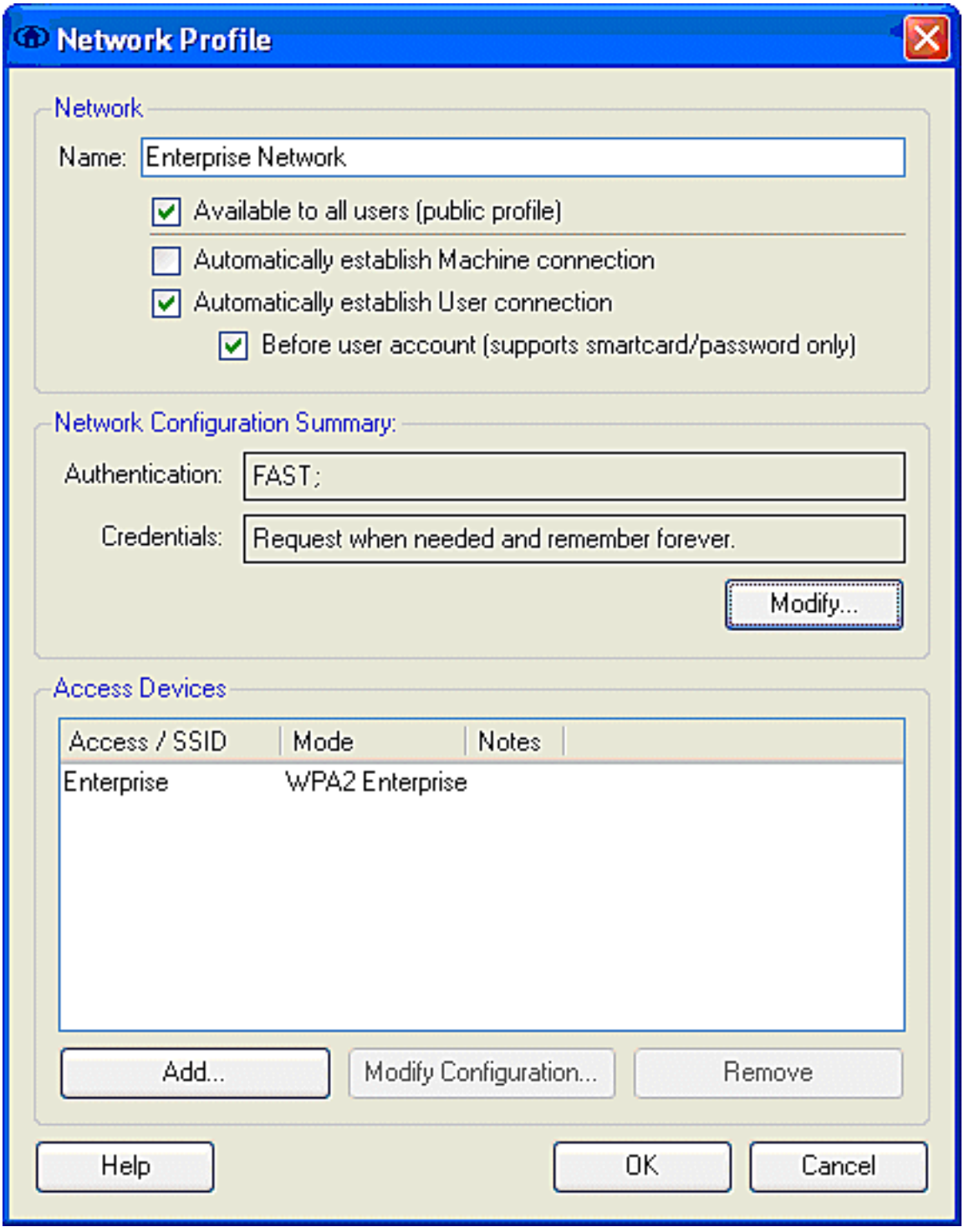
Create Network 单选按钮将启动“Network Profile”窗口，用于将所选（或已配置的）SSID 与身份验证机制相关联。为配置文件指定描述性名称。

注意： 在此身份验证配置文件下，可以关联多种 WLAN 安全类型和/或 SSID。

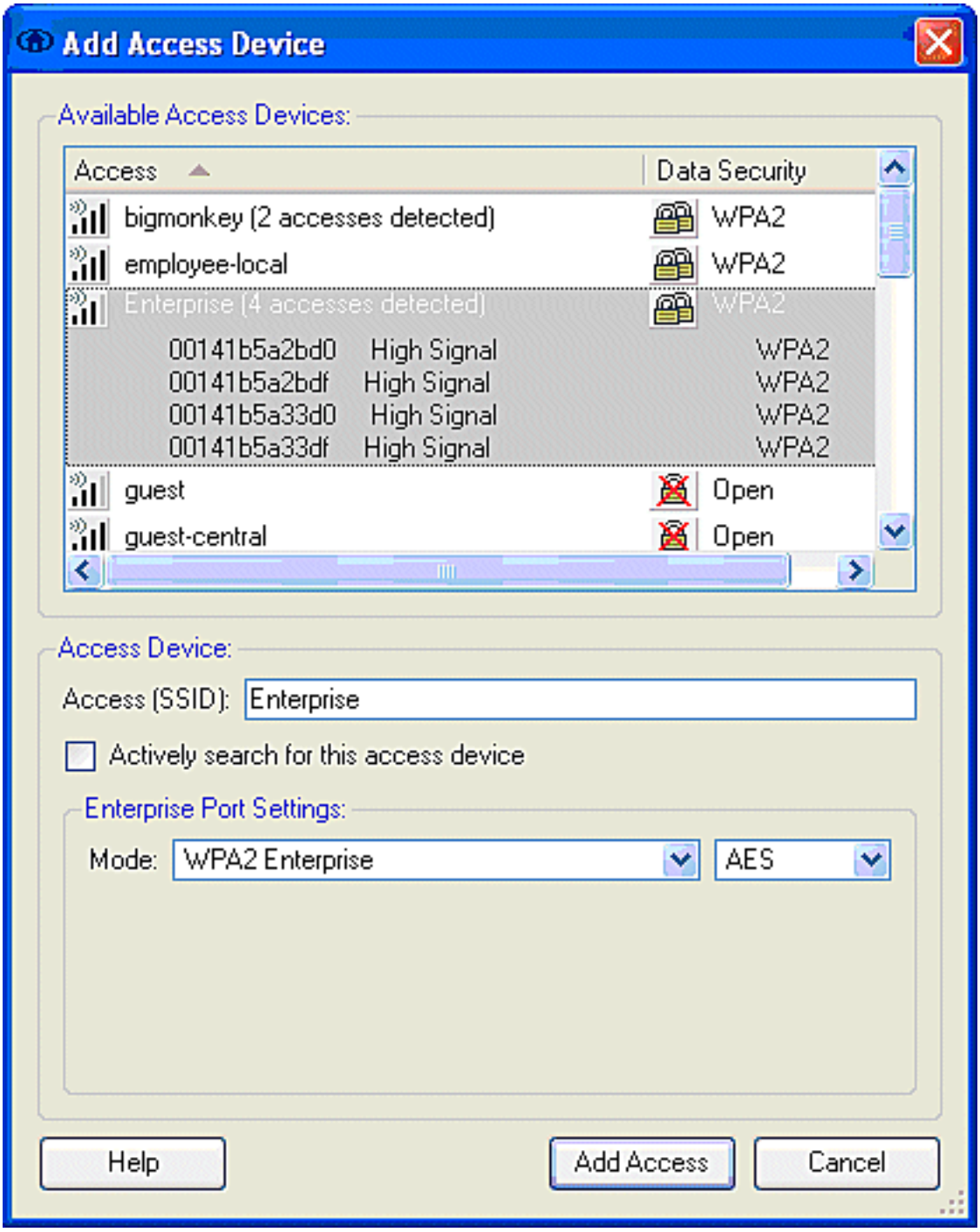
要使客户端在 RF 覆盖范围内时自动连接到网络，请选择 **Automatically establish User**

connection。如果该计算机上的其他用户帐户无需使用此配置文件，请取消选中 **Available to all users**。如果选中了 **Automatically establish**，则用户必须打开 CSSC 窗口，并通过“Connect”单选按钮手动启动 WLAN 连接。

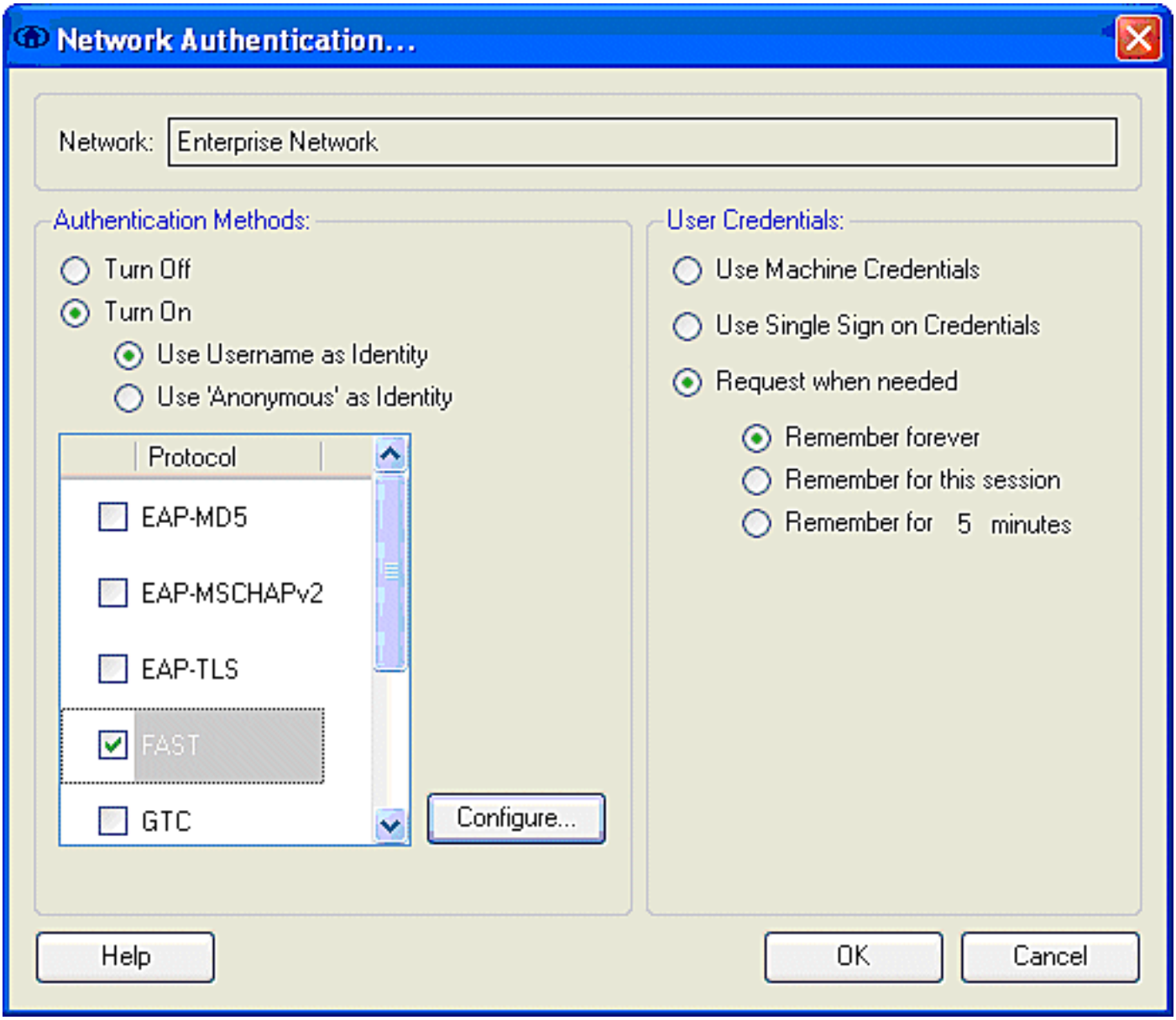
如果需要在用户登录之前启动 WLAN 连接，请选中 **Before user account**。这样就会使用已保存的用户凭据（在 EAP-FAST 中使用 TLS 时，则为密码或证书/智能卡）实现单一登录操作。



注意： 对于使用 Cisco Aironet 350 系列客户端适配器的 WPA/TKIP 操作，必须禁用 WPA 握手验证，因为目前 WPA 握手哈希验证在 CSSC 客户端与 350 驱动程序之间不兼容。这是在 **Client > Advanced Settings > WPA/WPA2 Handshake Validation** 下禁用的。禁用的握手验证仍然允许 WPA 内继承的安全特性（TKIP 每数据包密钥和消息完整性检查），但会禁用初始的 WPA 密钥身份验证。



在“Network Configuration Summary”下，单击 **Modify** 以配置 EAP/凭据设置。指定 **Turn On** 身份验证，在“Protocol”下选择“FAST”，然后选择“Anonymous”作为“Identity”（为了避免在初始 EAP 请求中使用用户名）。可以使用 **Use Username as Identity** 作为外部 EAP 身份，但是许多客户都不希望在最初未加密的 EAP 请求中暴露用户 ID。指定 **Use Single Sign on Credentials**，以使用登录凭据进行网络身份验证。单击 **Configure** 以设置 EAP-FAST 参数。



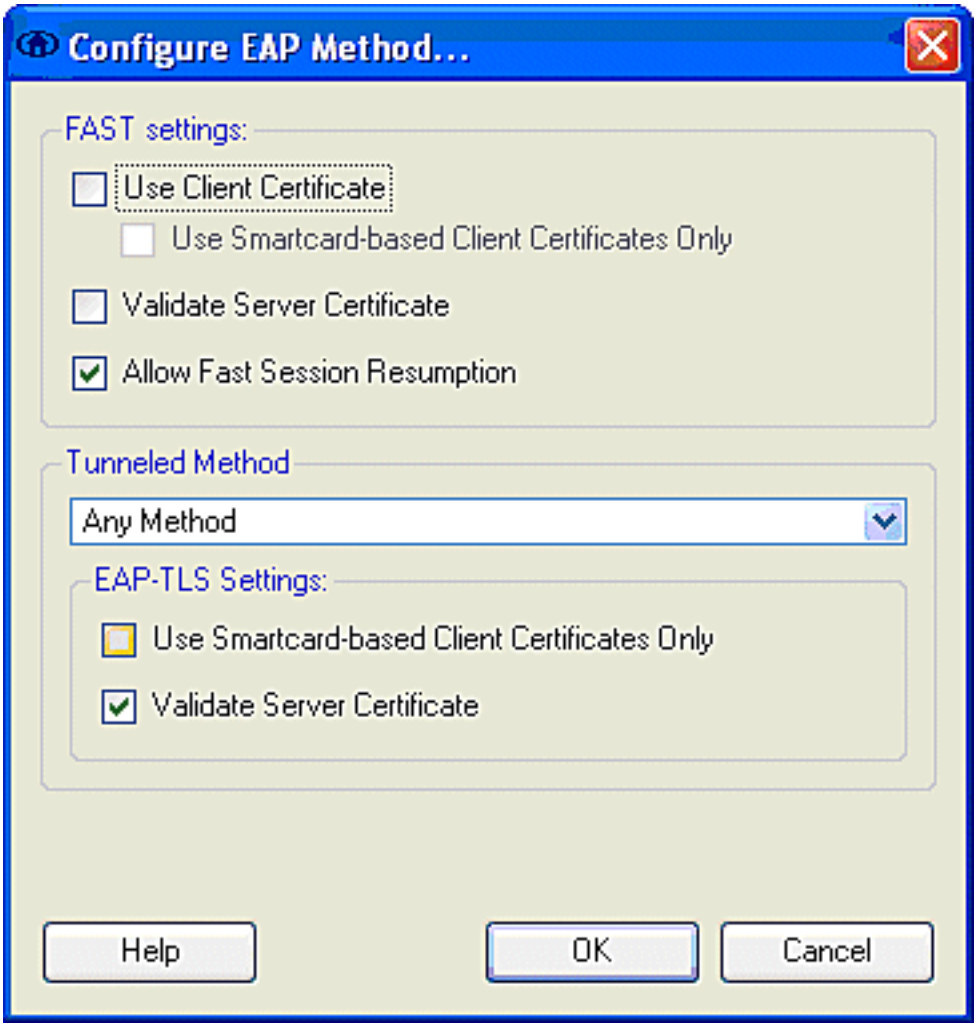
在 FAST 设置下，可以指定 **Validate Server Certificate**，使客户端能够在建立 EAP-FAST 会话之前验证 EAP-FAST 服务器 (ACS) 证书。这会为客户端设备提供保护，防止连接到未知或非法的 EAP-FAST 服务器，并防止无意中将其身份验证凭据提交给不受信任的源。这将要求在 ACS 服务器上安装证书，并且在客户端上安装相应的根证书颁发机构证书。在本示例中，未启用服务器证书验证。

在 FAST 设置下，可以指定 **Allow Fast Session Resumption**，允许恢复基于隧道（TLS 会话）的 EAP-FAST 会话信息，而无需完整的 EAP-FAST 重新验证。如果 EAP-FAST 服务器和客户端在初次 EAP-FAST 身份验证交换过程中协商了 TLS 会话信息，则可以发生会话恢复。

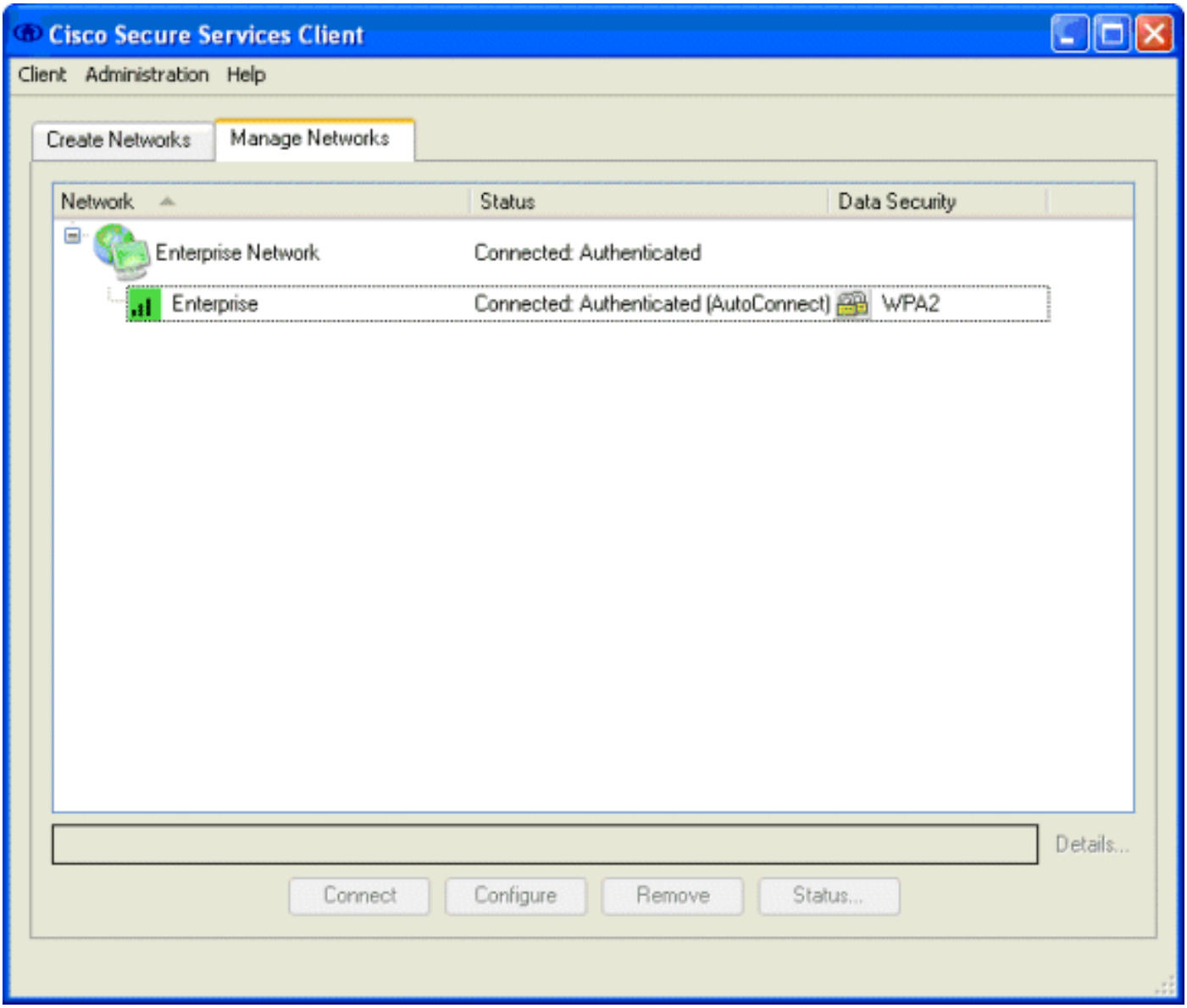
注意： EAP-FAST 服务器和客户端都必须配置，以进行 EAP-FAST 会话恢复。

在“Tunneled Method > EAP-TLS Settings”下，指定 **Any Method**，以允许 EAP-MSCHAPv2 进行 PAC 自动配置，并允许 EAP-GTC 进行身份验证。如果使用 Microsoft 格式的数据库（例如 Active Directory），并且网络上不支持任何 EAP-FAST v1 客户端，也可以指定仅使用 **MSCHAPv2** 作为“Tunneled Method”。

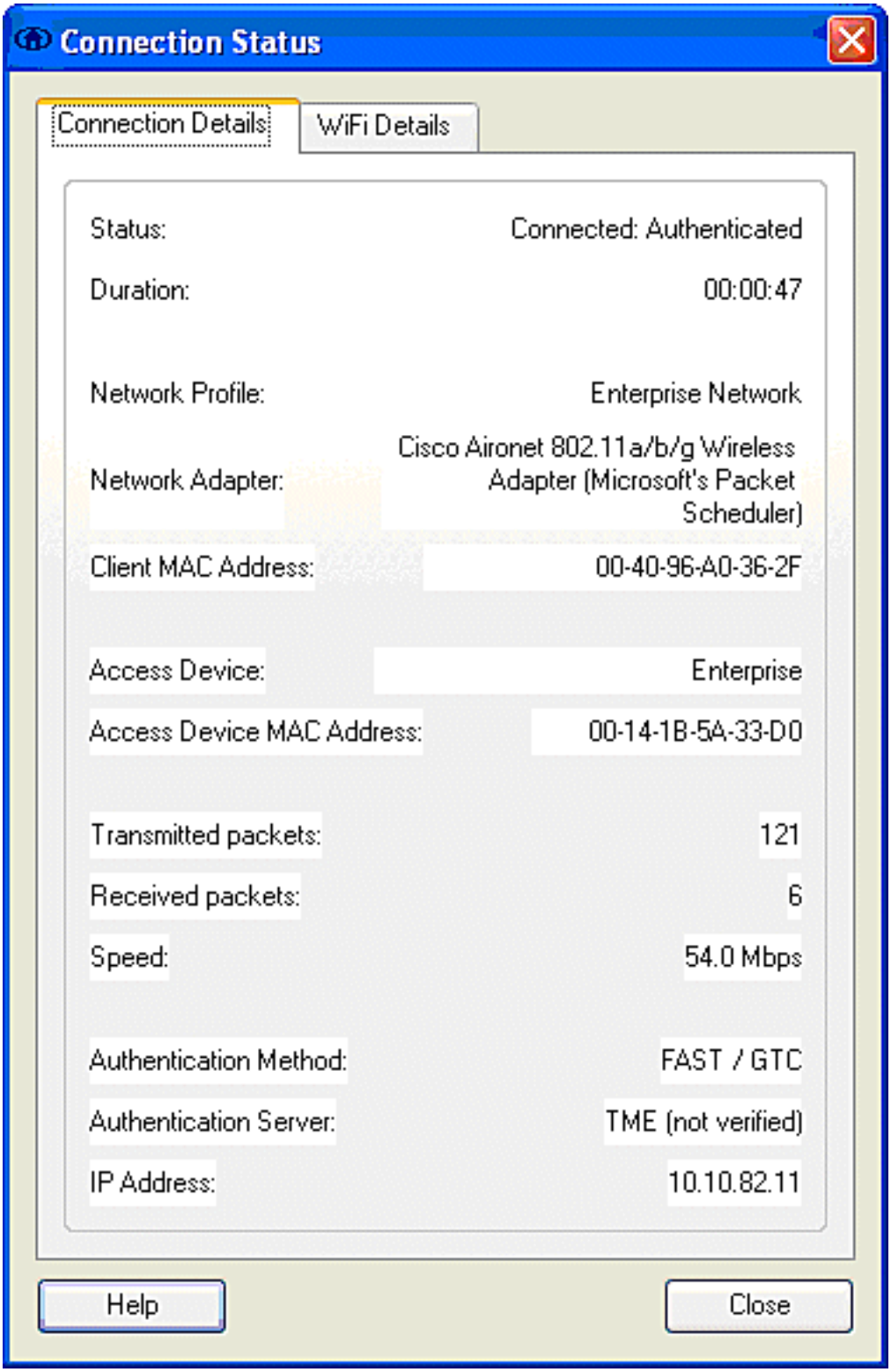
注意： 默认情况下，此窗口的 EAP-TLS 设置下“Validate Server Certificate”出于启用状态。因为本示例不使用 EAP-TLS 作为内部身份验证方法，所以此字段不适用。如果启用此字段，则除了在 EAP-TLS 中对客户端证书进行服务器验证以外，它还会允许客户端验证服务器证书。

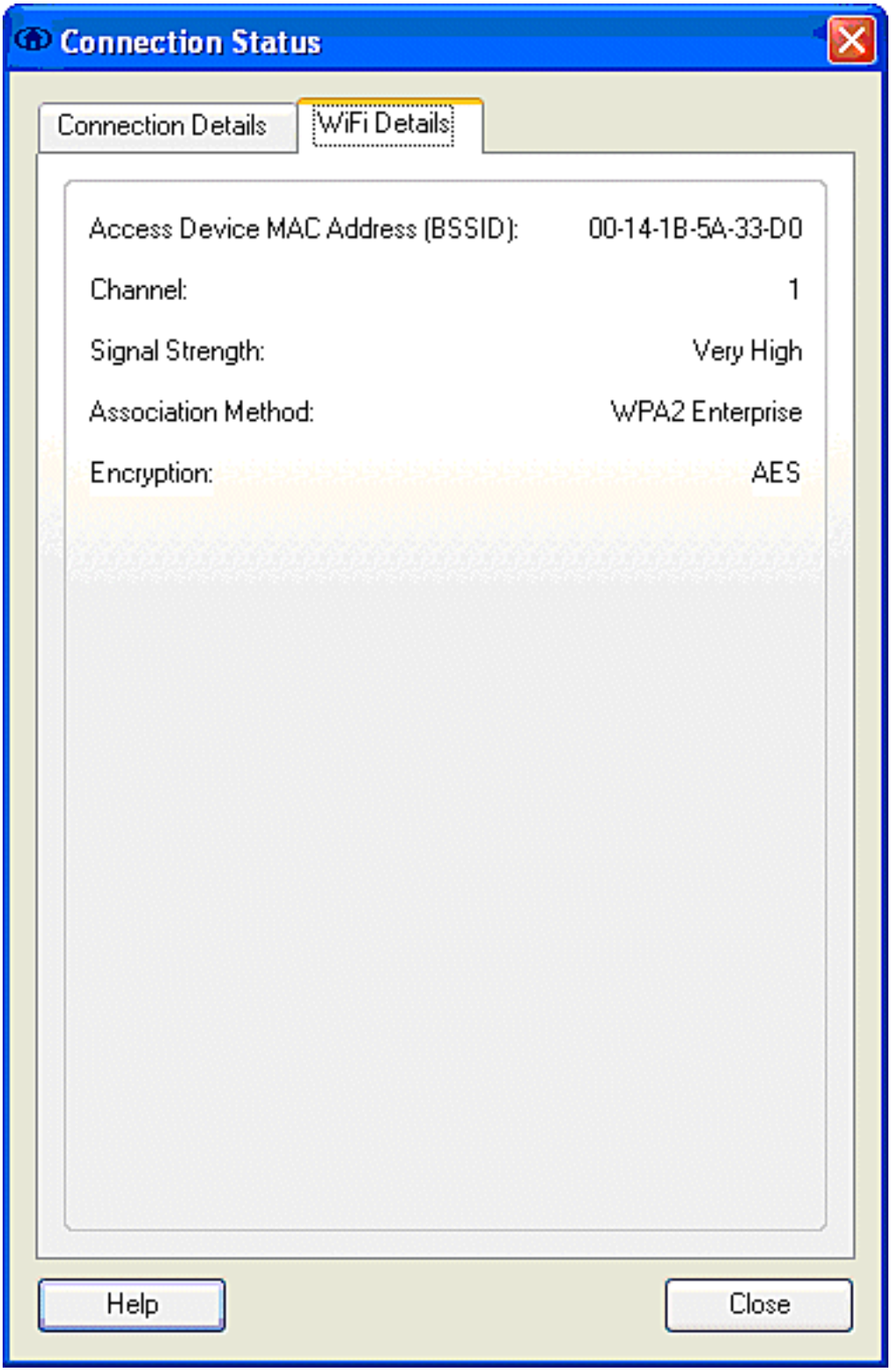


单击 OK 以保存 EAP-FAST 设置。由于客户端在配置文件中被配置为“自动建立”，因此它会自动启动与网络的关联/身份验证。在“Manage Networks”选项卡上，“Network”、“Status”和“Data Security”字段指示了客户端的连接状态。从示例中，可以看到正在使用 Profile Enterprise Network，并且 Network Access Device 是 SSID Enterprise，该设备指示 Connected:Authenticated 并使用 Autoconnect。“Data Security”字段指示使用的 802.11 加密类型。对于本示例，使用的是 WPA2。



在客户端验证之后，在“Manage Networks”选项卡中的“Profile”下选择 **SSID**，然后单击“Status”以查询有关连接的详细信息。“Connection Details”窗口提供了有关客户端设备、连接状态和统计信息以及身份验证方法的信息。“WiFi Details”选项卡提供了有关 802.11 连接状态的详细信息，包括 RSSI、802.11 通道以及身份验证/加密。


Connection Status
Connection Details
WiFi Details
Status:
Connected: Authenticated
Duration:
00:00:47
Network Profile:
Enterprise Network
Network Adapter:
Cisco Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:
00-40-96-A0-36-2F
Access Device:
Enterprise
Access Device MAC Address:
00-14-1B-5A-33-D0
Transmitted packets:
121
Received packets:
6
Speed:
54.0 Mbps
Authentication Method:
FAST / GTC
Authentication Server:
TME (not verified)
IP Address:
10.10.82.11
Help
Close



系统管理员有权使用诊断工具 Cisco 安全服务客户端系统报告，标准 CSSC 分发中就提供了此工具。此工具可以从“开始”菜单或 CSSC 目录访问。要获取数据，请单击 **Collect Data > Copy to Clipboard > Locate Report File**。这会打开 Microsoft 资源管理器窗口，并显示压缩的报告文件所在的目录。在压缩的文件中，最有用的数据位于日志 (log_current) 下。

该工具提供了 CSSC 的当前状态、接口和驱动程序详细信息，以及 WLAN 信息（检测到的 SSID、关联状态等）。这对于诊断 CSSC 与 WLAN 适配器之间的连接问题尤其有用。

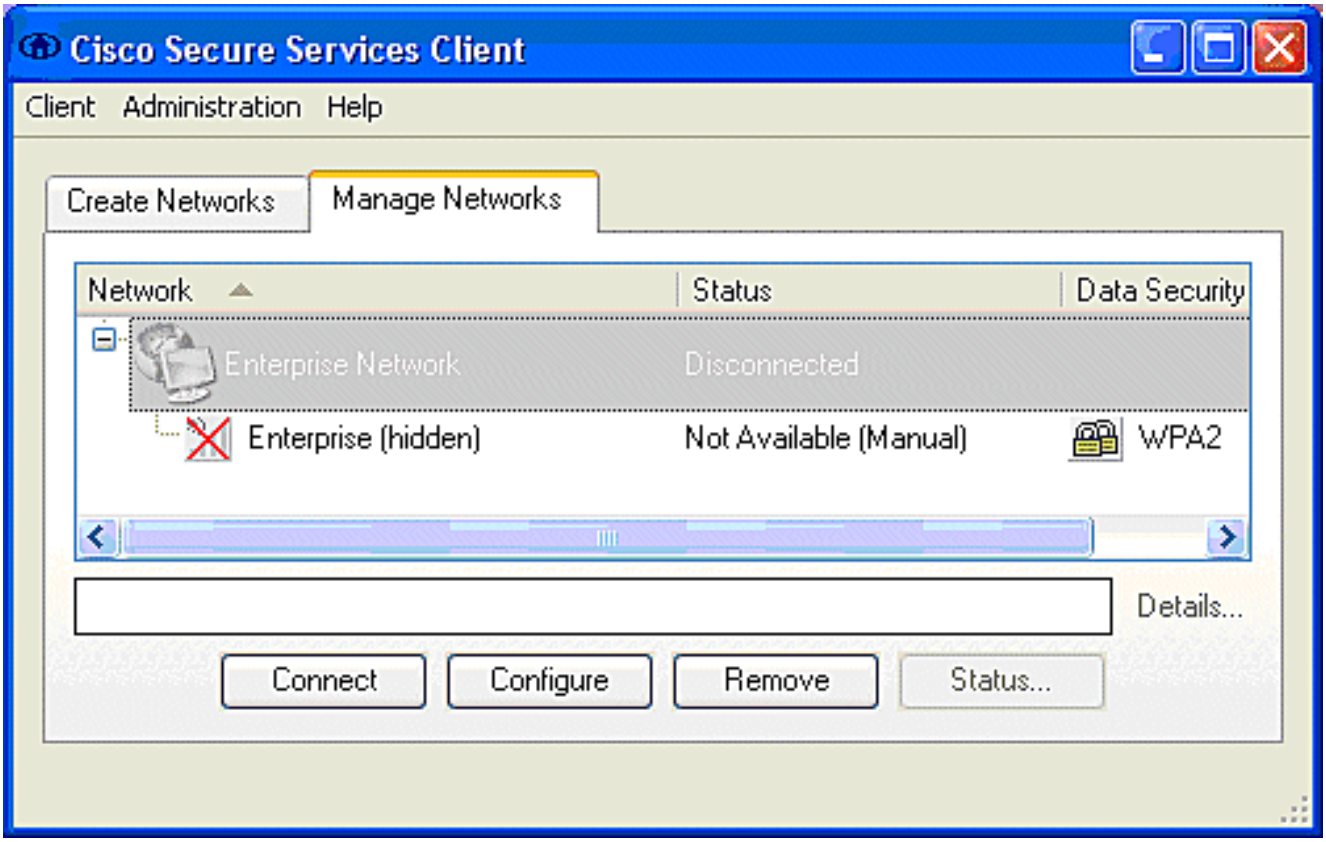
验证操作

配置 Cisco Secure ACS 服务器、WLAN 控制器、CSSC 客户端之后，如果配置和数据库数据填充

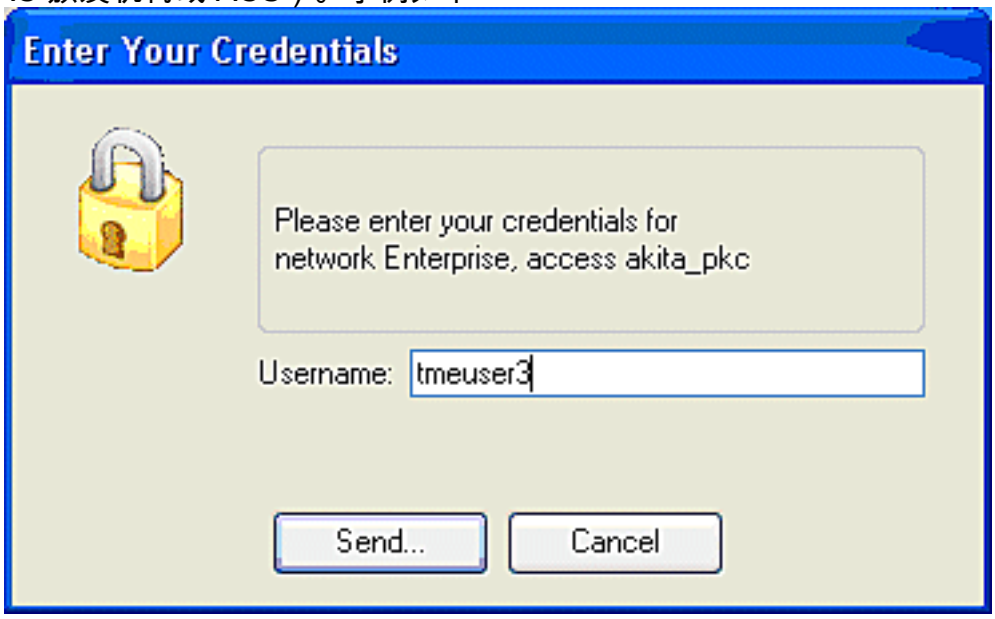
也是正确的，则 WLAN 网络即已配置好，可进行 EAP-FAST 身份验证和安全的客户端通信。可以监视许多要点，以便检查安全会话的进度/错误。

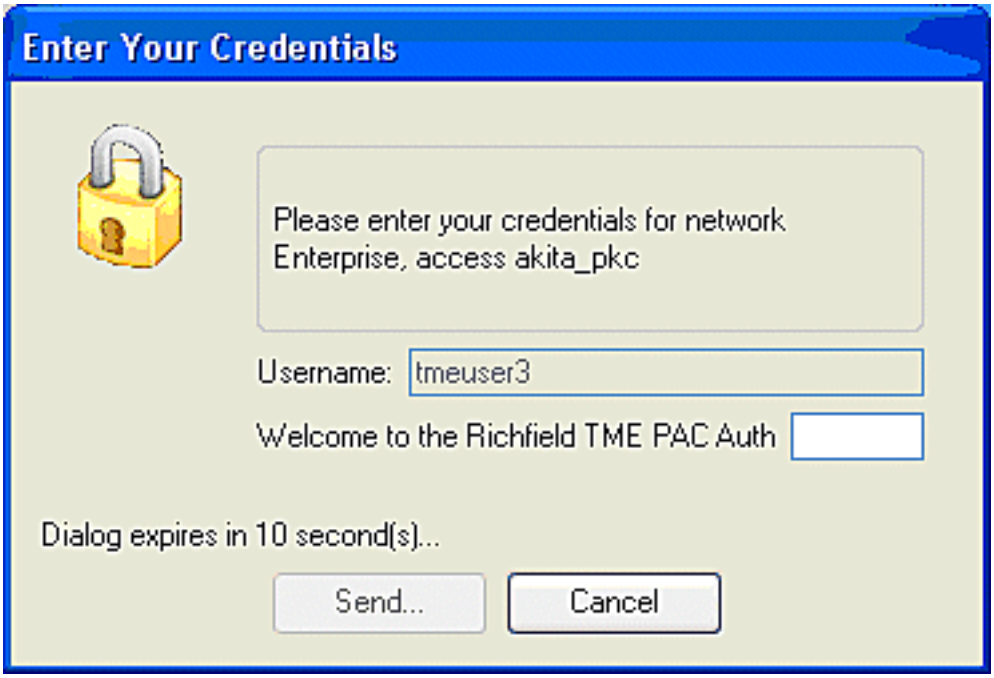
要测试该配置，请尝试将无线客户端与具有 EAP-FAST 身份验证的 WLAN 控制器相关联。

1. 如果将 CSSC 配置为自动连接，则客户端将自动尝试此连接。如果未配置自动连接和单一登录操作，则用户必须通过 **Connect** 单选按钮启动 WLAN 连接。这将启动 802.11 关联过程，并在其中执行 EAP 身份验证。示例如下：

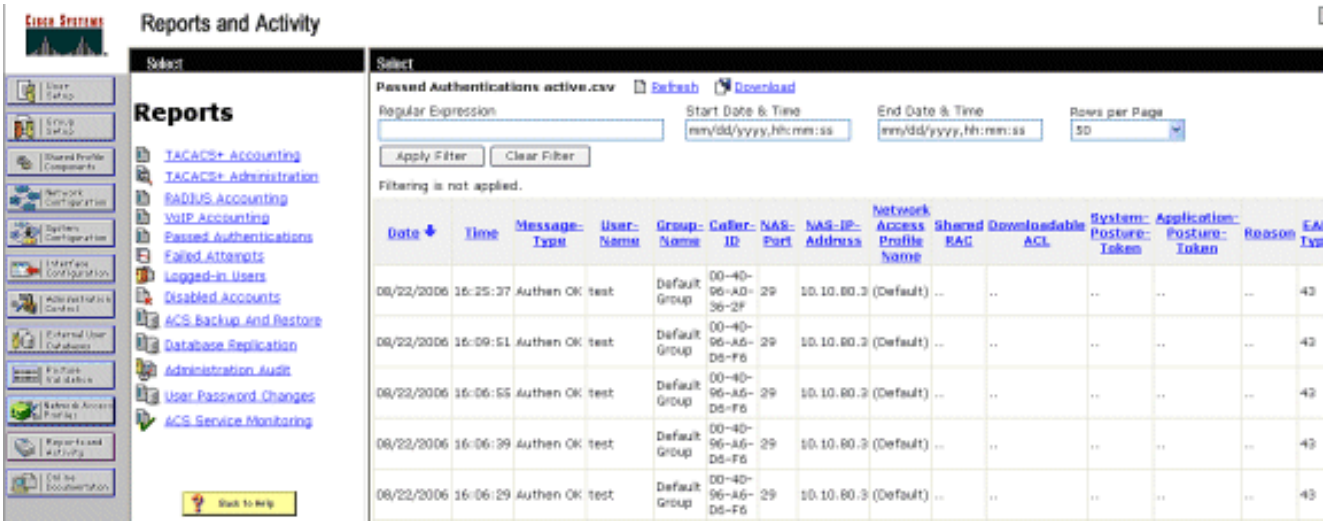


2. 随后，系统将提示用户提供用户名和密码，以便进行 EAP-FAST 身份验证（从 EAP-FAST PAC 颁发机构或 ACS）。示例如下：

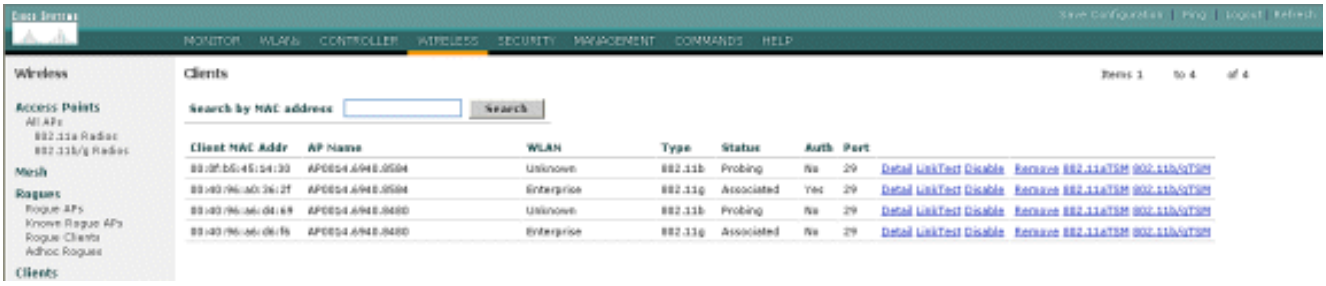




3. 然后，CSSC 客户端担当 WLC，将用户凭据传递给 RADIUS 服务器（Cisco Secure ACS），以便验证这些凭据。ACS 会将数据与已配置的数据库（在示例配置中，外部数据库是 Windows Active Directory）进行比较，以便验证用户凭据，并在用户凭据有效时，向无线客户端提供访问权限。ACS 服务器上的“Passed Authentications”报告显示了已通过 RADIUS/EAP 身份验证的客户端。示例如下：



4. 在成功的RADIUS/EAP验证，无线客户端(在本例中的00:40:96:ab:36:2f)用AP WLAN控制器验证。



附录

除了 Cisco Secure ACS 和 Cisco WLAN 控制器提供的诊断和状态信息以外，还有一些附加的要点可用于诊断 EAP-FAST 身份验证。尽管在不使用 WLAN 嗅探器或不在 WLAN 控制器上调试 EAP

交换时，大多数身份验证问题都能得到诊断，但仍然提供此参考资料来帮助解决疑难问题。

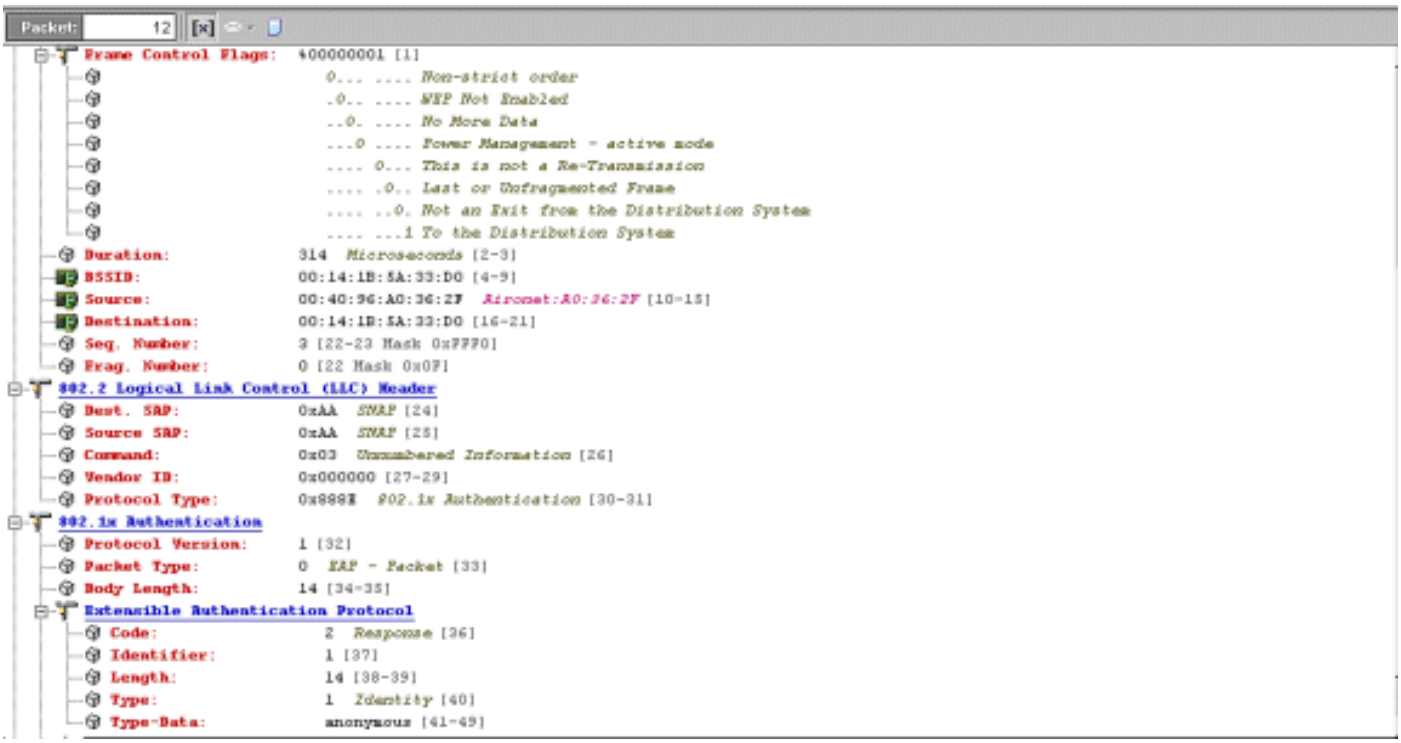
用于 EAP-FAST 交换的嗅探器捕获

此 802.11 嗅探器捕获显示了身份验证交换。

Source	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Summary
00:14:1B:5A:33:D0	*	11	68%	36.0	101	00.033877	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0	*	11	70%	24.0	101	00.036453	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0		11	71%	54.0	90	00.036494	802.1x	FC=.F......,SN=2868,FN= 0
Aironet:A0:36:2F		11	54%	1.0	82	00.123205	EAP Response	FC=T.......,SN= 3,FN= 0
00:14:1B:5A:33:D0	*	11	71%	1.0	14	00.123517	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	67%	54.0	65	00.165611	802.1x	FC=.F......,SN=2870,FN= 0
Aironet:A0:36:2F		11	55%	1.0	82	00.173920	EAP Response	FC=T.......,SN= 4,FN= 0
00:14:1B:5A:33:D0	*	11	70%	1.0	14	00.174228	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	68%	54.0	66	00.178863	802.1x	FC=.F......,SN=2871,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.200632	EAP Response	FC=T.......,SN= 5,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.203340	EAP Response	FC=T..R....,SN= 5,FN= 0
00:14:1B:5A:33:D0	*	11	71%	1.0	14	00.203639	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	70%	54.0	188	00.207634	802.1x	FC=.F......,SN=2872,FN= 0
Aironet:A0:36:2F		11	55%	1.0	105	00.216295	EAP Response	FC=T.......,SN= 6,FN= 0
Aironet:A0:36:2F		11	57%	1.0	105	00.217444	EAP Response	FC=T..R....,SN= 6,FN= 0
00:14:1B:5A:33:D0	*	11	70%	1.0	14	00.217754	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	67%	54.0	99	00.222799	802.1x	FC=.F......,SN=2874,FN= 0
Aironet:A0:36:2F		11	55%	1.0	152	00.254189	EAP Response	FC=T.......,SN= 7,FN= 0
00:14:1B:5A:33:D0	*	11	68%	1.0	14	00.254499	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	64%	54.0	147	00.288950	802.1x	FC=.F.R....,SN=2875,FN= 0
Aironet:A0:36:2F		11	55%	1.0	232	00.318087	EAP Response	FC=T.......,SN= 8,FN= 0
00:14:1B:5A:33:D0	*	11	70%	1.0	14	00.318383	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	68%	54.0	44	00.326833	802.1x	FC=.F......,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	65%	54.0	44	00.326882	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	48.0	44	00.326922	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	157	00.326964	802.1x	FC=.F......,SN=2878,FN= 0
Aironet:A0:36:2F		11	57%	1.0	157	00.333742	EAP01-Key	FC=T.......,SN= 9,FN= 0
00:14:1B:5A:33:D0	*	11	70%	1.0	14	00.334019	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	65%	54.0	207	00.340467	802.1x	FC=.F......,SN=2879,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	207	00.341130	802.1x	FC=.F.R....,SN=2879,FN= 0
Aironet:A0:36:2F		11	57%	1.0	135	00.342542	EAP01-Key	FC=T.......,SN= 10,FN= 0

此数据包显示了最初的 EAP-FAST EAP 响应。

注意： 就像 CSSC 客户端上配置的一样，在最初的 EAP 响应中，使用匿名作为外部 EAP 身份。



在 WLAN 控制器上进行调试

可以在 WLAN 控制器上使用以下 debug 命令来监视身份验证交换的进度：

- debug aaa events enable
- debug aaa detail enable
- debug dot1x events enable
- debug dot1x states enable

下面是一个示例，演示如何在 WLAN 控制器上使用 debug 命令，监视 CSSC 客户端与 ACS 之间的身份验证事务：

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing RSN IE type 48,
   length 20 for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received RSN IE with
   0 PMKIDs from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
   moving mobile 00:40:96:a0:36:2f into Connecting state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-
   Request/Identity to mobile 00:40:96:a0:36:2f (EAP Id 1)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Identity Response
   (count=1) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f EAP State update from
   Connecting to Authenticating for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x - moving mobile
   00:40:96:a0:36:2f into Authenticating state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth
   Response state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AuthenticationRequest: 0x138dd764
Thu Aug 24 18:20:54 2006:       Callback.......0x10372764
Thu Aug 24 18:20:54 2006:       protocolType...0x00040001
Thu Aug 24 18:20:54 2006:       proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006:       Packet contains 15 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Successful transmission of
   Authentication Packet (id 84) to 10.1.1.12:1812, proxy state0
Thu Aug 24 18:20:54 2006: ****Enter processIncomingMessages: response code=11
Thu Aug 24 18:20:54 2006: ****Enter processRadiusResponse: response code=11
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Access-Challenge received from
   RADIUS server 10.1.1.12 for mobile 00:40:96:a0:36:2f rec7
Thu Aug 24 18:20:54 2006: AuthorizationResponse: 0x11c8a394
Thu Aug 24 18:20:54 2006:       structureSize..147
Thu Aug 24 18:20:54 2006:       resultCode.....255
Thu Aug 24 18:20:54 2006:       protocolUsed...0x00000001
Thu Aug 24 18:20:54 2006:       proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006:       Packet contains 4 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-Challenge
   for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth Req state
   (id=249) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f WARNING:
   updated EAP-Identifer 1 ===> 249 for STA 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP Request from
   AAA to mobile 00:40:96:a0:36:2f (EAP Id 249)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAP Response from
   mobile 00:40:96:a0:36:2f (EAP Id 249, EAP Type 3)
```

下面是来自控制器 debug 命令的信息，显示 EAP 交换已成功完成（使用 WPA2 身份验证）：

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-
   Accept for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Applying new AAA
   override for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Override values for station
```

```
   00:40:96:a0:36:2f source: 4, valid bits: 0x0
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout:
   -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, r1'
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Unable to apply override
   policy for station 00:40:96:a0:36:2f - VapAllowRadiusOverride E
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Creating a new PMK Cache Entry
   for station 00:40:96:a0:36:2f (RSN 2)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Adding BSSID
   00:14:1b:5a:33:d0 to PMKID cache for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: New PMKID: (16)
Thu Aug 24 18:20:54 2006:      [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b
   72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-Success
   to mobile 00:40:96:a0:36:2f (EAP Id 0)
Thu Aug 24 18:20:54 2006: Including PMKID in M1  (16)
Thu Aug 24 18:20:54 2006:
   [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b 72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message to
   mobile 00:40:96:a0:36:2f state INITPMK (message 1), repl0
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend
   Auth Success state (id=0) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Auth Success
   while in Authenticating state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
   moving mobile 00:40:96:a0:36:2f into Authenticated state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-
   Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version
   (1) in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key
   in PKT_START state (message 2) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Stopping retransmission
   timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message
   to mobile 00:40:96:a0:36:2f state PTKINITNEGOTIATING (messa1
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received
   EAPOL-Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version (1)
   in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key in
   PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AccountingMessage
   Accounting Interim: 0x138dd764
Thu Aug 24 18:20:54 2006: Packet contains 20 AVPs:
Thu Aug 24 18:20:54 2006:
   AVP[01] User-Name.................enterprise (10 bytes)
Thu Aug 24 18:20:54 2006: AVP[02]
   Nas-Port..........................0x0000001d (29) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[03]
   Nas-Ip-Address....................0x0a0a5003 (168448003) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[04]
   Class.............................CACS:0/28b5/a0a5003/29 (22 bytes)
Thu Aug 24 18:20:54 2006: AVP[05]
   NAS-Identifier....................ws-3750 (7 bytes)
Thu Aug 24 18:20:54 2006: AVP[06]
   Airespace / WLAN-Identifier........0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[07]
   Acct-Session-Id...................44ede3b0/00:40:
   96:a0:36:2f/14 (29 bytes)
Thu Aug 24 18:20:54 2006: AVP[08]
   Acct-Authentic....................0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[09]
   Tunnel-Type.......................0x0000000d (13) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[10]
```

```
   Tunnel-Medium-Type.................0x00000006 (6) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[11]
   Tunnel-Group-Id....................0x3832 (14386) (2 bytes)
Thu Aug 24 18:20:54 2006: AVP[12]
   Acct-Status-Type...................0x00000003 (3) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[13]
   Acct-Input-Octets..................0x000b99a6 (760230) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[14]
   Acct-Output-Octets.................0x00043a27 (277031) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[15]
   Acct-Input-Packets.................0x0000444b (17483) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[16]
   Acct-Output-Packets................0x0000099b (2459) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[17]
   Acct-Session-Time..................0x00000a57 (2647) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[18]
   Acct-Delay-Time....................0x00000000 (0) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[19]
   Calling-Station-Id.................10.10.82.11 (11 bytes)
Thu Aug 24 18:20:54 2006: AVP[20]
   Called-Station-Id..................10.10.80.3 (10 bytes)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f
   Stopping retransmission timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:57 2006: User admin authenticated
```

相关信息

- Cisco Secure ACS for Windows Server 安装指南
- Cisco Secure ACS 4.1 配置指南
- 根据 WLC 和 Cisco Secure ACS 的 SSID 限制 WLAN 访问的配置示例
- ACS 4.0 和 Windows 2003 中统一无线网络下的 EAP-TLS
- 带有RADIUS服务器的动态VLAN分配和无线局域网控制器的配置示例
- 技术支持和文档 - Cisco Systems