LDAP Configuration

Overview

Cisco WAE supports authentication and authorization of foreign users using the LDAP protocol. The embedded directory service within the WAE system is based upon Java Enterprise Directory libraries that are linked with the Tomcat server instance. The objective of the LDAP module is to allow customers to map multiple LDAP user groups to privilege level roles in the WAE system.

Before You Begin

You should have the following:

- Cisco WAE Release 6.0 or above installed
- An external LDAP server
- An ldapsearch Linux library
- An LDAP user account with permissions to read the necessary LDAP schema

Pre-Installation Steps

Step 1 Install the ldapsearch binary.

Note The ldapsearch binary is not required for the normal operation of LDAP with a WAE server. It is only necessary to discover the correct formatting of the LDAP schema required to configure the LDAP server settings. If necessary, the ldapsearch binary can be installed on an alternative machine. We recommend installing the binary on the WAE server as it can assist in troubleshooting LDAP protocol connection issues with the LDAP servers.

For Redhat or Centos systems:

```
sudo yum install openldap-clients
```

For Debian systems:

```
sudo apt-get install ldap-utils openssl libpam-ldap
```

Step 2 Gather LDAP server information. See Table 4-1 for a list of information required and the variables that are used throughout this chapter to represent this information.

Step 3 Retrieve the LDAP schema from the LDAP server.

```
ldapsearch -x -v -W -LLL -a always -h <ldap-server> -b <ldap-base-ou> -D <admin-user-dn>
```

This command assumes that the LDAP server does not use certificates or SSL encryption.

Note If you are dealing with a large LDAP dataset we recommend you use command line filters and/or pipe the output to a file.

This example uses parameters from a fictitious company:

```
ldapsearch -x -v -W -LLL -a always -h ldap-server.company.com -b "dc=company, dc=com" -D
"cn=admin,dc=company,dc=com"


ldap_initialize( ldap://ldap-server.company.com )
Enter LDAP Password: <admin-password>
```

Step 4 Review the LDAP schema.

Example 4-1shows a trimmed down version of an LDAP schema. Bold text denotes information that is required later for LDAP authentication and authorization.

Example 4-1 Trimmed Example of LDAP Schema

```
filter: (objectclass=*)
requesting: All userApplication attributes
dn: dc=company,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: ipnec
dc: ipnec

dn: cn=admin,dc=company,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: ****************************
```

(These are Organization Units containing other LDAP objects)

```
dn: ou=People,dc=company,dc=com
objectClass: organizationalUnit
ou: People

dn: ou=Groups,dc=company,dc=com
objectClass: organizationalUnit
ou: Groups
```

(This is a User Object)

```
dn: uid=cisco-mate-user1,ou=People,dc=company,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
uid: cisco-mate-user1
sn: mate-user1
givenName: cisco
cn: cisco-mate-user1
displayName: cisco-mate-user1
uidNumber: 1001
gidNumber: 101
loginShell: /bin/bash
```

```
homeDirectory: /home/cisco-mate-user1
userPassword:: ****************************
```

(This is a Group Ojbect)

```
dn: cn=cisco-mate-admin,ou=Groups,dc=company,dc=com
objectClass: groupOfUniqueNames
cn: cisco-mate-admin
uniqueMember: uid=cisco-mate-user1,ou=People,dc=company,dc=com
uniqueMember: uid=cisco-mate-user2,ou=People,dc=company,dc=com
```

Table 4-1 LDAP Server Information Needed for Configuration

Required Information	Notes / Variables Used
LDAP username and password	This user account must have at least read permissions to all the LDAP server tree scope that you wish use. For the remainder of this document the LDAP user Distinguished Name (DN) will be denoted as <admin-user-dn> For the remainder of this document the LDAP user password will be denoted as <admin-password> For examples used in this document the DN for the LDAP user name will be "cn=admin,dc=company,dc=com" Please consult your LDAP systems administrator if you are unsure about the DN for the LDAP user name.
LDAP search base Organizational Unit (OU) for all possible WAE users	For the remainder of this document the base OU will be denoted as <ldap-base-ou> The examples used in this document will use the base OU "dc=company, dc=com" There are performance benefits for the WAE/MATE login process if a more specific base OU is used
LDAP server IP or DNS address	LDAP servers can be clustered and use DNS load balancing, it is recommended that you use the DNS name. For the remainder of this document the LDAP server address will be denoted as <ldap-server> The examples used in this document will use the LDAP dns server address "ldap-server.company.com"

Configuring LDAP

You must have administrator privileges to configure LDAP.

Step 1 From the WAE UI, select **System > LDAP Server**.

Step 2 Enter the information needed for all fields, except within the Groups To Roles Mapping area. Leave the Groups To Roles Mapping area blank. For field descriptions, see Table 4-2.

Table 4-2 LDAP Server Field Descriptions

Field	Description
Enabled	Select to enable use of the LDAP server for user authentication. This must be selected to use the LDAP server for authentication.
Server <ldap-server>	LDAP server IP address or FQDN, which is the server's hostname with the DNS domain name appended to the end. FQDN format: *<LDAP_hostname>.<domain>*.com
Protocol	Protocol used to reach the LDAP server. • LDAP—Transmits communication in clear text. • LDAPS—Transmits communication that is encrypted and secure. Default value is LDAP.
Accept Any SSL Certificates	Applicable only if LDAPS is selected as the protocol. Use this option if you do not expect the LDAP server to have a valid SSL certificate for establishing encrypted communication with this system. If this option is not selected, the communication cannot be established unless the certificate used by the LDAP server to establish communication is valid.
Port	Port used to reach the LDAP server. For unencrypted authentication the default is TCP 389. For encrypted authentication the default is TCP 636. Default value is 389.
LDAP Client Username <admin-user>	The DN for the LDAP user login which requires minimum read only access to the necessary sections of the LDAP Tree schema. This should be in the DN format: "cn=admin,dc=company,dc=com" This information was collected in Pre-Installation Steps.
Password <admin-password>	The LDAP user password. This information was collected in Pre-Installation Steps.
Search Base <ldap-base-ou>	This is the Distinguished Name of the base search OU for all user accounts that should have permission to login to the WAE Server. This information was collected in Pre-Installation Steps.

Step 3 Click **Validate** to test the LDAP configuration you have entered. A window displaying test results appears.

Note If there are failures, you may have entered an incorrect server address or the LDAP user login is invalid. To resolve these issues, contact your LDAP system administrator.

Step 4 Configure LDAP group to roles mapping.

WAE mappings defaults to support Microsoft's Active Directory LDAP Schema.If you are using Active Directory you will not need to perform any advanced configurations.

The WAE LDAP system supports only one of the following mappings (cannot be mixed):

- LDAP Administrative Groups to Mate/WAE Groups in a Many : One relationship
- LDAP Specific Users to Mate/WAE Groups in a Many : One relationship

Note To configure LDAP specific users group mappings, contact your support representative.

a. From the LDAP schema that you downloaded in Pre-Installation Steps, identify the LDAP administrative groups (see Example 4-1). Locate the DN for the LDAP group objects that contain the LDAP attribute **objectClass: groupOfUniqueNames**.

b. Click **+Add Mapping**.

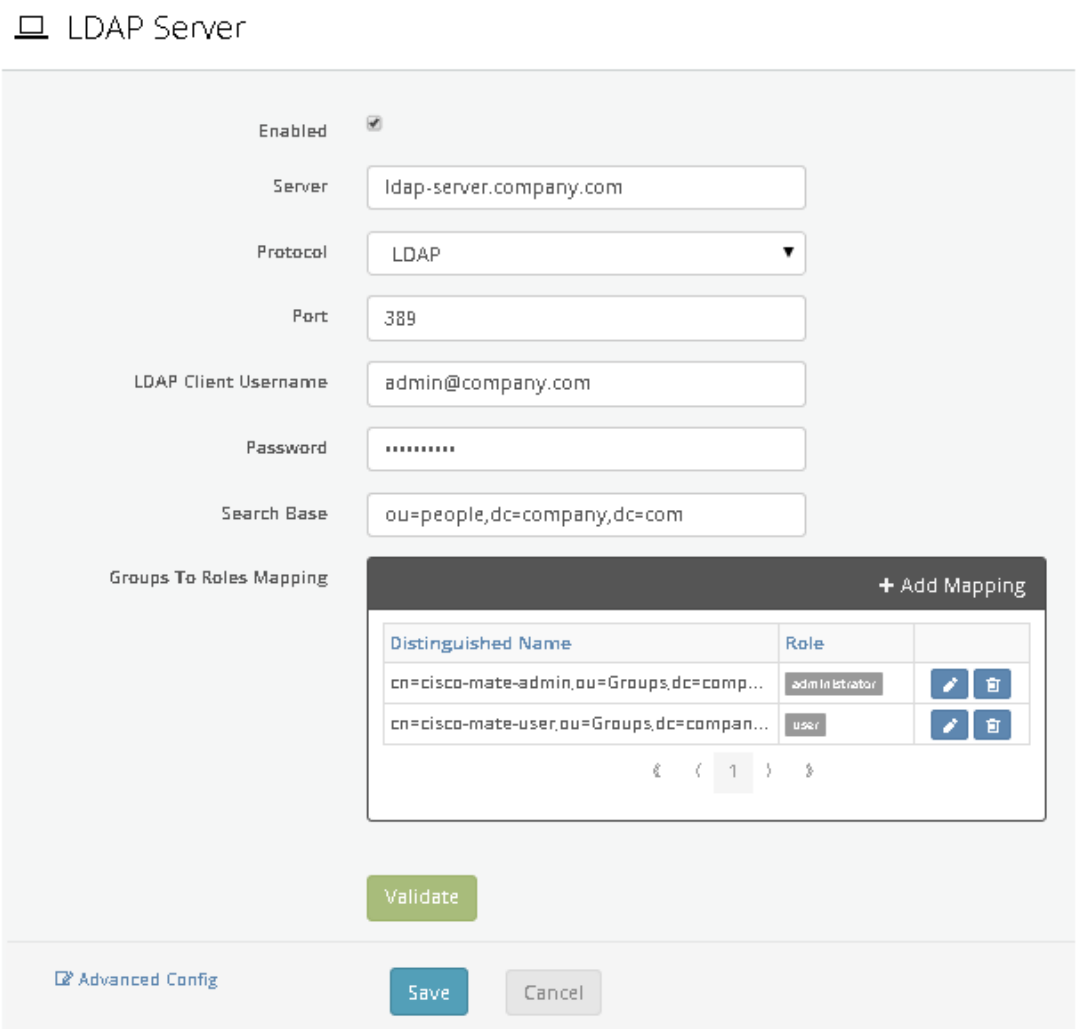
c. Enter the Distinguished Name. For example, cn=cisco-mate-admin,ou=Groups,dc=company,dc=com.

d. Check either the User or Administrator Role check box.

e. Repeat these steps to add more mappings.

Figure 4-1 shows an example of an LDAP Server page with populated fields.

Figure 4-1 Example of LDAP Server Page With Populated Fields



Step 5 Click the **Advanced Configuration** link located at the bottom left of the LDAP Server page. The Edit System Object window appears.

Step 6 View Table 4-3 and determine if lines 7 and 8 must be edited, then click **Save**.

Table 4-3 System Object Attributes

Attribute	Description
LDAP.Principal.Expr	Default : `"LDAP.Principal.Expr": "(userPrincipalName={0})",` The `{0}` token will be replaced by the user's input for username at the login page. The `userPrincipalName=` must match a User Objects' LDAP attribute that identifies the user under the LDAP search base. From the LDAP schema (Example 4-1), use the User Unique Attribute `uid`. The WAE server will search all objects under the LDAP search base tree for: `uid=cisco-mate-user1` Common alternatives include `userPrincipalName` or `userName` etc.
LDAP.Principal.Group.Attr	Default : `"LDAP.Principal.Group.Attr": "user.memberOf"` There are 2 options available here: • User searches (default): The WAE server will look for `user.memberOf` attributes, located under the LDAP User object itself. User based searches requires the ability for the server to execute a reverse LDAP lookup. For example, looking at a user object to determine the user's primary group object using the `memberOf` user attribute. • Group searches: Group based searches locates the membership of each administrative group that a particular user is a member of. Administrative Groups are based on `objectClass: groupOfUniqueNames` LDAP objects types. From the LDAP schema, find the unique attribute that lists the user association to the Group of Unique Names. In Example 4-1, this is `uniqueMember: uid=cisco-mate-user1,ou=People,dc=company,dc=com` `uniqueMember` is the attribute that the software is looking for to determine if a particular user is a member of a particular group.

Table 4-4 lists configuration examples that were based on tested default installations of the LDAP servers with default LDAP schema that were provided by the software vendor.

Step 7 From the LDAP Server page, click **Save**.

Step 8 To validate configuration, log off and log on to the WAE UI with a valid LDAP user account.

Note If you are experience issues, we recommend the following:

- Use an unencrypted LDAP first
- Review the log files listed in
  - $CARIDEN_HOME/lib/web/apache-tomcat-6.0.37/logs/catalina.
  - $CARIDEN_HOME/lib/web/apache-tomcat-6.0.37/logs/catalina.out
  - $CARIDEN_HOME/lib/web/apache-tomcat-6.0.37/logs/mate_live.log
  - $CARIDEN_HOME/lib/web/apache-tomcat-6.0.37/logs/user_manager.log

Table 4-4 Advanced Configurations Tested on Default LDAP Server Installations With Default LDAP Schema

LDAP Server / Vendor	Search Type	Default Advanced Configuration Settings
Sun One Directory Server Sun Enterprise Directory Server Oracle Directory Server Enterprise Edition	Group	"LDAP.Principal.Expr": "(uid={0})" "LDAP.Principal.Group.Attr": "group.uniquemember”
OpenLDAP	Group	"LDAP.Principal.Expr": "(uid={0})" "LDAP.Principal.Group.Attr": "group.uniqueMember"
Microsoft Active Directory (default)	User	"LDAP.Principal.Expr": "(userPrincipalName={0})" "LDAP.Principal.Group.Attr": "user.memberOf"
Novell Directory Services Novell eDirectory NetWare Directory Services NetIQ eDirectory	Group	"LDAP.Principal.Expr": "(Uif={0})" "LDAP.Principal.Group.Attr": "group.uniquemember"