LDAP Servers for AAA

This chapter describes how to configure LDAP servers used in AAA.

About LDAP and the ASA

The ASA is compatible with the most LDAPv3 directory servers, including:

- Sun Microsystems JAVA System Directory Server, now part of Oracle Directory Server Enterprise Edition, and formerly named the Sun ONE Directory Server
- Microsoft Active Directory
- Novell
- OpenLDAP

By default, the ASA autodetects whether it is connected to Microsoft Active Directory, Sun LDAP, Novell, OpenLDAP, or a generic LDAPv3 directory server. However, if autodetection fails to determine the LDAP server type, you can manually configure it.

How Authentication Works with LDAP

During authentication, the ASA acts as a client proxy to the LDAP server for the user, and authenticates to the LDAP server in either plain text or by using the SASL protocol. By default, the ASA passes authentication parameters, usually a username and password, to the LDAP server in plain text.

The ASA supports only Digest-MD5 SASL mechanism. Using this mechanism, ASA responds to LDAP server with an MD5 value computed from the username and password.

When user LDAP authentication has succeeded, the LDAP server returns the attributes for the authenticated user. For VPN authentication, these attributes generally include authorization data that is applied to the VPN session. In this case, using LDAP accomplishes authentication and authorization in a single step.

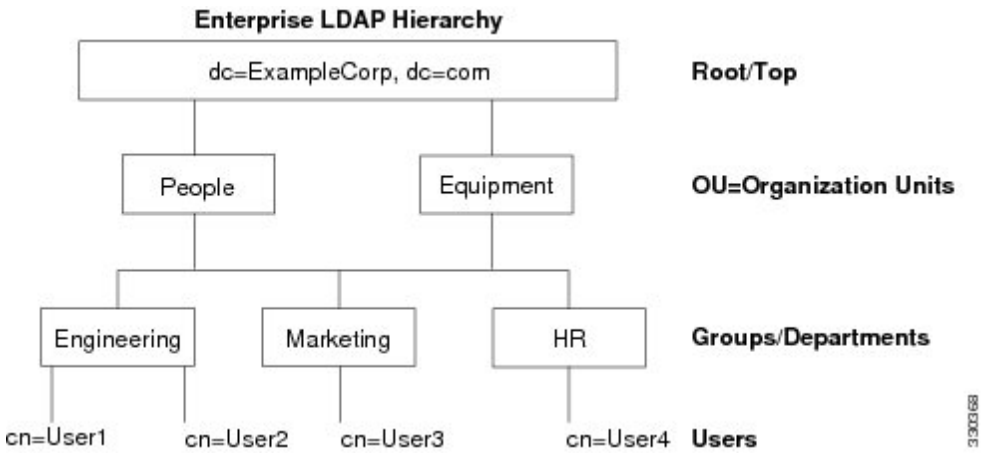
Note For more information about LDAP, see RFCs 1777, 2251, and 2849.

LDAP Hierarchy

Your LDAP configuration should reflect the logical hierarchy of your organization. For example, suppose an employee at your company, Example Corporation, is named Employee1. Employee1 works in the Engineering group. Your LDAP hierarchy could have one or many levels. You might decide to set up a single-level hierarchy in which Employee1 is considered a member of Example Corporation. Or you could set up a multi-level hierarchy in which Employee1 is considered to be a member of the department Engineering, which is a member of an organizational unit called People, which is itself a member of Example Corporation. See the following figure for an example of a multi-level hierarchy.

A multi-level hierarchy has more detail, but searches return results more quickly in a single-level hierarchy.

Figure 1: A Multi-Level LDAP Hierarchy



Search the LDAP Hierarchy

The ASA lets you tailor the search within the LDAP hierarchy. You configure the following three fields on the ASA to define where in the LDAP hierarchy that your search begins, the extent, and the type of information you are looking for. Together, these fields limit the search of the hierarchy to only the part that includes the user permissions.

- LDAP Base DN defines where in the LDAP hierarchy that the server should begin searching for user information when it receives an authorization request from the ASA.
- Search Scope defines the extent of the search in the LDAP hierarchy. The search proceeds this many levels in the hierarchy below the LDAP Base DN. You can choose to have the server search only the level immediately below it, or it can search the entire subtree. A single level search is quicker, but a subtree search is more extensive.
- Naming Attribute(s) defines the RDN that uniquely identifies an entry in the LDAP server. Common naming attributes can include cn (Common Name), sAMAccountName, and userPrincipalName.

The figure shows a sample LDAP hierarchy for Example Corporation. Given this hierarchy, you could define your search in different ways. The following table shows two sample search configurations.

In the first example configuration, when Employee1 establishes the IPsec tunnel with LDAP authorization required, the ASA sends a search request to the LDAP server, indicating it should search for Employee1 in the Engineering group. This search is quick.

In the second example configuration, the ASA sends a search request indicating that the server should search for Employee1 within Example Corporation. This search takes longer.

Table 1: Example Search Configurations

No.	LDAP Base DN	Search Scope	Naming Attribute	Result
1	group= Engineering,ou=People,dc=ExampleCorporation, dc=com	One Level	cn=Employee1	Quicker search
2	dc=ExampleCorporation,dc=com	Subtree	cn=Employee1	Longer search

Bind to an LDAP Server

The ASA uses the login DN and login password to establish trust (bind) with an LDAP server. When performing a Microsoft Active Directory read-only operation (such as authentication, authorization, or group search), the ASA can bind using a login DN with fewer privileges. For example, the login DN can be a user whose AD "Member Of" designation is part of Domain Users. For VPN password management operations, the login DN needs elevated privileges, and must be part of the Account Operators AD group.

The following is an example of a login DN:

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

The ASA supports the following authentication methods:

- Simple LDAP authentication with an unencrypted password on port 389
- Secure LDAP (LDAP-S) on port 636
- Simple Authentication and Security Layer (SASL) MD5

The ASA does not support anonymous authentication.

Note As an LDAP client, the ASA does not support the transmission of anonymous binds or requests.

LDAP Attribute Maps

The ASA can use an LDAP directory for authenticating users for:

- VPN remote access users
- Firewall network access/cut-through-proxy sessions

- Setting policy permissions (also called authorization attributes), such as ACLs, bookmark lists, DNS or WINS settings, and session timers.
- Setting the key attributes in a local group policy

The ASA uses LDAP attribute maps to translate native LDAP user attributes to ASA attributes. You can bind these attribute maps to LDAP servers or remove them. You can also show or clear attribute maps.

The LDAP attribute map does not support multi-valued attributes. For example, if a user is a member of several AD groups, and the LDAP attribute map matches more than one group, the value chosen is based on the alphabetization of the matched entries.

To use the attribute mapping features correctly, you need to understand LDAP attribute names and values, as well as the user-defined attribute names and values.

The names of frequently mapped LDAP attributes and the type of user-defined attributes that they would commonly be mapped to include the following:

- IETF-Radius-Class (Group_Policy in ASA version 8.2 and later)—Sets the group policy based on the directory department or user group (for example, Microsoft Active Directory memberOf) attribute value. The group policy attribute replaced the IETF-Radius-Class attribute with ASDM version 6.2/ASA version 8.2 or later.
- IETF-Radius-Filter-Id—Applies an access control list or ACL to VPN clients, IPsec, and SSL.
- IETF-Radius-Framed-IP-Address—Assigns a static IP address assigned to a VPN remote access client, IPsec, and SSL.
- Banner1—Displays a text banner when the VPN remote access user logs in.
- Tunneling-Protocols—Allows or denies the VPN remote access session based on the access type.

Note A single LDAP attribute map may contain one or many attributes. You can only map one LDAP attribute from a specific LDAP server.

Guidelines for LDAP Servers for AAA

This section includes the guidelines and limitations that you should check before configuring LDAP servers for AAA.

IPv6

The AAA server can use either an IPv4 or IPv6 address.

Additional Guidelines

- The DN configured on the ASA to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACL on the default password policy.
- You must configure LDAP over SSL to enable password management with Microsoft Active Directory and Sun servers.

- The ASA does not support password management with Novell, OpenLDAP, and other LDAPv3 directory servers.
- Beginning with Version 7.1(x), the ASA performs authentication and authorization using the native LDAP schema, and the Cisco schema is no longer needed.
- You can have up to 200 server groups in single mode or 4 server groups per context in multiple mode.
- Each group can have up to 16 servers in single mode or 8 servers in multiple mode.
- When a user logs in, the LDAP servers are accessed one at a time, starting with the first server that you specify in the configuration, until a server responds. If all servers in the group are unavailable, the ASA tries the local database if you configured it as a fallback method (management authentication and authorization only). If you do not have a fallback method, the ASA continues to try the LDAP servers.

Configure LDAP Servers for AAA

This section describes how to configure LDAP servers for AAA.

Procedure

Step 1 Configure LDAP attribute maps. See Configure LDAP Attribute Maps, on page 5.

Step 2 Add an LDAP server group. See Configure LDAP Server Groups, on page 6.

Step 3 Add a server to the group, then configure server parameters. See Add an LDAP Server to a Server Group , on page 7.

Configure LDAP Attribute Maps

To configure LDAP attribute maps, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **AAA Local Users** > **LDAP Attribute Map** (for local users), or **Configuration** > **Device Management** > **Users/AAA** > **LDAP Attribute Map** (for all other users), then click **Add**.

The **Add LDAP Attribute Map** dialog box appears with the **Mapping of Attribute Name** tab active.

Step 2 Create a name for this attribute map.

Step 3 Add the name of one of the LDAP attributes to be mapped.

Step 4 Choose a Cisco attribute.

Step 5 Click **Add**.

Step 6 To map more attributes, repeat Steps 1 through 5.

Step 7 Click the **Mapping of Attribute Value** tab to map the value of any of the LDAP attributes to a new value in the mapped Cisco attribute.

Step 8 Click **Add** to display the **Add Mapping of Attribute Value** dialog box.

Step 9 Enter the value for this LDAP attribute that you expect to be returned from the LDAP server.

Step 10 Enter the value you want to use in the Cisco attribute when this LDAP attribute contains the previous LDAP attribute value.

Step 11 Click **Add**.

Step 12 To map more attribute values, repeat Steps 8 through 11.

Step 13 Click **OK** twice to close each dialog box.

Step 14 Click **Apply** to save the settings to the running configuration.

Configure LDAP Server Groups

To create and configure an LDAP server group, then add an LDAP server to that group, perform the following steps:

Before you begin

You must add an attribute map before you may add an LDAP server to an LDAP server group.

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups**, or **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **AAA Server Groups** for VPN users.

Step 2 Click **Add**.

The **Add AAA Server Group** dialog box appears.

Step 3 Enter a name for the AAA server group.

Step 4 Choose the LDAP server type from the **Protocol** drop-down list.

Step 5 Click the radio button for the reactivation mode you want to use (**Depletion** or **Timed**).

In Depletion mode, failed servers are reactivated only after all of the servers in the group are inactive.

In Timed mode, failed servers are reactivated after 30 seconds of down time.

a) If you chose the Depletion reactivation mode, enter a time interval in the **Dead Time** field.

The dead time is the duration of time, in minutes, that elapses between the disabling of the last server in a group and the subsequent re-enabling of all servers. Deadtime applies only if you configure fallback to the local database; authentication is attempted locally until the deadtime elapses.

Step 6 Add the maximum number of failed AAA transactions with the server to allow.

This option sets the number of failed connection attempts allowed before declaring a non-responsive server to be inactive.

Step 7 Click **OK**.

The **Add AAA Server Group** dialog box closes, and the new server group is added to the AAA server group.

Step 8 Click **Apply** to save the changes to the running configuration.

Add an LDAP Server to a Server Group

To add an LDAP server to a server group, perform the following steps:

Procedure

Step 1 Choose one of the following:

- **Configuration Remote Access VPN AAA/Local Users AAA Server Groups** for VPN users.
- **Configuration** >**Device Management** > **Users/AAA** > **AAA Server Groups**

Step 2 Select the server group to which you want to add a server, then click **Add**.

The **Add AAA Server** dialog box appears for the selected server group.

Step 3 Choose the name of the interface that connects to the LDAP server.

Step 4 Add either the server name or IP address of the LDAP server.

Step 5 Add a timeout value or keep the default. The timeout is the duration of time, in seconds, that the ASA waits for a response from the primary server before sending the request to the backup server.

Step 6 In the **LDAP Parameters for authentication/authorization** area, configure the following settings:

- **Enable LDAP over SSL** (also called secure LDAP or LDAP-S)—Check this check box to use SSL to secure communications between the ASA and the LDAP server.

  Note
  If you do not configure the SASL protocol, we strongly recommend that you secure LDAP communications with SSL.

- **Reference Identity Name**—Enter reference-identity name to validate LDAP server identity.
- **Server Port**—Enter TCP port number 389, the port which the ASA uses to access the LDAP server for simple (non-secure) authentication, or TCP port 636 for secure authentication (LDAP-S). All LDAP servers support authentication and authorization. Only Microsoft AD and Sun LDAP servers additionally provide a VPN remote access password management capability, which requires LDAP-S.
- **Server Type**—Specify the LDAP server type from the drop-down list. The available options include the following:
  - **Detect Automatically/Use Generic Type**
  - **Microsoft**
  - **Novell**
  - **OpenLDAP**
  - **Sun, now part of Oracle Directory Server Enterprise Edition**

- **Base DN**—Enter the base distinguished name (DN) or location in the LDAP hierarchy where the server should begin searching when it receives an LDAP request (for example, OU=people, dc=cisco, dc=com).
- **Scope**—Specify the extent of the search that the server should perform in the LDAP hierarchy when it receives an authorization request from the drop-down list. The following options are available:
  - **One Level**—Searches only one level beneath the Base DN. This option is quicker.
  - **All Levels**—Searches all levels beneath the Base DN (that is, searches the entire subtree hierarchy). This option takes more time.
- **Naming Attribute(s)**—Enter the relative distinguished name attribute(s) that uniquely identify an entry on the LDAP server. Common naming attributes are Common Name (CN), sAMAccountName, userPrincipalName, and User ID (uid).
- **Login DN and Login Password**—The ASA uses the login DN and login password to establish trust (bind) with an LDAP server. Specify the login password, which is the password for the login DN user account.
- **LDAP Attribute Map**—Select one of the attribute maps that you created for this LDAP server to use. These attribute maps map LDAP attribute names to Cisco attribute names and values.
- **SASL MD5 authentication**—This enables the MD5 mechanism of the SASL to authenticate communications between the ASA and the LDAP server.
- **LDAP Parameters for Group Search**—The fields in this area configure how the ASA requests AD groups.
  - **Group Base DN**—Specifies the location in the LDAP hierarchy to begin searching for the AD groups (that is, the list of memberOf enumerations). If this field is not configured, the ASA uses the base DN for AD group retrieval. ASDM uses the list of retrieved AD groups to define AAA selection criteria for dynamic access policies. For more information, see the **show ad-groups** command.
  - **Group Search Timeout**—Specify the maximum time to wait for a response from an AD server that was queried for available groups.
- **LDAP SSL Client Certificate/Client Identity Certificate Trustpoint**—If you enable LDAP over SSL, you can select the certificate trustpoint that the ASA client should present to the LDAP server for authentication. A trustpoint is required if you configure the LDAP server to authenticate client certificates. If you do not configure a certificate, the ASA does not present one when the LDAP server asks for it. If an LDAP server is configured to require a peer certificate, the secure LDAP session will not complete and authentication/authorization requests will fail.

Step 7 Click **OK**.

The **Add AAA Server** dialog box closes, and the AAA server is added to the AAA server group.

Step 8 Click **Apply** to save the changes to the running configuration.

Test LDAP Server Authentication and Authorization

To determine whether the ASA can contact an LDAP server and authenticate or authorize a user, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups**.

Step 2 Select the server group in which the server resides.

Step 3 Select the server that you want to test.

Step 4 Click **Test**.

The **Test AAA Server** dialog box appears for the selected server.

Step 5 Click the type of test that you want to perform—**Authentication** or **Authorization**.

Step 6 Enter a username.

Step 7 If you are testing authentication, enter the password for the username.

Step 8 Click **OK**.

The ASA sends either an authentication or authorization test message to the server. If the test fails, an error message appears.

Monitoring LDAP Servers for AAA

See the following commands for monitoring LDAP servers for AAA:

- **Monitoring > Properties > AAA Servers**

  This pane shows the configured AAA server statistics.

- **Tools > Command Line Interface**

  This pane allows you to issue various non-interactive commands and view results.

History for LDAP Servers for AAA

Table 2: History for AAA Servers

Feature Name	Platform Releases	Description
LDAP Servers for AAA	7.0(1)	LDAP Servers describe support for AAA and how to configure LDAP servers. We introduced the following screens: Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Remote Access VPN > AAA Local Users > LDAP Attribute Map.
LDAP servers with IPv6 addresses for AAA	9.7(1)	You can now use either an IPv4 or IPv6 address for the AAA server.
Increased limits for AAA server groups and servers per group.	9.13(1)	You can configure more AAA server groups. In single context mode, you can configure 200 AAA server groups (the former limit was 100). In multiple context mode, you can configure 8 (the former limit was 4). In addition, in multiple context mode, you can configure 8 servers per group (the former limit was 4 servers per group). The single context mode per-group limit of 16 remains unchanged. We modified the AAA screens to accept these new limits.
Mutual LDAPS authentication.	9.18(1)	You can configure a client certificate for the ASA to present to the LDAP server when it requests a certificate to authenticate. This feature applies when using LDAP over SSL. If an LDAP server is configured to require a peer certificate, the secure LDAP session will not complete and authentication/authorization requests will fail. We modified the following screen: **Configuration** > **Device Management** > **Users/AAA** > > **AAA Server Groups**, Add/Edit LDAP server.