包含 ACS 5.1 和 Windows 2003 Server 的统一无线网络中的 PEAP

目录

简介

本文档介绍如何使用无线局域网控制器、Microsoft Windows 2003 软件和 Cisco 安全访问控制服务

器 (ACS) 5.1，通过受保护的扩展身份验证协议 (PEAP) 以及 Microsoft 质询握手身份验证协议 (MS-CHAP) 版本 2 来配置安全的无线访问。

注意： 有关安全的无线部署的信息，请参阅 Microsoft Wi-Fi 网站 和 Cisco SAFE 无线蓝图。

先决条件

要求

我们假设安装者已掌握安装 Windows 2003 和 Cisco 无线局域网控制器的基本知识，因为本文档仅涵盖有助于开展测试的特定配置。

有关 Cisco 5508 系列控制器的初始安装和配置方面的信息，请参阅 Cisco 5500 系列无线控制器安装指南。有关 Cisco 2100 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 2100 系列无线局域网控制器 (WLC)。

有关 Microsoft Windows 2003 安装和配置指南，请访问安装 Windows Server 2003 R2 。

开始之前，请在测试实验室中的每台服务器上安装 Microsoft Windows Server 2003 SP1 操作系统并更新所有 Service Pack。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。

此外还会用到 Windows Server 2003 Enterprise Edition SP1，以便配置自动注册用户功能以及进行 PEAP 身份验证所需的工作站证书。证书自动注册和自动续订功能可用于续订证书以及让证书自动过期，因此可以方便证书的部署并提高安全性。

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 7.0.98.0 的 Cisco 2106 或 5508 系列控制器
- Cisco 1142 轻量接入点协议 (LWAPP) AP
- 装有 Internet Information Server (IIS)、证书颁发机构 (CA)、DHCP 和域名系统 (DNS) 的 Windows 2003 Enterprise
- Cisco 1121 安全访问控制系统设备 (ACS) 5.1
- 具有 SP（和更新的 Service Pack）以及无线网络接口卡 (NIC)（支持 CCX v3）或第三方请求方的 Windows XP Professional。
- Cisco 3750 交换机

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。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

Cisco 安全无线实验室拓扑
本文档的主要目的是提供分步过程，帮助您在装有 ACS 5.1 和 Windows 2003 Enterprise 服务器的统一无线网络下实施 PEAP。重点是自动注册客户端，使得客户端能够自动注册并从服务器获取证书。

注意： 要向 Windows XP Professional SP 中添加通过临时密钥完整性协议 (TKIP)/高级加密标准 (AES) 实现的 Wi-Fi 保护访问 (WPA)/WPA2，请参阅 Windows XP Service Pack 2 的 WPA2/无线配置服务信息元素 (WPS IE) 更新。

Windows Enterprise 2003 中关于 IIS、证书颁发机构、DNS、DHCP 的设置 (CA)

CA (democa)

CA 是一台运行 Windows Server 2003 Enterprise Edition SP2 的计算机，该计算机担当以下角色：

- **demo.local** 域的域控制器，运行 IIS
- **demo.local** DNS 域的 DNS 服务器
- DHCP 服务器
- **demo.local** 域的企业根 CA

要为这些服务配置 CA，请执行以下步骤：

1. 执行基本安装和配置。
2. 将计算机配置为域控制器。
3. 提升域功能级别。
4. 安装并配置 DHCP。
5. 安装证书服务。
6. 验证证书的管理员权限。
7. 向域中添加计算机。
8. 允许计算机进行无线访问。
9. 向域中添加用户。
10. 允许用户进行无线访问。
11. 向域中添加组。
12. 向 wirelessusers 组中添加用户。
13. 向 wirelessusers 组中添加客户端计算机。

执行基本安装和配置

请执行以下步骤：

1. 将 Windows Server 2003 Enterprise Edition SP2 安装为独立服务器。
2. 用 IP 地址 *10.0.10.10* 和子网掩码 *255.255.255.0* 配置 TCP/IP 协议。

将计算机配置为域控制器

请执行以下步骤：

1. 要启动 Active Directory 安装向导，请选择**开始 > 运行**，键入 **dcpromo.exe**，然后单击“确定”。
2. 在“欢迎使用 Active Directory 安装向导”页上，单击**下一步**。
3. 在“操作系统兼容性”页上，单击**下一步**。
4. 在“域控制器类型”页上，选择**新域的域控制器**，然后单击“下一步”。
5. 在“创建一个新域”页上，选择**在新林中新建域**，然后单击“下一步”。
6. 在“安装或配置 DNS”页上，选择**否，只在这台计算机上安装并配置 DNS**，然后单击“下一步”。
7. 在“新的域名”页上，键入 **demo.local**，然后单击**下一步**。
8. 在“NetBIOS 域名”页上，键入 NetBIOS 域名 **demo**，然后单击**下一步**。
9. 在“数据库和日志文件夹位置”页上，接受默认的数据库和日志文件夹目录，然后单击**下一步**。
10. 在“共享的系统卷”页上，验证默认文件夹位置正确，然后单击**下一步**。
11. 在“权限”页上，验证选中了**只与 Windows 2000 或 Windows Server 2003 操作系统兼容的权限**，然后单击“下一步”。
12. 在“目录服务恢复模式管理密码”页上，将密码框保留为空，然后单击**下一步**。
13. 查看“摘要”页上的信息，然后单击**下一步**。
14. 当您完成 Active Directory 的安装后，单击**完成**。
15. 当提示重新启动计算机时，单击**立即重新启动**。

提升域功能级别

请执行以下步骤：

1. 从**管理工具**文件夹打开 **Active Directory 域和信任关系**管理单元（**“开始”>“程序”>“管理工具”>“Active Directory 域和信任关系”**），然后右键单击域计算机 **CA.demo.local**。
2. 单击**提升域功能级别**，然后在“提升域功能级别”页上选择 **Windows Server 2003**。
3. 单击**提升**，单击“确定”，然后再次单击“确定”。

安装并配置 DHCP

请执行以下步骤：

1. 使用“控制面板”中的“添加或删除程序”安装**动态主机配置协议 (DHCP)** 作为网络服务组件。
2. 从**管理工具**文件夹打开 **DHCP** 管理单元（**“开始”>“程序”>“管理工具”>“DHCP”**），然后突出显示 DHCP 服务器 **CA.demo.local**。
3. 单击**操作**，然后单击“授权”以便授权 DHCP 服务。
4. 在控制台树中，右键单击 **CA.demo.local**，然后单击“新建作用域”。
5. 在“新建作用域向导”的“欢迎”页上，单击**下一步**。
6. 在“作用域名称”页上，在“名称”字段中键入 **CorpNet**。
7. 单击**下一步** 并填写以下参数：起始 IP 地址 - **10.0.20.1**结束 IP 地址 - **10.0.20.200**长度 - **24**子网掩码 - **255.255.255.0**
8. 单击**下一步**，然后输入 *10.0.20.1* 作为要排除的“起始 IP 地址”，输入 *10.0.20.100* 作为要排除的“结束 IP 地址”。然后，单击**下一步**。这将保留从 10.0.20.1 到 10.0.20.100 范围内的 IP 地址。这些保留的 IP 地址不会被 DHCP 服务器分配。
9. 在“租约期限”页上，单击**下一步**。

10. 在“配置 DHCP 选项”页上，选择**是，我想现在配置这些选项**，然后单击“下一步”。
11. 在“路由器(默认网关)”页上，添加默认路由器地址 *10.0.20.1*，然后单击**下一步**。
12. 在域名和DNS服务器页，请*在*父域字段键入*demo.local*，键入*在*IP地址字段的10.0.10.10和然后单击Addand其次单击**。**
13. 在“WINS 服务器”页上，单击**下一步**。
14. 在“激活作用域”页上，选择**是，我想现在激活此作用域**，然后单击“下一步”。
15. 当您完成“新建作用域向导”页时，单击**完成**。

安装证书服务

请执行以下步骤：

注意： 必须在安装证书服务之前安装 IIS，并且用户应该是 Enterprise Admin OU 的一部分。

1. 在“控制面板”中，打开**添加或删除程序**，然后单击“添加/删除 Windows 组件”。
2. 在“Windows 组件向导”页上，选择**证书服务**，然后单击“下一步”。
3. 在“CA 类型”页上，选择**企业根 CA**，然后单击“下一步”。
4. 在“CA 识别信息”页的“此 CA 的公用名称”框中键入 *democa*。您也可以输入其他可选的详细信息。然后单击**下一步**，并接受“证书数据库设置”页上的默认值。
5. 单击 **Next**。在安装完成时，单击**完成**。
6. 在您读完有关安装 IIS 的警告消息后，单击**确定**。

验证证书的管理员权限

请执行以下步骤：

1. 选择**开始 > 管理工具 > 证书颁发机构**。
2. 右键单击 **democa CA**，然后单击**属性**。
3. 在“安全性”选项卡上，单击“组或用户名称”列表中的**管理员**。
4. 在“管理员的权限”列表中，确保以下选项均设置为**允许**：颁发和管理证书管理 CA请求证书如果其中任意一项设置为“拒绝”或未选中，请将其权限设置为**允许**。
5. 单击**确定**关闭“democa CA 属性”对话框，然后关闭“证书颁发机构”。

向域中添加计算机

请执行以下步骤：

注意： 如果计算机已添加到域中，请继续执行向域中添加用户。

1. 打开 **Active Directory 用户和计算机**管理单元。
2. 在控制台树中，展开 **demo.local**。
3. 右键单击**计算机**，单击**新建**，然后单击**计算机**。
4. 在“新建对象 – 计算机”对话框中，在“计算机名称”字段中键入计算机的名称，然后单击**下一步**。本示例使用计算机名称 *Client*。
5. 在“托管”对话框中，单击**下一步**。
6. 在“新建对象 – 计算机”对话框中，单击**完成**。
7. 重复步骤 3 到步骤 6，创建更多计算机帐户。

允许计算机进行无线访问

请执行以下步骤：

1. 在“Active Directory 用户和计算机”控制台树中，单击**计算机**文件夹，然后右键单击要分配无线访问权限的计算机。本示例显示的操作步骤针对您在步骤 7 中添加的计算机 **Client**。请单击**属性**，然后转至**拨号**选项卡。
2. 在“远程访问权限”中选择**允许访问**，然后单击**确定**。

向域中添加用户

请执行以下步骤：

1. 在“Active Directory 用户和计算机”控制台树中，右键单击**用户**，单击“新建”，然后单击“用户”。
2. 在“新建对象 - 用户”对话框中，键入无线用户的名称。本示例在“名字”字段中使用名称 *wirelessuser*，在“用户登录名”字段中使用 *wirelessuser*。单击 **Next**。
3. 在“新建对象 – 用户”对话框中，在“密码”和“确认密码”字段中键入您选择的密码。清除**用户必须在下次登录时更改密码**复选框，然后单击“下一步”。
4. 在“新建对象 – 用户”对话框中，单击**完成**。
5. 重复步骤 2 到步骤 4，以便创建更多用户帐户。

允许用户进行无线访问

请执行以下步骤：

1. 在“Active Directory 用户和计算机”控制台树中，单击**用户**文件夹，右键单击 **wirelessuser**，单击**属性**，然后转至**拨号**选项卡。
2. 在“远程访问权限”中选择**允许访问**，然后单击**确定**。

向域中添加组

请执行以下步骤：

1. 在 Active Directory 用户和计算机控制台树中，右键单击“用户”，单击“新建”，然后单击“组”。
2. 在“新建对象 – 组”对话框中，在“组名”字段中键入组的名称，然后单击**确定**。本文档使用组名 *wirelessusers*。

向 wirelessusers 组中添加用户

请执行以下步骤：

1. 在“Active Directory 用户和计算机”的详细信息窗格中，双击组 *WirelessUsers*。
2. 转至“成员”选项卡，然后单击**添加**。
3. 在“选择用户、联系人、计算机或组”对话框中，键入要添加到组中的用户的名称。本示例显示如何将用户 *wirelessuser* 添加到组中。单击 **Ok**。
4. 在“发现多个名称”对话框中，单击**确定**。此时会将 wirelessuser 用户帐户添加到 wirelessusers 组中。

5. 单击**确定**，以便保存对 wirelessusers 组的更改。
6. 重复此过程，向该组中添加更多用户。

向 wirelessusers 组中添加客户端计算机

请执行以下步骤：

1. 重复本文档向 wirelessusers 组中添加用户部分中的步骤 1 和步骤 2。
2. 在“选择用户、联系人或计算机”对话框中，键入要添加到组中的计算机的名称。本示例显示如何将名为 *client* 的计算机添加到组中。
3. 单击**对象类型**，清除“用户”复选框，然后选中“计算机”。
4. 单击**确定**两次。此时会将 CLIENT 计算机帐户添加到 wirelessusers 组中。
5. 重复此过程，向该组中添加更多计算机。

Cisco 1121 安全 ACS 5.1

使用 CSACS-1121 系列设备进行安装

CSACS-1121 设备已预先安装了 ACS 5.1 软件。本部分概述安装过程及在安装 ACS 之前必须执行的任务。

1. 将 CSACS-1121 连接到网络和设备控制台。请参阅第 4 章“连接电缆”。
2. 启动 CSACS-1121 设备。请参阅第 4 章“启动 CSACS-1121 系列设备”。
3. 在 CLI 提示符下运行 **setup** 命令，以配置 ACS 服务器的初始设置。请参阅“运行安装程序”。

安装 ACS 服务器

本部分描述在 CSACS-1121 系列设备上安装 ACS 服务器的过程。

- 运行安装程序
- 验证安装过程
- 安装后任务

有关安装 Cisco Secure ACS 服务器的详细信息，请参阅 Cisco 安全访问控制系统 5.1 安装和升级指南。

Cisco WLC5508 控制器配置

为 WPAv2/WPA 创建必要的配置

请执行以下步骤：

注意： 假设控制器与网络之间具有基本的连接，并且能够成功通过 IP 访问管理接口。

1. 浏览到 **https://10.0.1.10**，以便登录控制器。
2. 单击 **Login**。
3. 用默认用户 *admin* 和默认密码 *admin* 进行登录。
4. 在 **Controller** 菜单下为 VLAN 映射创建新接口。

5. 单击 **Interfaces**。
6. 单击 **New**。
7. 在 Interface name 字段中输入 *Employee*。（此字段可以是您喜欢的任何值。）
8. 在 VLAN ID 字段中输入 *20*。（此字段可以是网络中支持的任何 VLAN。）
9. 单击 **Apply**。
10. 在显示此 Interfaces > Edit 窗口时，配置相关信息：接口 IP 地址 - **10.0.20.2**网络掩码 - **255.255.255.0**网关 - **10.0.10.1**主 DHCP - **10.0.10.10**
11. 单击 **Apply**。
12. 单击 **WLANs** 选项卡。
13. 选择 **Create New**，然后单击 **Go**。
14. 输入配置文件名称，然后在 WLAN SSID 字段中输入 *Employee*。
15. 为 WLAN 选择 ID，然后单击 **Apply**。
16. 在显示 WLANs > Edit 窗口时，为此 WLAN 配置信息。**注意：** WPAv2 是为此实验室选择的第 2 层加密方法。要允许具有 TKIP-MIC 的 WPA 客户端关联到此 SSID，您还可以选中 **WPA compatibility mode** 和“Allow WPA2 TKIP Clients”复选框，或者不支持 802.11i AES 加密方法的那些客户端。
17. 在“WLANs > Edit”屏幕上，单击 **General** 选项卡。
18. 确保选中 **Enabled** 状态框，并且选择了适当的 **Interface** (employee)。并且，确保选中“Broadcast SSID”的**“Enabled”复选框**。
19. 单击 **Security** 选项卡。
20. 在“Layer 2”子菜单下，针对“Layer 2 Security”选中 **WPA + WPA2** 。对于“WPA2 encryption”，请选中 **AES + TKIP**，以便启用 TKIP 客户端。
21. 选择 **802.1x** 作为身份验证方法。
22. 跳过“Layer 3”子菜单，因为不需要。配置 RADIUS 服务器之后，可以从“Authentication”菜单中选择适当的服务器。
23. 除非需要特殊的配置，否则可以使 **QoS** 和 **Advanced** 选项卡保留默认设置。
24. 单击 **Security** 菜单，以便添加 RADIUS 服务器。
25. 在“RADIUS”子菜单下，单击 **Authentication**。然后单击 **New**。
26. 添加 RADIUS 服务器 IP 地址 (10.0.10.20)，该服务器是前面配置的 ACS 服务器。
27. 确保共享密钥与 ACS 服务器中配置的 AAA 客户端相匹配。确保选中 **Network User** 复选框，然后单击 **Apply**。
28. 基本配置到此已经全部完成，您可以开始测试 PEAP。

PEAP 身份验证

具有 MS-CHAP 2 的 PEAP 要求在 ACS 服务器上有证书，而不要求无线客户端上有证书。可以为 ACS 服务器自动注册计算机证书，从而简化部署过程。

要配置 CA 服务器以便自动注册计算机和用户证书，请完成本部分中的步骤。

注意： Microsoft 已在 Windows 2003 企业 CA 发行版中更改了 Web 服务器模板，因此将无法再导出密钥，该选项将变灰。证书服务没有为服务器身份验证提供其他证书模板，但是可以在下拉菜单中将密钥标记为可导出，从而使您能够为服务器身份验证创建新模板。

注意： Windows 2000 允许使用可导出的密钥，因此如果您使用的是 Windows 2000，则不需要执行以下步骤。

安装证书模板管理单元

请执行以下步骤：

1. 选择**“开始”>“运行”**，输入 *mmc*，然后单击**确定**。
2. 在“文件”菜单上，单击**添加/删除管理单元**，然后单击**添加**。
3. 在“管理单元”下，双击**证书模板**，单击“关闭”，然后单击“确定”。
4. 在控制台树中，单击**证书模板**。所有证书模板都将显示在“详细信息”窗格中。
5. 要跳过步骤 2 到步骤 4，请输入 *certtmpl.msc*，以打开“证书模板”管理单元。

为 ACS Web Server 创建证书模板

请执行以下步骤：

1. 在“证书模板”管理单元的“详细信息”窗格中，单击 **Web Server** 模板。
2. 在“操作”菜单上，单击**复制模板**。
3. 在“模板显示名称”字段中输入 *ACS*。
4. 转到“请求处理”选项卡，并选中**允许导出私钥**。并且，确保从“用途”下拉菜单中选择了**签名和加密**。
5. 选择**请求必须使用以下的一个 CSP** 并选中“Microsoft Base Cryptographic Provider v1.0”。取消选中其他已选中的 CSP，然后单击**确定**。
6. 转至**使用者名称**选项卡，选择**在请求中提供**，然后单击**确定**。
7. 转至**安全性**选项卡，突出显示**域管理员组**，并确保在“允许”下选中**注册**选项。**注意：** 如果您选择从此 Active Directory 信息开始构建，只需选中**用户主体名称 (UPN)**，并且取消选中“在主题名称中包含电子邮件名称”和“电子邮件名称”，因为在“Active Directory 用户和计算机”管理单元中没有为无线用户输入电子邮件名称。如果您不禁用这两个选项，自动注册功能将尝试使用电子邮件，这会导致自动注册错误。
8. 如果需要，还有一些附加的安全措施，可防止证书被自动推出。这些措施可以在“颁发要求”选项卡下找到。此内容在本文档中不做进一步讨论。
9. 单击**确定**以保存模板，然后从“证书颁发机构”管理单元发布此模板。

启用新的 ACS Web Server 证书模板

请执行以下步骤：

1. 打开“证书颁发机构”管理单元。执行为 ACS Web Server 创建证书模板部分中的步骤 1 到步骤 3，选择**证书颁发机构**选项，选择**本地计算机**，然后单击**完成**。
2. 在“证书颁发机构”控制台树中，展开 **ca.demo.local**，然后右键单击**证书模板**。
3. 转至**新建 > 要颁发的证书模板**。
4. 单击 **ACS** 证书模板。
5. 单击**确定**，然后打开“Active Directory 用户和计算机”管理单元。
6. 在控制台树中，双击 **Active Directory 用户和计算机**，右键单击 **demo.local**，然后单击**属性**。
7. 在“组策略”选项卡上，单击**默认域策略**，然后单击“编辑”。这将打开“组策略对象编辑器”管理单元。
8. 在控制台树中，展开**计算机配置 > Windows 设置 > 安全设置 > 公钥策略**，然后选择**自动证书申请设置**。
9. 右键单击**自动证书申请设置**，然后选择**新建 > 自动证书申请**。
10. 在“欢迎使用自动证书申请设置向导”页上，单击**下一步**。
11. 在“证书模板”页上，单击**计算机**，然后单击**下一步**。
12. 当您完成“自动证书申请设置向导”页时，单击**完成**。“计算机”证书类型现在就会显示在“组策略

对象编辑器”管理单元的详细信息窗格中。
13. 在控制台树中，展开**用户配置 > Windows 设置 > 安全设置 > 公钥策略**。
14. 在详细信息窗格中，双击**自动注册设置**。
15. 选择**自动注册证书**，然后选中“续订过期证书、更新未决证书并删除吊销的证书”和“更新使用证书模板的证书”。
16. 单击 **Ok**。

ACS 5.1 证书设置

为 ACS 配置可导出的证书

注意： ACS 服务器必须从企业根 CA 服务器获取服务器证书，才能对 WLAN PEAP 客户端进行身份验证。

注意： 请勿在证书设置过程中打开 IIS 管理器，因为缓存的信息会导致问题。

1. 使用管理员帐户权限登录到 ACS 服务器。
2. 转至 **System Administration > Configuration > Local Server Certificates**。单击 **Add**。
3. 选择服务器证书创建方法时，请选择 **Generate Certificate Signing Request**。单击 **Next**。
4. 输入证书使用者和密钥长度作为示例，然后单击 **Finish**：证书使用者 (Certificate Subject) - **CN=acs.demo.local**密钥长度 (Key Length) - **1024**
5. 生成证书签名申请后，ACS 将进行提示。单击 **Ok**。
6. 在 System Administration 下，转至 **Configuration > Local Server Certificates > Outstanding Signing Requests**。**注意：** 之所以采用这一步骤，是因为 Windows 2003 不允许使用可导出的密钥；若要使用可导出的密钥，就必须根据此前创建的 ACS 证书来生成证书申请。
7. 选择 **Certificate Signing Request** 条目，然后单击 **Export**。
8. 将 ACS 证书 **.pem** 文件保存到桌面。

在 ACS 5.1 软件中安装证书

请执行以下步骤：

1. 打开浏览器并连接到 CA 服务器 URL **http://10.0.10.10/certsrv**。
2. 此时将显示“Microsoft 证书服务”窗口。选择 **Request a certificate**。
3. 单击以提交**高级证书申请**。
4. 在“高级申请”中，单击**使用 Base 64 编码的...提交证书申请**。
5. 如果浏览器安全许可，请在“保存的申请”字段中浏览到上一个 ACS 证书申请文件并插入该文件。
6. 浏览器的安全设置可能不允许访问磁盘上的文件。如果出现这种情况，请单击**确定**进行手动粘贴。
7. 找到之前从 ACS 导出的 ACS *.pem 文件。使用文本编辑器（如 Notepad）打开该文件。
8. 突出显示文件的整个内容，然后单击**复制**。
9. 返回到 Microsoft 证书申请窗口。将复制的内容**粘贴**到“保存的申请”字段。
10. 选择 **ACS** 作为“证书模板”，然后单击**提交**。
11. 发布证书后，请选择 **Base 64 编码**，然后单击**下载证书**。
12. 单击**保存**，将证书保存到桌面。
13. 转至 **ACS** > System **Administration > Configuration > Local Server Certificates**。选择 **Bind**

CA Signed Certificate，然后单击 Next。
14. 单击 Browse 并找到保存的证书。
15. 选择由 CA 服务器发布的 ACS 证书，然后单击 Open。
16. 同时，选中 Protocol 下的 EAP 复选框，然后单击 Finish。
17. CA 发布的 ACS 证书将在 ACS 本地证书中出现。

为 Active Directory 配置 ACS 标识存储

请执行以下步骤：

1. 使用管理员帐户连接到 ACS 并登录。
2. 转至 Users and Identity Stores > External Identity Stores > Active Directory。
3. 输入活动目录域*demo.local，输入*服务器的密码，并且点击TestConnection。**点击**OKIN命令继续。
4. 点击**Save Changes**。**注意：** 关于ACS 5.x集成步骤的更多信息参考ACS 5.x和以后：与Microsoft Active Directory配置示例的集成。

将控制器作为 AAA 客户端添加到 ACS

请执行以下步骤：

1. 连接到 ACS，然后转至 Network Resources > Network Devices and AAA Clients。单击**创建**。
2. 在以下字段中输入相关内容：名称 (Name) - **wlc**IP - **10.0.1.10**RADIUS 复选框 - **选中**共享密钥 (Shared Secret) - **cisco**
3. 完成后，单击 Submit。此时控制器将显示为 ACS Network Devices 列表中的条目。

配置无线 ACS 访问策略

请执行以下步骤：

1. 在 ACS 中，转至 Access Policies > Access Services。
2. 在 Access Services 窗口中，单击 Create。
3. 创建访问服务并输入名称（如 WirelessAD）。选择 Based on service template，然后单击 Select。
4. 在 Webpage 对话框中，选择 Network Access – Simple。单击 Ok。
5. 在 Webpage 对话框中，选择 Network Access – Simple。单击 Ok。选择模板后，单击 Next。
6. 在 Allowed Protocols 下，选中 Allow MS-CHAPv2 和 Allow PEAP 复选框。单击 **完成**。
7. ACS 提示您激活新服务时，请单击 Yes。
8. 在刚刚创建/激活的新访问服务中，展开并选择 Identity。对于 Identity Source，请单击 Select。
9. 为在 ACS 中配置的 Active Directory 选择 AD1，然后单击 OK。
10. 确认 Identity Source 为 AD1，然后单击 Save Changes。

创建 ACS 访问策略和服务规则

请执行以下步骤：

1. 转至 **Access Policies > Service Selection Rules**。
2. 在 Service Selection Policy 窗口中单击 **Create**。输入新规则名称（如 *WirelessRule*）。选中 **Protocol** 复选框以匹配 **Radius**。
3. 选择 **Radius**，然后单击 **OK**。
4. 在 Results 下，针对 Service 选择 **WirelessAD**（已在上一步创建）。
5. 创建新的无线规则后，请选择此规则并将其**移动**到顶部，该规则将成为第一个使用 Active Directory 来确定无线 RADIUS 身份验证的规则。

使用 Windows Zero Touch 的 PEAP 的客户端配置

在我们的示例中，CLIENT 是一台运行 Windows XP Professional SP 的计算机，该计算机担当无线客户端，并通过无线 AP 获取对 Intranet 资源的访问权限。要将 CLIENT 配置为无线客户端，请完成本部分中的步骤。

执行基本安装和配置

请执行以下步骤：

1. 使用与集线器相连的以太网电缆，将 CLIENT 连接到 Intranet 网络段。
2. 在 CLIENT 上，安装 Windows XP Professional SP2，使其成为 demo.local 域中名为 CLIENT 的成员计算机。
3. 安装 Windows XP Professional SP2。必须安装此操作系统才能获得 PEAP 支持。**注意**：Windows 防火墙在 Windows XP Professional SP2 中会自动打开。请勿关闭防火墙。

安装无线网络适配器

请执行以下步骤：

1. 关闭 CLIENT 计算机。
2. 从 Intranet 网络段断开 CLIENT 计算机的连接。
3. 重新启动 CLIENT 计算机，然后使用本地管理员帐户进行登录。
4. 安装无线网络适配器。**注意：** 请勿安装制造商为无线适配器提供的配置软件。使用“添加硬件向导”安装无线网络适配器的驱动程序。并且在出现提示时，提供由制造商提供的 CD 或包含用于 Windows XP Professional SP2 的更新驱动程序的磁盘。

配置无线网络连接

请执行以下步骤：

1. 注销，然后使用 **demo.local domain** 中的 **WirelessUser** 帐户登录。
2. 选择**开始 > 控制面板**，双击“网络连接”，然后右键单击“无线网络连接”。
3. 单击**属性**，转至**无线网络**选项卡，确保选中了**用 Windows 来配置我的无线网络设置**。
4. 单击 **Add**。
5. 在“关联”选项卡的“网络名称 (SSID)”字段中输入 *Employee*。
6. 针对“网络身份验证”选择 **WPA**，并确保将“数据加密”设置为 **TKIP**。
7. 单击 **Authentication** 选项卡。
8. 验证“EAP 类型”配置为使用**受保护的 EAP (PEAP)**。如果不是，请从下拉菜单中选择此选项。

9. 如果您希望计算机在登录之前进行身份验证（从而应用登录脚本或组策略推送），请选中**当计算机信息可用时身份验证为计算机**。
10. 单击 **Properties**。
11. 由于 PEAP 涉及由客户端对服务器进行身份验证，请确保选中**验证服务器证书**。并且，确保在*受信任的根证书颁发机构*菜单下选中“颁发 ACS 证书的 CA”。
12. 在“身份验证方法”下选择**安全密码 (EAP-MSCHAP v2)**，因为它用于内部身份验证。
13. 确保选中“启用快速重新连接”复选框。然后，单击三次**确定**。
14. 右键单击系统任务栏中的无线网络连接图标，然后单击**查看可用的无线网络**。
15. 单击 Employee 无线网络，然后单击**连接**。如果连接成功，无线客户端将显示**已连接**。
16. 身份验证成功后，使用“网络连接”来检查无线适配器的 TCP/IP 配置。它的地址范围 10.0.20.100-10.0.20.200 应该来自 DHCP 范围或为 CorpNet 无线客户端创建的范围。
17. 要测试功能，请打开浏览器并浏览到 **http://10.0.10.10**（或 CA 服务器的 IP 地址）。

使用 ACS 排除无线身份验证故障

请执行以下步骤：

1. 转至 **ACS > Monitoring and Reports**，然后单击 **Launch Monitoring & Report Viewer**。
2. 此时将打开一个单独的 ACS 窗口。单击 **Dashboard**。
3. 在 My Favorite Reports 部分，单击 **Authentications – RADIUS – Today**。
4. 此时将显示一个日志，其中包括所有通过 (Pass) 或失败 (Fail) 的 RADIUS 身份验证。在已记录的条目中，单击 Details 列中的**放大镜图标**。
5. RADIUS 身份验证详细信息将提供已记录尝试的更多信息。
6. ACS Service Hit Count 可以对符合 ACS 中的已创建规则的尝试进行概述。转至 **ACS** > Access **Policies** > Access **Services**，然后单击 **Service Selection Rules**。

使用 ACS Server 进行 PEAP 身份验证失败

当您的客户端未能通过 ACS 服务器的 PEAP 身份验证时，请检查您是否能在 ACS 的 **Report and Activity** 菜单下的 **Failed attempts option** 中找到 NAS duplicated authentication attempt 错误消息。

如果在客户端计算机上安装了 Microsoft Windows XP SP2，并且 Windows XP SP2 针对第三方服务器而不是 Microsoft IAS 进行身份验证，就会收到此错误消息。特别是，Cisco RADIUS 服务器 (ACS) 使用不同的方法来计算“可扩展身份验证协议类型:长度：值”格式 (EAP-TLV) ID，而不是 Windows XP 所使用的方法。Microsoft 认为此问题是 XP SP2 请求方中的缺陷。

有关修补程序，请与 Microsoft 联系，并请参阅文章连接第三方 RADIUS 服务器时 PEAP 身份验证不成功 。 问题的根源在客户端上：默认情况下，*Windows 实用程序* 中为 PEAP 禁用了**快速重新连接**选项。而在服务器端 (ACS)，此选项在默认情况下是启用的。要解决此问题，请取消选中 ACS 服务器上的 Fast Reconnect 选项（位于 Global System Options 下）。此外，您也可以在客户端上启用“快速重新连接”选项，以便解决此问题。

要在运行 Windows XP 的客户端上使用 Windows 实用程序启用“快速重新连接”，请执行以下步骤：

1. 转至**“开始”>“设置”>“控制面板”**。
2. 双击**网络连接**图标。
3. 右键单击**无线网络连接**图标，然后单击**属性**。
4. 单击 **Wireless Networks** 选项卡。
5. 选中**用 Windows 来配置我的无线网络设置**选项，以便通过 Windows 配置客户端适配器。

6. 如果您已经配置了 SSID，请选择该 SSID 并单击**属性**。否则，请单击**新建**以添加新的 WLAN。
7. 在**关联**选项卡下输入 SSID。确保网络身份验证设置为**开**，并且“数据加密”设置为“WEP”。
8. 单击**身份验证**。
9. 选中**为此网络启用 IEEE 802.1X 身份验证**选项。
10. 选择 **PEAP** 作为“EAP 类型”，然后单击**属性**。
11. 选中页面底部的**启用快速重新连接**选项。

相关信息

- ACS 4.0 和 Windows 2003 中统一无线网络下的 PEAP
- 用于 Web 身份验证的 Cisco 无线 LAN 控制器 (WLC) 和 Cisco ACS 5.x (TACACS+) 配置示例
- Cisco 安全访问控制系统 5.1 安装和升级指南
- 技术支持和文档 - Cisco Systems