

NAC: Configure the LDAP Over SSL on the Clean Access Manager (CAM)

Document ID: 107322

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Configure

- Steps to Configure LDAP over SSL on CAM

Verify

Troubleshoot

[NetPro Discussion Forums – Featured Conversations](#)

Related Information

Introduction

This document describes how to configure the Lightweight Directory Access Protocol (LDAP) over SSL on the Clean Access Manager (CAM).

Prerequisites

Requirements

This configuration is applicable to the CAM version 3.5 and later.

Components Used

The information in this document is based on the Clean Access Manager version 4.1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Steps to Configure LDAP over SSL on CAM

Complete these steps:

1. Obtain the root certificate of the untrusted CA which has issued the certificate to the Domain Controller and place it on your desktop.
 - a. Choose **Administrator > CAM > SSL certificate**, and then browse and upload the Root CA certificate as **Trust Non-Standard 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, there is a 'Choose an action:' dropdown menu set to 'Import Certificate'. The 'Certificate File:' field contains the path 'C:\Documents and Settings\Adminir' with a 'Browse...' button next to it. The 'File Type' dropdown is set to '^ Trust Non-Standard CA' with an 'Upload' button. Below the file selection, there is an 'Uploaded Certificate List' table with three rows: '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 located at the bottom of the list. A small blue note at the bottom of the page reads: '(+ "Trust Non-Standard CA" is for SSL communication between the Clean Access Manager and some authentication servers, e.g. LDAP Server.)'

- b. Click **Verify** and install the Root CA certificate.
2. Configure the LDAP server on the CAM.
 - a. Choose **User Management > Auth Servers** and choose **New**.
 - b. Choose **LDAP** as the Authentication type.
 - c. Choose **ldaps://ip.address:636** as the Server URL.
 - d. Choose **SSL** as the Security Type.
 - e. Choose **Handle (Follow)!** as the Referral. This option is set for the Partition Domain Environment, for example, Root and Child Domains.
 - f. Admin privilege user and password is required to successfully bind the CAM (ldap client) to the LDAP server.

User Management > Auth Servers

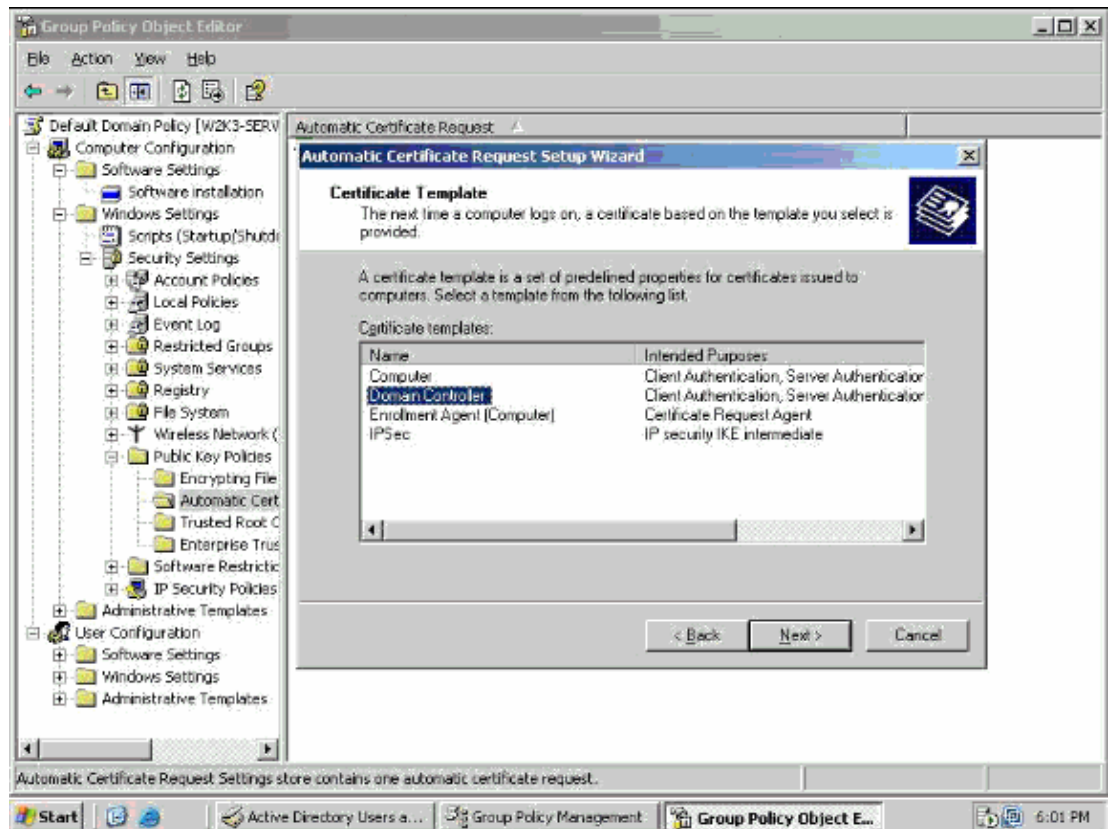
Auth Servers	Lookup Servers	Mapping Rules	Auth Test	Accounting
List · Edit				
Authentication Type	LDAP	Provider Name	RootHdapS	
Server URL	ldaps://192.168.137.9:63	Server version	Auto	
Search(Admin) Full DN	CN=root123, CN=users,	Search(Admin) Password	●●●●●●●●	
Search Base Context	DC=CCA, DC=CISCO, D	Search Filter	sAMAccountName=*	
Referral	Handle (Follow)	DerefLink	ON	
DerefAlias	Always	Security Type	SSL	
Default Role	Allow All			
Description				
		Update Server	Cancel	

3. Obtain the certificate on the Domain Controller (DC).

When you request a certificate for DC, make sure to put the CN as Active Directory fully qualified domain name. LDAPS certificate is located in the personal certificate store of the local computer. Refer to How to enable LDAP over SSL with a third-party certification authority for more information.

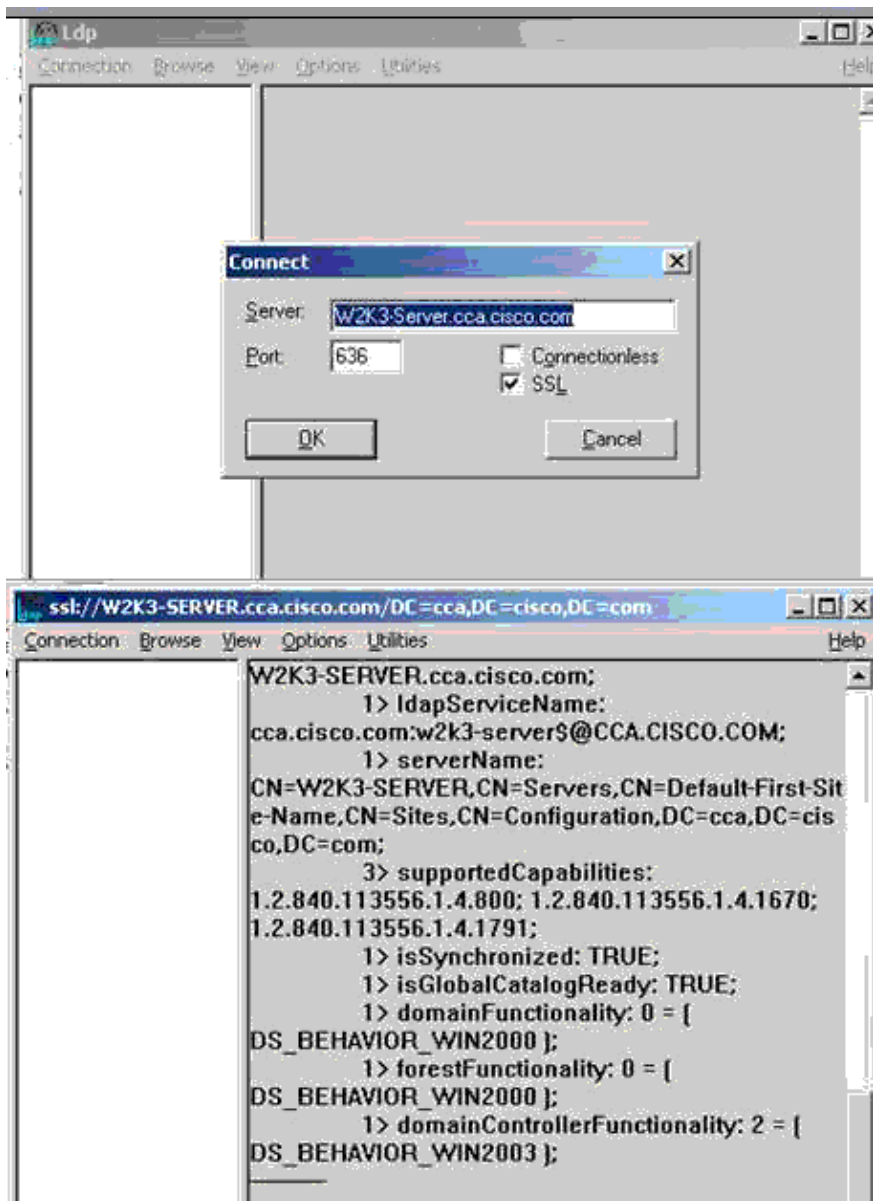
4. Configure the Domain Controller for SSL.

- On your DC, choose **Start > All Programs > Administrative Tools > Active Directory Users and Computer**.
- In the Active Directory Users and Computers window, right-click on your domain name and choose **Properties**.
- In the Domain Properties dialog box, choose the **Group Policy** tab.
- Choose the **Default Domain Policy** group policy and then click **Edit**.
- Choose **Computer Configuration > Windows Settings**.
- Choose **Security Settings** and then choose **Public Key Policies**.
- Choose **Automatic Certificate Request Settings**.
- Use the wizard in order to add a policy for Domain Controllers as in this example:

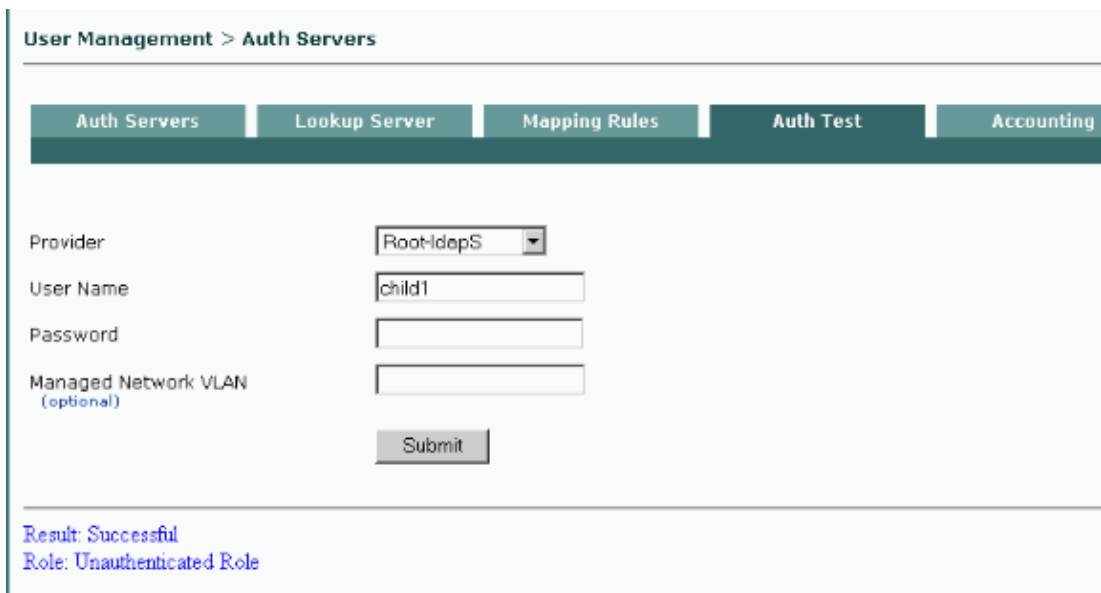


5. Verify the Domain Controller for LDAP over SSL.

On your DC, choose **Start > Run** and type **ldp.exe**. From the Connection Menu, click **Connect** and fill in the values for the server and port. This verifies that the LDAP over SSL is configured correctly on DC.



6. Choose **User Management > Auth Servers > AUTH Test** tab in order to verify the CAM LDAPS configuration.



Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Cisco NAC Appliance Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jun 02, 2008

Document ID: 107322
