ACS 5.X: Secure LDAP Server Configuration Example

Document ID: 113472

Contents

Introduction

Lightweight Directory Access Protocol (LDAP) is a networking protocol for querying and modifying directory services that run on TCP/IP and UDP. LDAP is a lightweight mechanism for accessing an x.500−based directory server. RFC 2251 defines LDAP.

Access Control Server (ACS) 5.x integrates with an LDAP external database, also called an identity store, by using the LDAP protocol. There are two methods to connect to the LDAP server: plain text (simple) and SSL (encrypted) connection. ACS 5.x can be configured to connect to the LDAP server using both the methods. In this document the ACS 5.x is configured to connect to an LDAP server using encrypted connection.

Prerequisites

Requirements

This document assumes that ACS 5.x has an IP connection to the LDAP server and the port TCP 636 is open.

The Microsoft® Active Directory LDAP server needs to be configured to accept secure LDAP connections on port TCP 636. This document assumes that you have the root certificate of the Certification Authority (CA) who issued the server certificate to the Microsoft LDAP server. For more information on how to configure the LDAP server, refer to How to enable LDAP over SSL with a third−party certification authority.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure ACS 5.x
- Microsoft Active Directory LDAP server

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 Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Directory Service

The directory service is a software application, or a set of applications, for storing and organizing information about a computer network's users and network resources. You can use the directory service to manage user access to these resources.

The LDAP directory service is based on a client−server model. A client starts an LDAP session by connecting to an LDAP server, and sends operation requests to the server. The server then sends its responses. One or more LDAP servers contain data from the LDAP directory tree or the LDAP back−end database.

The directory service manages the directory, which is the database that holds the information. Directory services use a distributed model for storing information, and that information is usually replicated between directory servers.

An LDAP directory is organized in a simple tree hierarchy and can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically.

An entry in the tree contains a set of attributes, where each attribute has a name (an attribute type or attribute description) and one or more values. The attributes are defined in a schema.

Each entry has a unique identifier: its Distinguished Name (DN). This name contains the Relative Distinguished Name (RDN) constructed from attributes in the entry, followed by the parent entry's DN. You can think of the DN as a full filename, and the RDN as a relative filename in a folder.

Authentication Using LDAP

ACS 5.x can authenticate a principal against an LDAP identity store by performing a bind operation on the directory server to find and authenticate the principal. If authentication succeeds, ACS can retrieve groups and attributes that belong to the principal. The attributes to retrieve can be configured in the ACS web interface (LDAP pages). These groups and attributes can be used by ACS to authorize the principal.

In order to authenticate a user or query the LDAP identity store, ACS connects to the LDAP server and maintains a connection pool.

LDAP Connection Management

ACS 5.x supports multiple concurrent LDAP connections. Connections are opened on demand at the time of the first LDAP authentication. The maximum number of connections is configured for each LDAP server. Opening connections in advance shortens the authentication time.

You can set the maximum number of connections to use for concurrent binding connections. The number of opened connections can be different for each LDAP server (primary or secondary) and is determined according to the maximum number of administration connections configured for each server.

ACS retains a list of open LDAP connections (including the bind information) for each LDAP server that is

configured in ACS. During the authentication process, the connection manager attempts to find an open connection from the pool.

If an open connection does not exist, a new one is opened. If the LDAP server closed the connection, the connection manager reports an error during the first call to search the directory, and tries to renew the connection.

After the authentication process is complete, the connection manager releases the connection to the connection manager. For more information, refer to the ACS 5.X User Guide.

Configure

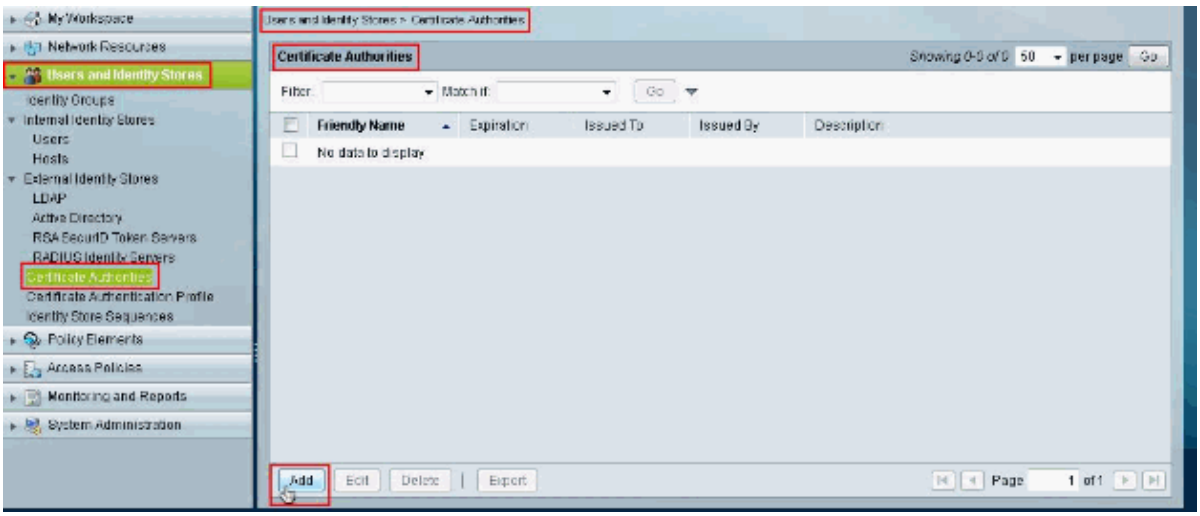
In this section, you are presented with the information to configure the features described in this document.

Install Root CA Certificate on ACS 5.x

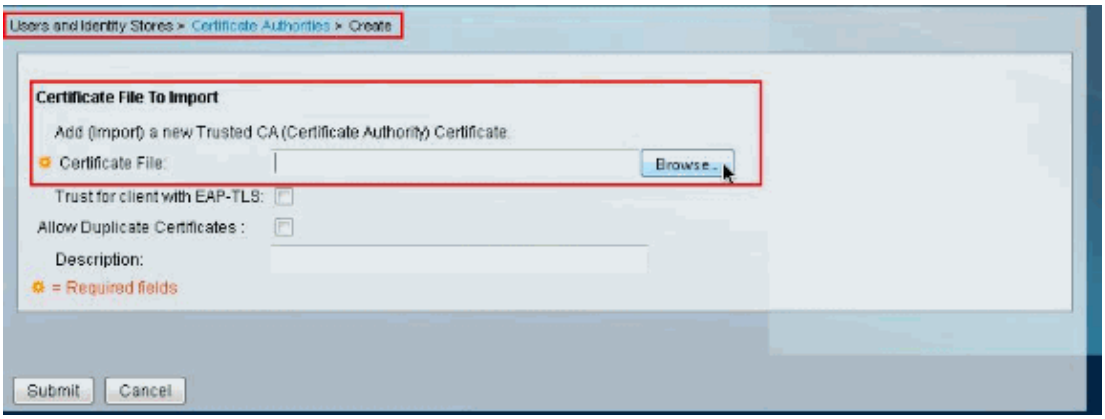
Complete these steps in order to install a Root CA Certificate on Cisco Secure ACS 5.x:

Note: Ensure that LDAP server is pre−configured to accept encrypted connections on port TCP 636. For more information on how to configure the Microsoft LDAP server, refer to How to enable LDAP over SSL with a third−party certification authority.

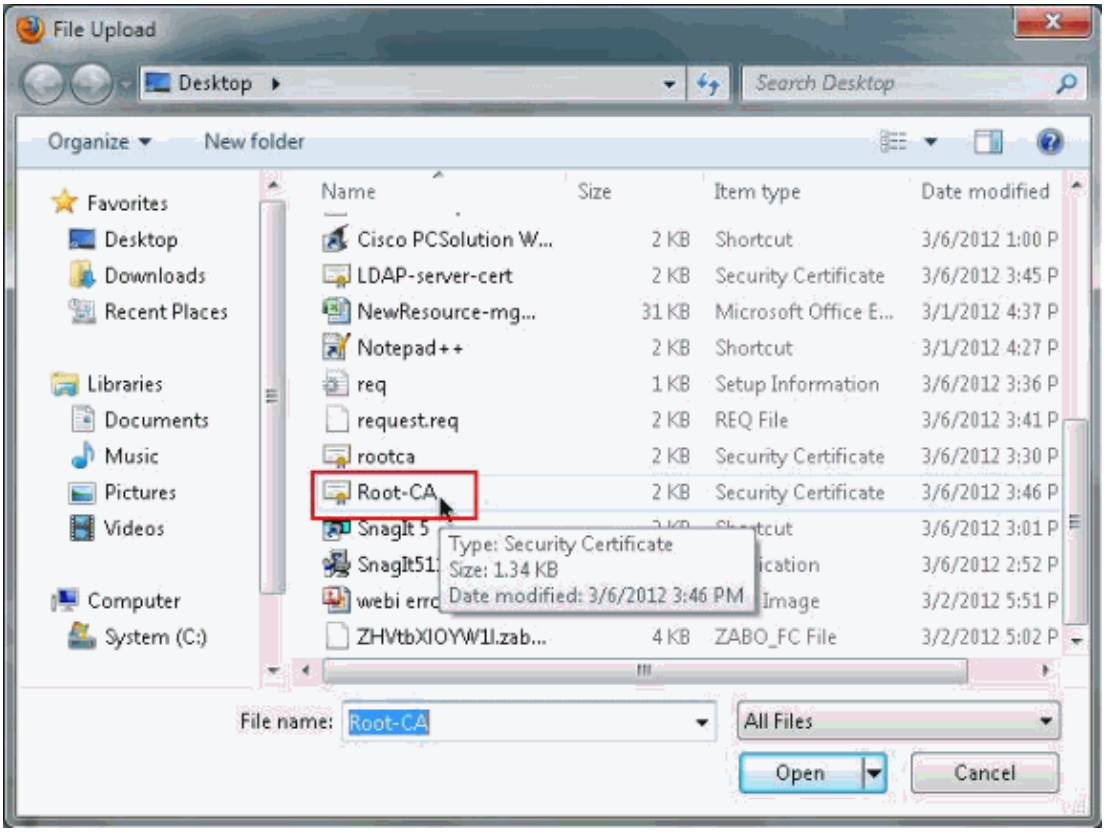
1. Choose **Users and Identity Stores** > **Certificate Authorities**, then click **Add** in order to add the root certificate of the CA who issued the server certificate to the Microsoft LDAP server.



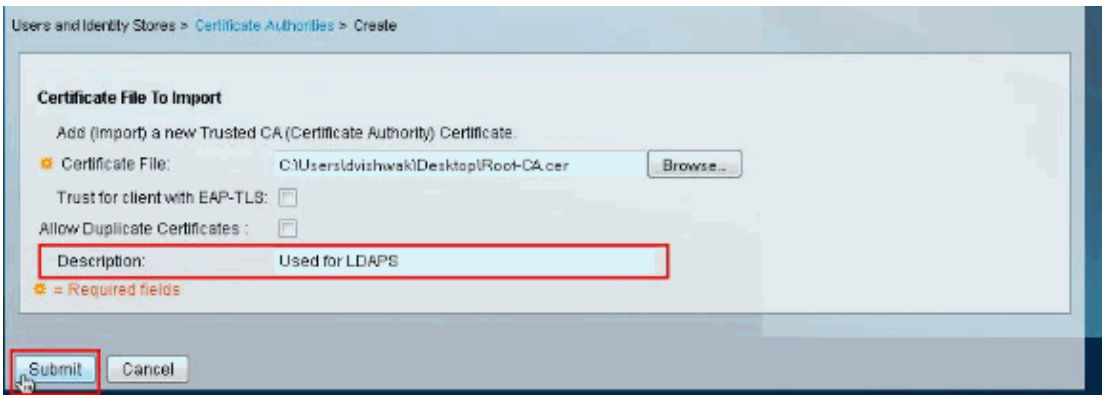
2. From the **Certificate File to Import** section, click **Browse** next to **Certificate File** in order to search for the Certificate File.



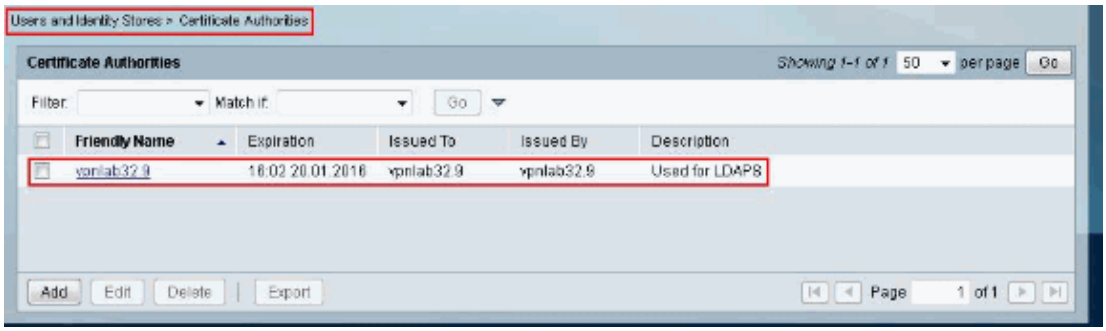
3. Choose the required **Certificate file** (the root certificate of the CA who issued the server certificate to the Microsoft LDAP server) and click **Open**.



4. Provide a **Description** in the space provided next to Description and click **Submit**.



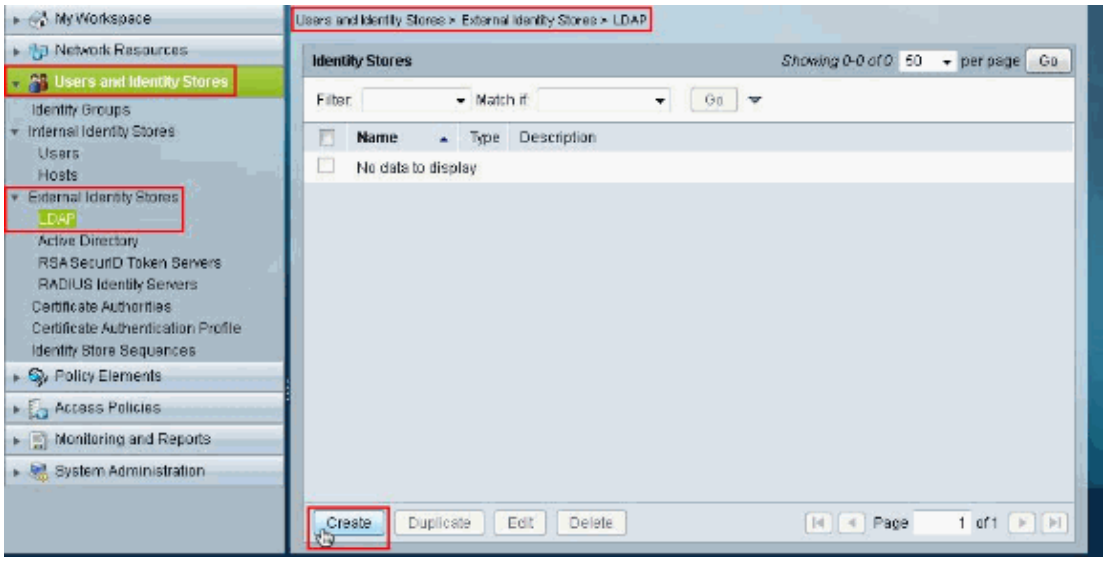
This image shows that the Root Certificate has been properly installed:



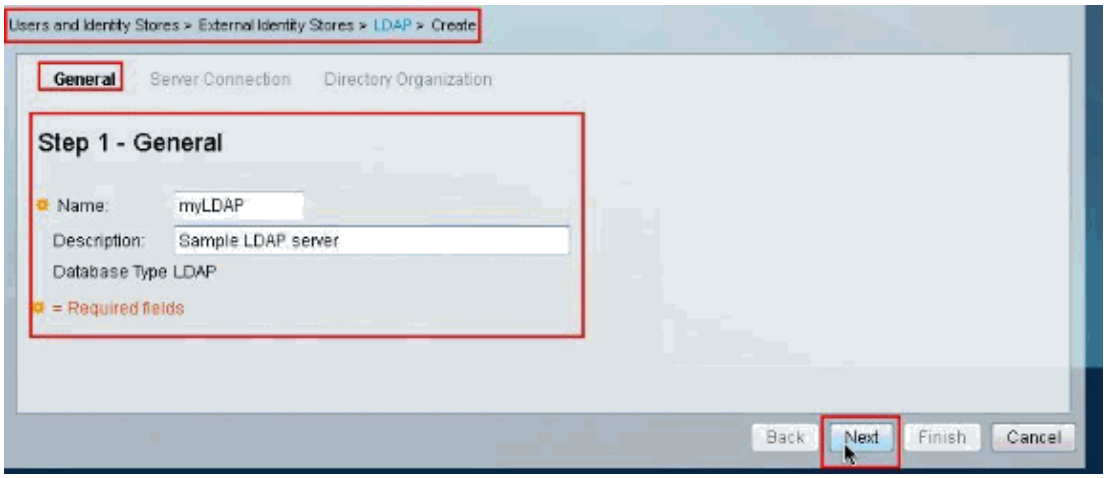
Configure ACS 5.X for Secure LDAP

Complete these steps in order to configure ACS 5.x for secure LDAP:

1. Choose **Users and Identity Stores > External Identity Stores > LDAP** and click **Create** to create a new LDAP connection.



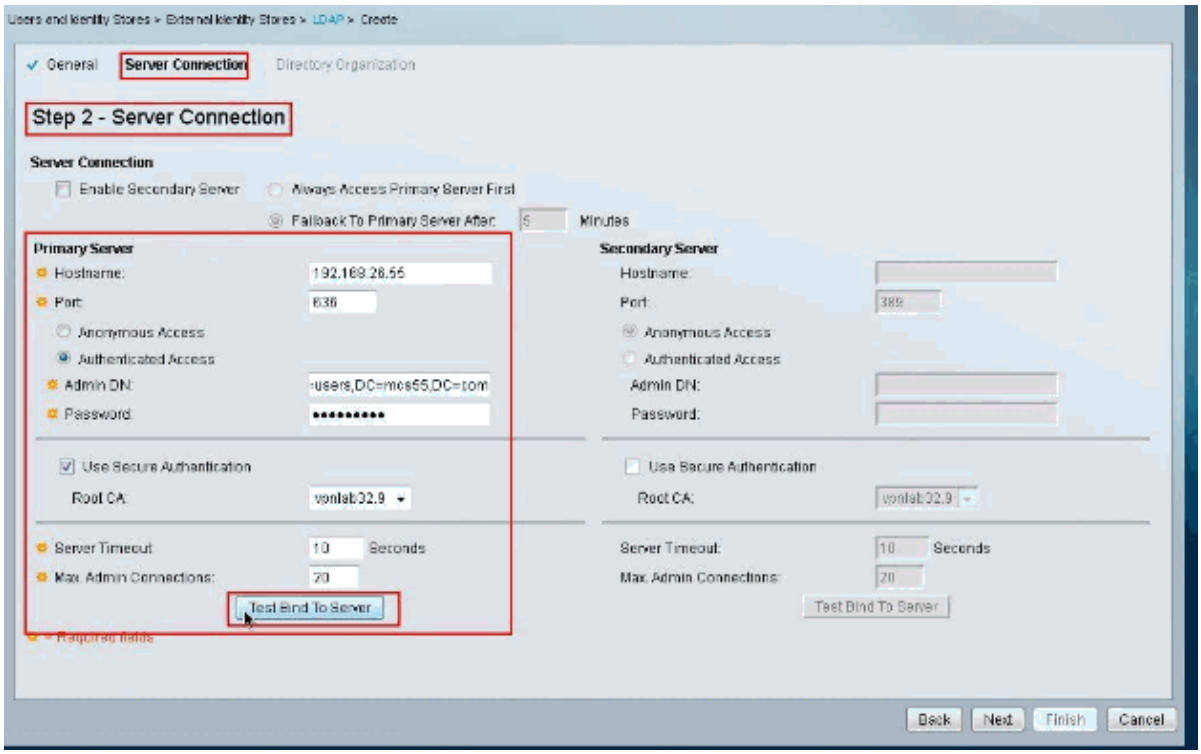
2. From the **General** tab provide the **Name** and **Description**(optional) for the new LDAP, then click **Next**.



3. From the **Server Connection** tab under the **Primary Server** section, provide the **Hostname, Port, Admin DN and Password**. Ensure that the checkbox next to **Use Secure Authentication** is checked and choose the recently installed **Root CA certificate**. Click **Test Bind To Server**.

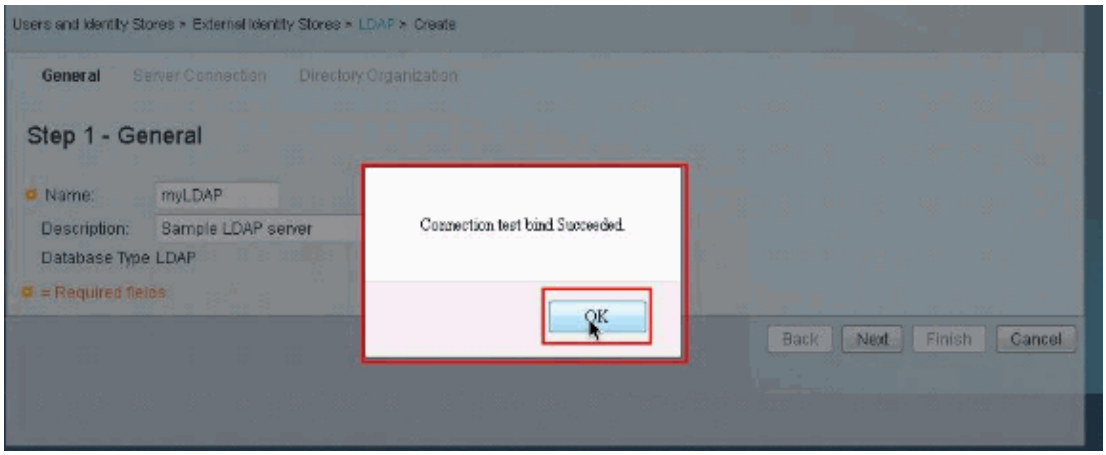
Note: IANA assigned port number for secure LDAP is TCP 636. However, confirm the port number that your LDAP server is using from your LDAP Admin.

Note: The Admin DN and Password should be provided to you by your LDAP Admin. The Admin DN must have read all permissions on all the OUs on the LDAP server.

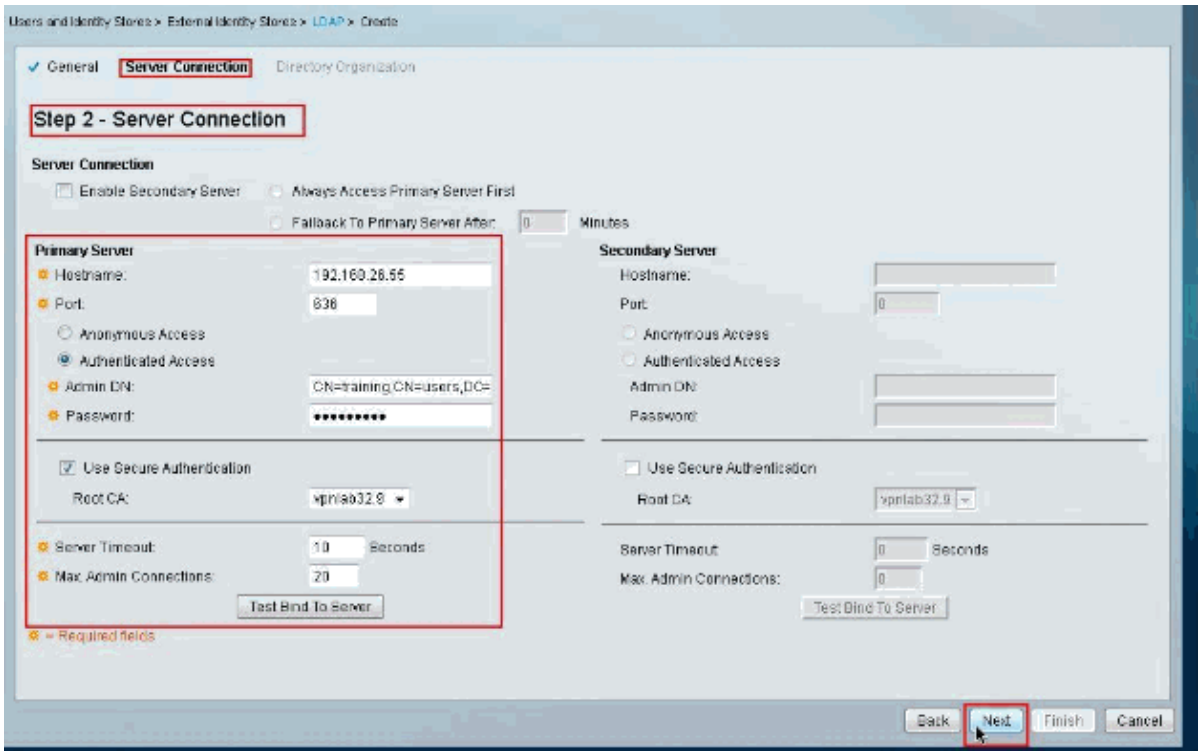


The next image shows that the **Connection Test Bind to the server** was successful.

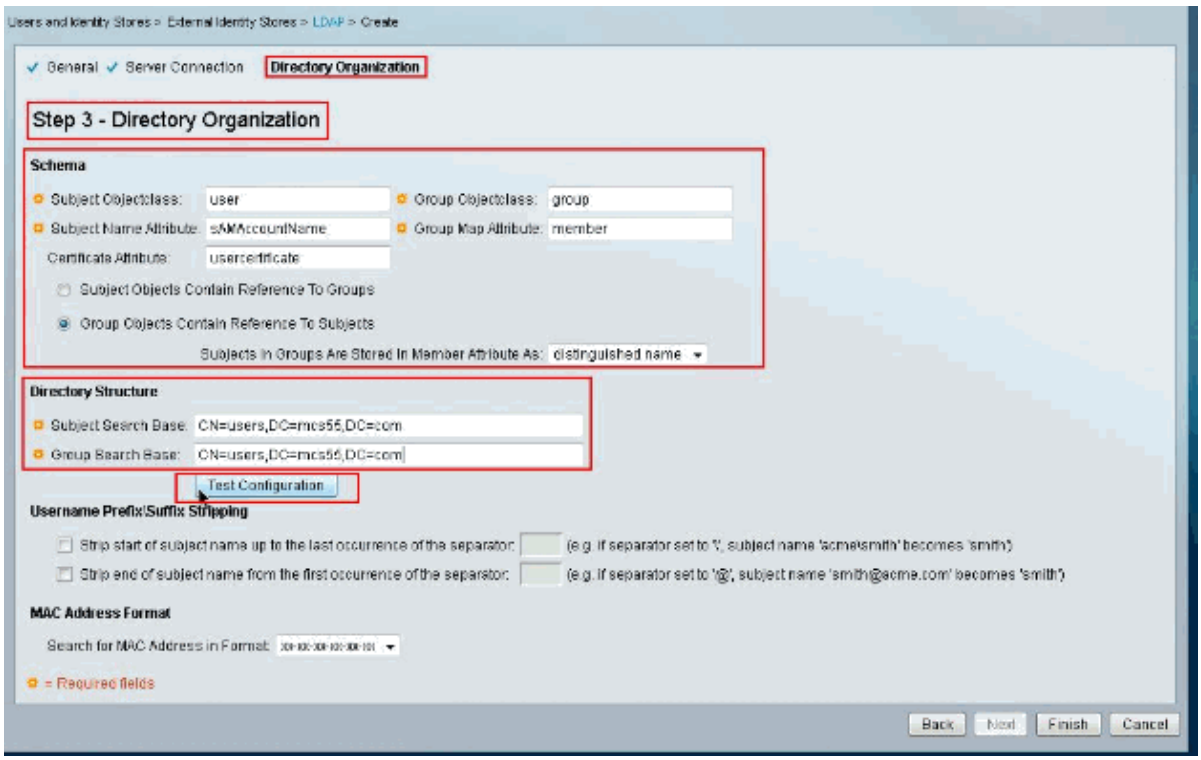
Note: If the Test Bind is not successful then re−verify the **Hostname, Port number, Admin DN, Password** and the **Root CA** from your LDAP Administrator.



4. Click **Next**.

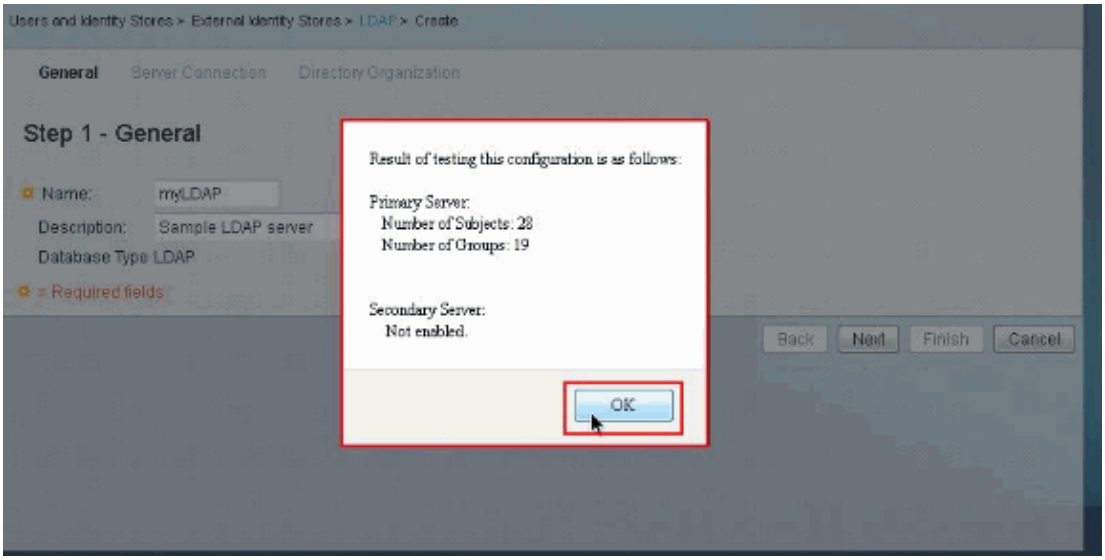


5. From the **Directory Organization** tab under the **Schema** section, provide the required details. Similarly, provide the required information under the **Directory Structure** section as provided by your LDAP Admin. Click **Test Configuration**.

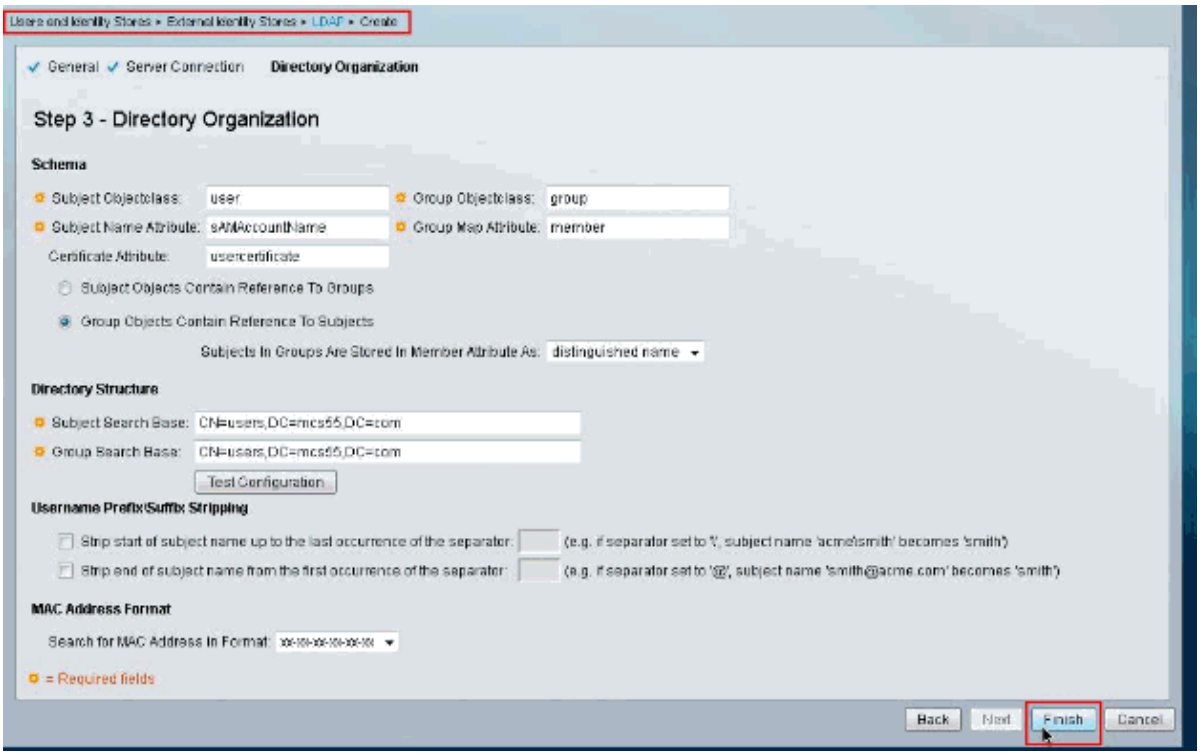


The next image shows that the **Configuration Test** is successful.

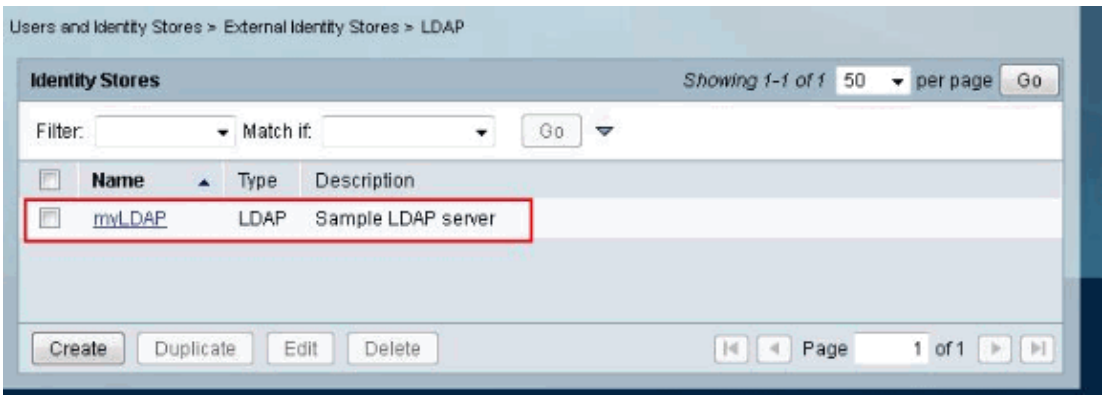
Note: If the Configuration Test is not successful then re−verify the parameters provided in the **Schema** and the **Directory Structure** from your LDAP Administrator.



6. Click **Finish**.



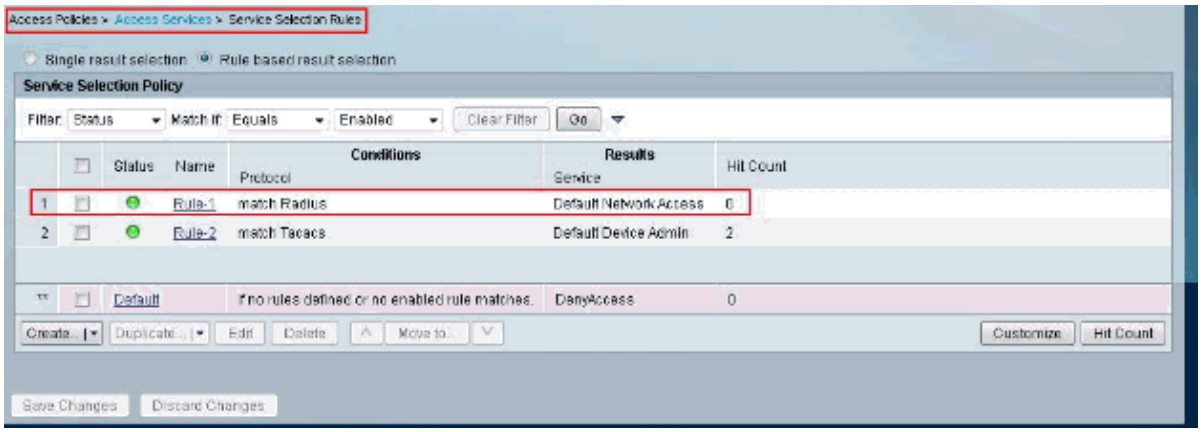
The **LDAP server** is created successfully.



Configure the Identity Store

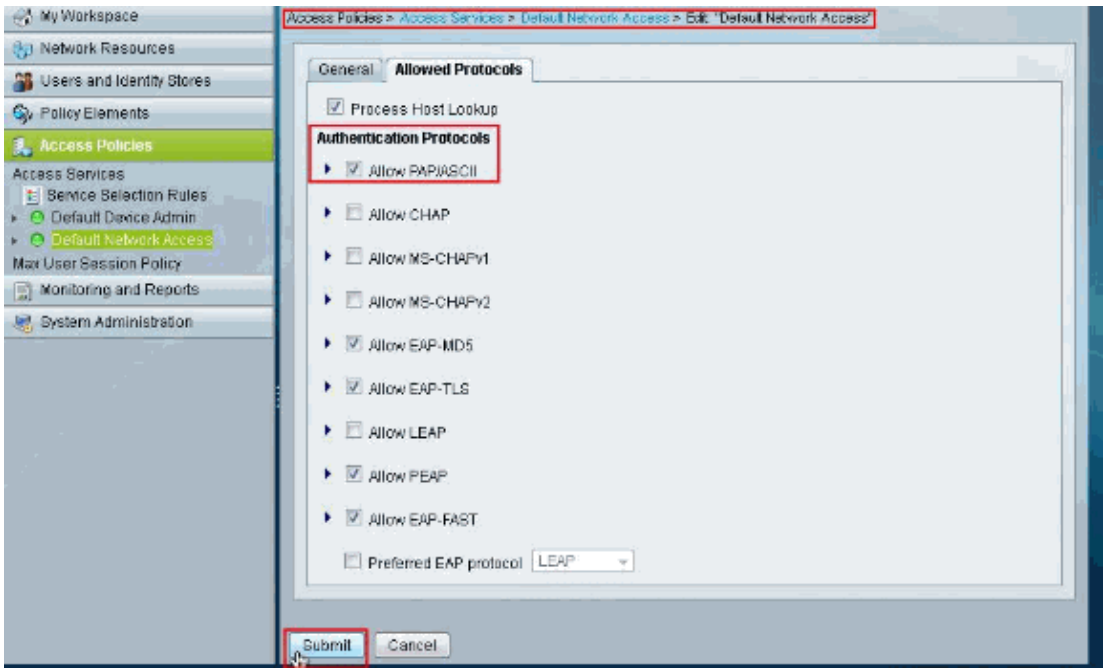
Compete these steps in order to configure the Identity Store:

1. Choose **Access Policies > Access Services > Service Selection Rules** and verify which service is going to use Secure LDAP server for Authentication. In this example the service is **Default Network Access**.

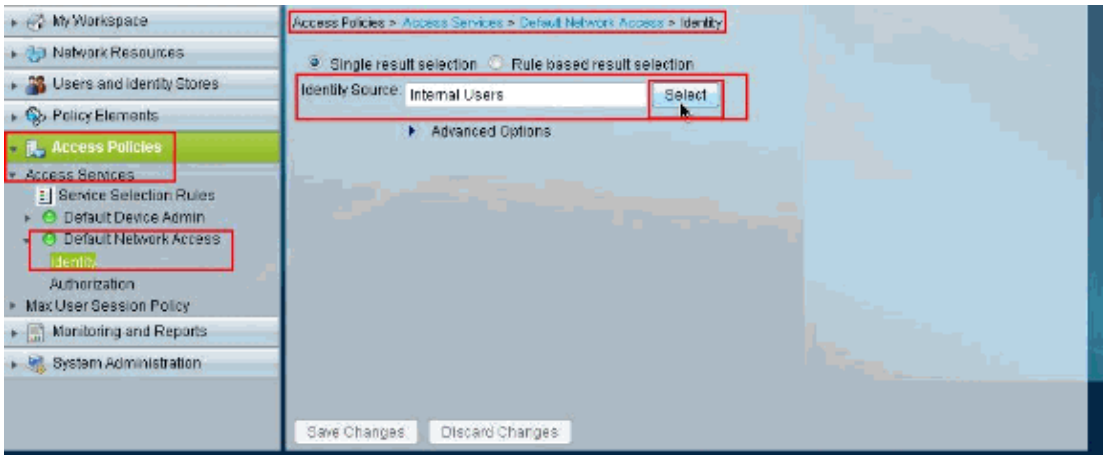


2. After you have verified the service in step 1, go to the particular service and click **Allowed Protocols**. Ensure that **Allow PAP/ASCII** is selected, then click **Submit**.

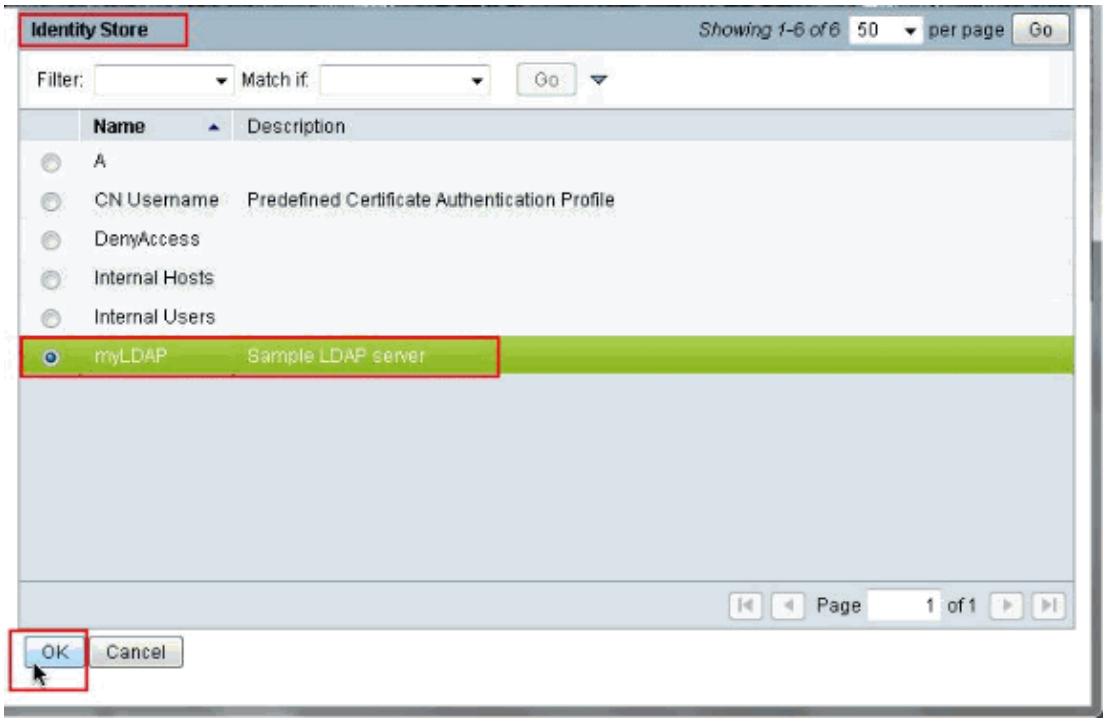
   Note: You can have other authentication protocols selected with Allow PAP/ASCII.



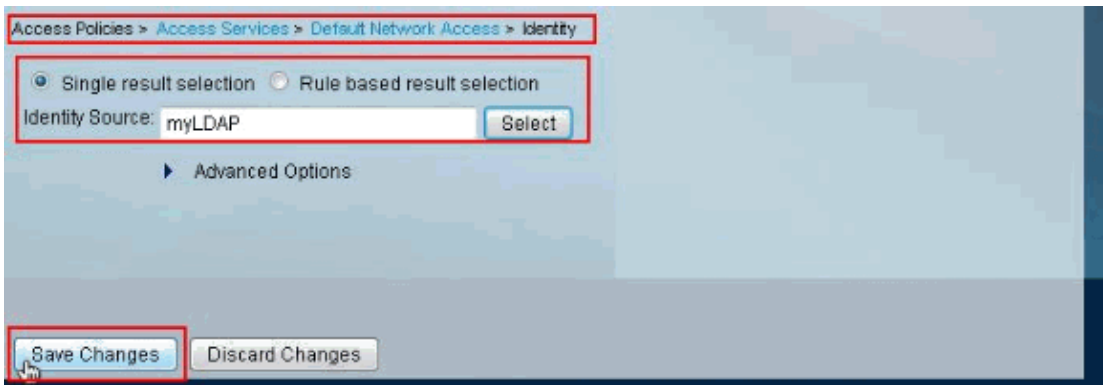
3. Click the service identified in step 1, then click **Identity**. Click **Select** next to **Identity Source**.



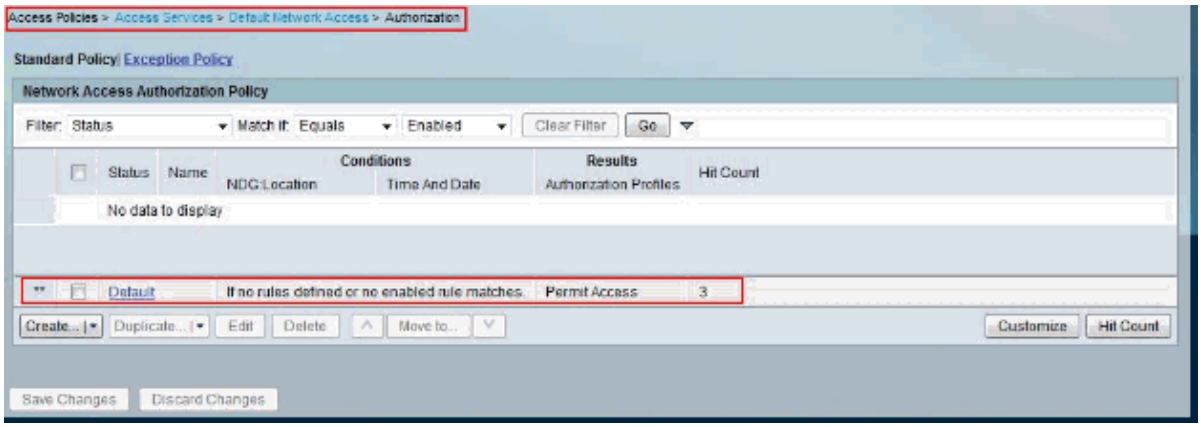
4. Select the newly created **secure LDAP Server** (**myLDAP** in this example), then click **OK**.



5. Click **Save Changes**.



6. Go to the **Authorization** section of the service identified in **step 1** and ensure that there is at least one rule that permits **Authentication**.



Troubleshoot

The ACS sends a bind request to authenticate the user against an LDAP server. The bind request contains the user's DN and user password in clear text. A user is authenticated when the user's DN and password matches the username and password in the LDAP directory.

- **Authentication Errors** ACS logs authentication errors in the ACS log files.
- **Initialization Errors** Use the LDAP server timeout settings to configure the number of seconds that the ACS waits for a response from an LDAP server before determining that the connection or authentication on that server has failed. Possible reasons for an LDAP server to return an initialization error are:
    - ♦ LDAP is not supported
    - ♦ The server is down
    - ♦ The server is out of memory
    - ♦ The user has no privileges
    - ♦ Incorrect administrator credentials are configured
- **Bind Errors** Possible reasons for an LDAP server to return bind (authentication) errors are:
    - ♦ Filtering errors
    - ♦ A search using filter criteria fails
    - ♦ Parameter errors
    - ♦ Invalid parameters were entered
    - ♦ User account is restricted (disabled, locked out, expired, password expired, and so on)

These errors are logged as external resource errors, which indicates a possible problem with the LDAP server:

- A connection error occurred
- The timeout expired
- The server is down
- The server is out of memory

This error is logged as an Unknown User error: `A user does not exist in the database`.

This error is logged as an Invalid Password error, where the user exists, but the password sent is invalid: `An invalid password was entered`.

Related Information

- **Cisco Secure Access Control System**

- **Requests for Comments (RFCs)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 19, 2012 Document ID: 113472