

美洲台：在Clean Access Manager (CAM)上配置SSL上的LDAP

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[配置在SSL的LDAP的步骤在CAM](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文描述如何配置在SSL的轻量级目录访问协议(LDAP)在Clean Access管理器(CAM)。

先决条件

要求

此配置是可适用的对CAM版本3.5和以上。

使用的组件

本文档中的信息根据Clean Access管理器版本4.1。

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。

配置在SSL的LDAP的步骤在CAM

完成这些步骤：

1. 获取发出证书到域控制器不信任CA的根证明并且放置它在您的桌面。选择**管理员 > CAM > SSL证书**，然后浏览并且上传根CA证书作为**托拉斯非标准CA**。

The screenshot shows the 'Administration > Clean Access Manager' interface. A navigation bar at the top includes 'Network & Failover', 'System Time', 'SSL Certificate', 'System Upgrade', 'Licensing', and 'Support Logs'. Below this, a dropdown menu is set to 'Import Certificate'. The 'Certificate File' field contains 'C:\Documents and Settings\Adminir' with a 'Browse...' button. The 'File Type' dropdown is set to '^Trust Non-Standard CA' with an 'Upload' button. An 'Uploaded Certificate List' table shows three entries: 'Private Key' with a 'View' button; 'CA-Signed Certificate' with 'View' and 'Details' buttons; and 'Root/Intermediate CA' with 'View', 'Details', and 'Delete' buttons. A 'Verify and Install Uploaded Certificates' button is at the bottom. A footnote states: '(+ "Trust Non-Standard CA" is for SSL communication between the Clean Access Manager and some authentication servers, e.g. LDAP Server.)'

单击**验证**并且安装根CA证书。

2. 配置在CAM的LDAP服务器。选择**用户管理 > 认证服务器**并且选择**新**。选择**LDAP**作为认证类型。选择**ldaps://ip.address:636**作为服务器URL。选择**SSL**作为安全类型。选择**把柄(请跟随)!**作为推举。此选项为分区域环境，例如，根和子域设置。Admin权限用户和密码要求顺利地绑定CAM (ldap客户端)到LDAP服务器。

User Management > Auth Servers

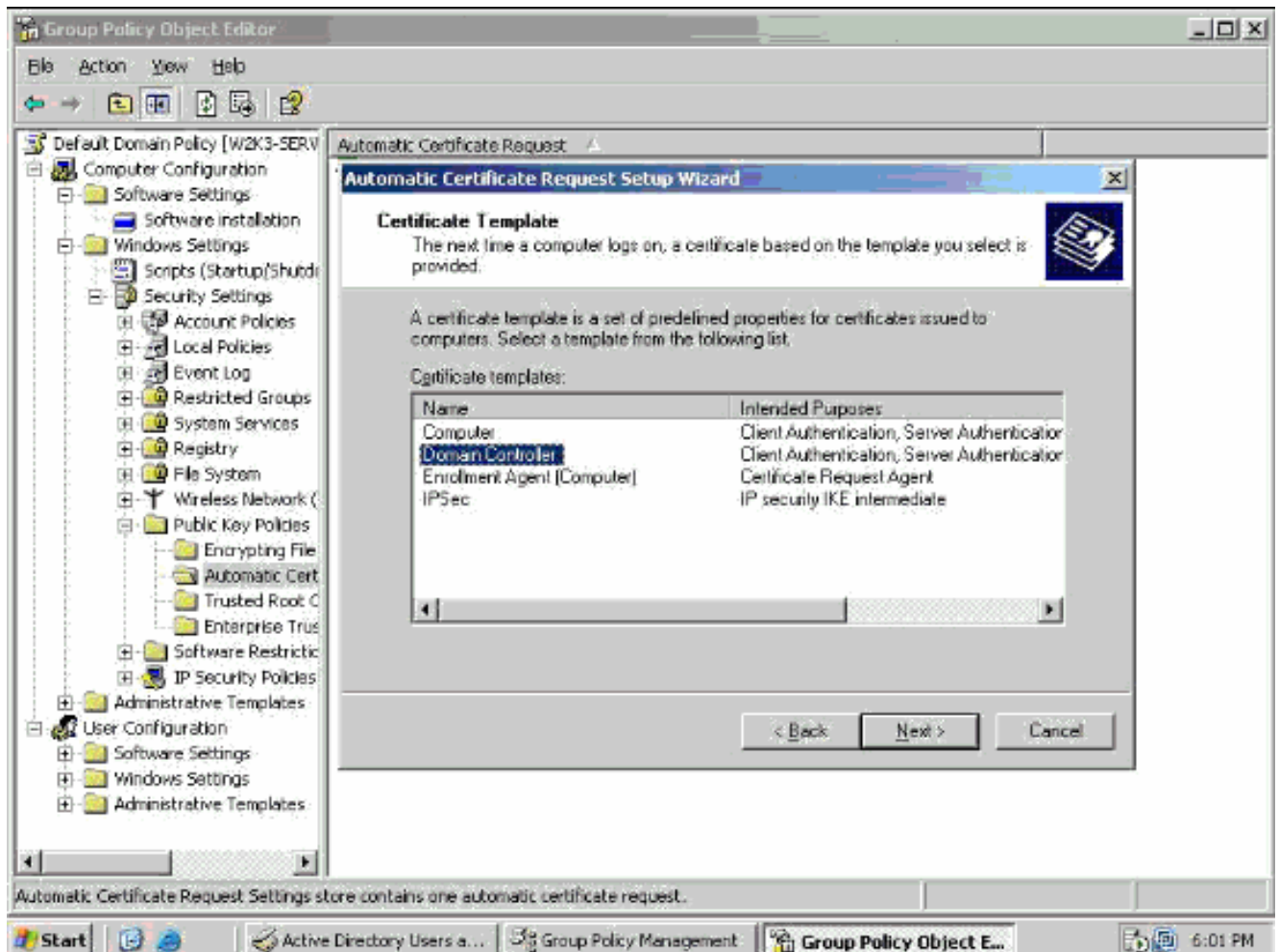
Auth Servers Lookup Servers Mapping Rules Auth Test Accounting

List · Edit

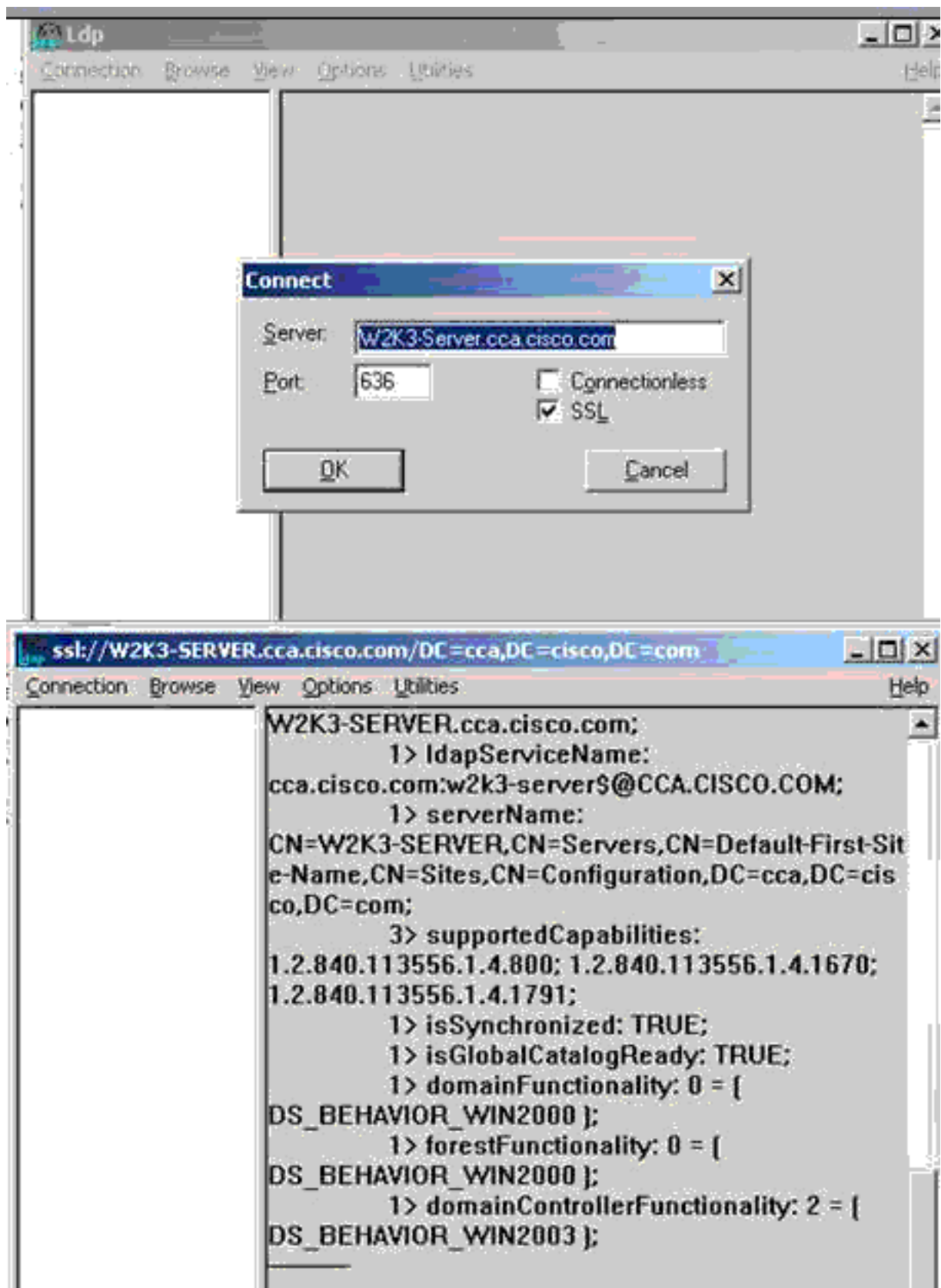
Authentication Type	LDAP	Provider Name	RootldapS
Server URL	ldaps://192.168.137.9:63	Server version	Auto
Search(Admin) Full DN	CN=root123, CN=users,	Search(Admin) Password	●●●●●●●●
Search Base Context	DC=CCA, DC=CISCO, D	Search Filter	sAMAccountName=\$us
Referral	Handle (Follow)	DerefLink	ON
DerefAlias	Always	Security Type	SSL
Default Role	Allow All		
Description			

Update Server Cancel

3. 获取在域控制器(DC)的证书。当您请求DC的时一证书，请确保放置CN作为活动目录完全限定域名。LDAP证书在本地计算机的个人证书存储查找。参考[如何启用在SSL的LDAP与一第三方证书颁发机构](#)欲知更多信息。
4. 配置SSL的域控制器。在您的DC，请选择开始>所有Programs > Administrative Tools>活动目录用户和计算机。在Active Directory Users及Computers窗口，请用鼠标右键单击在您的域名并且选择属性。在域Properties对话框中，请选择Group Policy选项。选择默认域策略组策略然后单击编辑。选择计算机Configuration> Windows设置。选择安全设置然后选择公共密钥策略。选择自动证书请求设置。请使用向导为了添加域控制器的一项策略正如在此示例：



5. 验证LDAP的域控制器在SSL。在您的DC，请选择Start > Run并且键入ldp.exe。从连接目录，请点击Connectand填写服务器和端口的值。这验证在SSL的LDAP在DC正确地配置。



6. 选择用户管理> Test选项认证服务器>的验证为了验证CAM IDAP配置。

User Management > Auth Servers

Auth Servers Lookup Server Mapping Rules **Auth Test** Accounting

Provider

User Name

Password

Managed Network VLAN
(optional)

Result: Successful
Role: Unauthenticated Role

[验证](#)

当前没有可用于此配置的验证过程。

[故障排除](#)

目前没有针对此配置的故障排除信息。

[相关信息](#)

- [Cisco NAC设备支持页面](#)
- [技术支持和文档 - Cisco Systems](#)