Integrating With LDAP

This chapter contains the following sections:

- Overview, on page 1
- Configuring LDAP to Work with the Spam Quarantine, on page 1
- Creating the LDAP Server Profile, on page 2
- Configuring LDAP Queries, on page 4
- Domain-Based Queries, on page 9
- Chain Queries, on page 10
- Configuring AsyncOS to Work With Multiple LDAP Servers, on page 12
- Configuring External Authentication of Administrative Users Using LDAP , on page 14

Overview

If you maintain end-user passphrases and email aliases in a corporate LDAP directory — for example, in Microsoft Active Directory, SunONE Directory Server, or OpenLDAP directories — you can use the LDAP directory to authenticate the following users:

- End users and administrative users who access the spam quarantine.

  When a user logs in to the web UI for the spam quarantine, the LDAP server validates the login name and passphrase, and AsyncOS retrieves a list of the corresponding email aliases. Quarantined messages sent to any of the user's email aliases can appear in the spam quarantine, as long as the appliance does not rewrite them.

  See Configuring LDAP to Work with the Spam Quarantine, on page 1.

- Administrative users who sign in to the Cisco Secure Email and Web Manager appliance when External Authentication is enabled and configured.

  See Configuring External Authentication of Administrative Users Using LDAP , on page 14.

Configuring LDAP to Work with the Spam Quarantine

When you configure your Cisco Content Security appliance to work with an LDAP directory, you must complete the following steps to set up for acceptance, routing, aliasing, and masquerading:

Procedure

Step 1 **Configure an LDAP server profile**.

The server profile contains information to enable AsyncOS to connect to the LDAP server, such as:

- Server name and port
- Base DN
- Authentication requirements for binding to the server

For more information about configuring a server profile, see Creating the LDAP Server Profile, on page 2.

When you create the LDAP server profile, you can configure AsyncOS to connect to multiple LDAP servers. For more information, see Configuring AsyncOS to Work With Multiple LDAP Servers, on page 12.

Step 2 **Configure the LDAP queries**.

You can either use the default spam quarantine queries generated for the LDAP server profile or create your own queries that are tailored to your particular LDAP implementation and schema. You then designate the active queries for spam notifications and end-user access to the quarantine.

For information about queries, see Configuring LDAP Queries, on page 4.

Step 3 **Enable LDAP end-user access and spam notifications for the spam quarantine**.

Enable LDAP end-user access to the spam quarantine to allow end-users to view and manage messages in their quarantine. You can also enable alias consolidation for spam notifications to prevent the user from receiving multiple notifications.

For more information, see Setting Up the Centralized Spam Quarantine.

Creating the LDAP Server Profile

When you configure AsyncOS to use LDAP directories, you create an LDAP server profile to store the information about the LDAP server.

Procedure

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > LDAP**.

Step 3 Click **Add LDAP Server Profile.**

Step 4 Enter a name for the server profile in the **LDAP Server Profile Name** text field.

Step 5 Enter the host name for the LDAP server in the **Host Name(s)** text field.

You can enter multiple host names to configure the LDAP servers for failover or load-balancing. Separate multiple entries with commas. For more information, see Configuring AsyncOS to Work With Multiple LDAP Servers, on page 12.

Step 6 Select an authentication method. You can use anonymous authentication or specify a user name and passphrase.

Note
You need to configure LDAP authentication to view client user IDs instead of client IP addresses on reports. Without LDAP authentication the system can only refer to users by their IP address. Choose the **Use Passphrase** radio button, and enter the User name and passphrase. The user name will now be seen on the User Mail Summary page.

Step 7 Select the LDAP server type: Active Directory, OpenLDAP, or Unknown or Other.

Step 8 Enter a port number.

The default port is `3268`. This is the default port for Active Directory that enables it to access the global catalog in a multi-server environment.

Step 9 Enter a base DN (distinguishing name) for the LDAP server.

If you authenticate with a user name and a passphrase, the user name must include the full DN to the entry that contains the passphrase. For example, a user with an email address of `joe@example.com` is a user of the marketing group. The entry for this user would look like the following entry:

```
uid=joe, ou=marketing, dc=example dc=com
```

- [Optional - Only if "Validate LDAP Server Certificate" is enabled in LDAP Global Settings]: Check whether the Custom Certificate Authority is uploaded to validate the server certificate.
- To add the Certificate Authority, use certconfig > CERTAUTHORITY sub command in the CLI. [Optional - Only if "Validate LDAP Server Certificate" is enabled in LDAP Global Settings and FQDN validation enabled in SSL Configuration settings]: Check whether the 'Common Name,' 'SAN: DNS Name' fields, or both present in the server certificate, are in the FQDN format.
- [Optional - Only if "Validate LDAP Server Certificate" is enabled in LDAP Global Settings]: Check whether the 'Common Name,' or 'SAN: DNS Name' fields, of the server certificate contain Hostname of the server. Reverse DNS name is used if IP is configured in Hostname field.
- [Optional - Only if the 'Validate LDAP Server Certificate' is enabled in the LDAP Global Settings page and X 509 validation is enabled in the SSL Configuration settings page]: Check for the signature algorithm of the server certificate.
- [Optional - Only if the 'Validate LDAP Server Certificate' is enabled in the LDAP Global Settings page]: Check whether the server name is present in the 'Common Name' or 'SAN: DNS Name' fields in the server certificate.
- [Optional - Only if the 'Validate LDAP Server Certificate' is enabled in the LDAP Global Settings page]: Check the server certificate version.

  Note
  Only version 1 and version 3 server certificates are allowed.

Step 10 Under Advanced, select whether to use SSL when communicating with the LDAP server.

Step 11 Enter the cache time-to-live. This value represents the amount of time to retain caches.

Step 12 Enter the maximum number of retained cache entries.

Step 13 Enter a maximum number of simultaneous connections.

If you configure the LDAP server profile for load balancing, these connections are distributed among the listed LDAP servers. For example, if you configure 10 simultaneous connections and load balance the connections over three servers, AsyncOS creates 10 connections to each server, for a total of 30 connections. For more information, see Load Balancing, on page 13.

Note
The maximum number of simultaneous connections includes LDAP connections used for LDAP queries. However, if you enable LDAP authentication for the spam quarantine, the appliance allows 20 additional connections for the end user quarantine for a total of 30 connections.

Step 14 Test the connection to the server by clicking the Test Server(s) button. If you specified multiple LDAP servers, they are all tested. The results of the test appear in the Connection Status field. For more information, see Testing LDAP Servers, on page 4.

Step 15 Create spam quarantine queries by selecting the check box and completing the fields.

You can configure the quarantine end-user authentication query to validate users when they log in to the end-user quarantine. You can configure the alias consolidation query so that end-users do not receive quarantine notices for each email alias. To use these queries, select the "Designate as the active query" check box. For more information, see Configuring LDAP Queries, on page 4.

Step 16 Test the spam quarantine queries by clicking the Test Query button.

Enter the test parameters and click Run Test. The results of the test appear in the Connection Status field. If you make any changes to the query definition or attributes, click **Update**.

Note
If you have configured the LDAP server to allow binds with empty passphrases, the query can pass the test with an empty passphrase field.

Step 17 Submit and commit your changes.

Active Directory server configurations do not allow authentication through TLS with Windows 2000. This is a known issue with Active Directory. TLS authentication for Active Directory and Windows 2003 *does* work.

Note
Although the number of server configurations is unlimited, you can configure only one end-user authentication query and one alias consolidation query per server.

Testing LDAP Servers

Use the Test Server(s) button on the Add/Edit LDAP Server Profile page (or the test subcommand of the ldapconfig command in the CLI) to test the connection to the LDAP server. AsyncOS displays a message stating whether the connection to the server port succeeded or failed. If you configured multiple LDAP servers, AsyncOS tests each server and displays individual results.

Configuring LDAP Queries

The following sections provide the default query strings and configuration details for each type of spam quarantine query:

- **Spam quarantine end-user authentication query.** For more information, see the Spam Quarantine End-User Authentication Queries, on page 6.
- **Spam quarantine alias consolidation query.** For more information, see Spam Quarantine Alias Consolidation Queries, on page 7.

To have the quarantine use an LDAP query for end-user access or spam notifications, select the "Designate as the active query" check box. You can designate one end-user authentication query to control quarantine

access and one alias consolidation query for spam notifications. Any existing active queries are disabled. On the Security Management appliance, choose **Management Appliance > System Administration > LDAP** page, an asterisk (*) is displayed next to the active queries.

You can also specify a domain-based query or chain query as an active end-user access or spam notification query. For more information, see Domain-Based Queries, on page 9 and Chain Queries, on page 10.

Note Use the Test Query button on the LDAP page (or the **ldaptest** command) to verify that your queries return the expected results.

- LDAP Query Syntax, on page 5
- Tokens, on page 5

LDAP Query Syntax

Spaces are allowed in LDAP paths, and they do not need to be quoted. The CN and DC syntax is not case-sensitive.

Cn=First Last,oU=user,dc=domain,DC=COM

The variable names you enter for queries are case-sensitive and must match your LDAP implementation in order to work correctly. For example, entering **mailLocalAddress** at a prompt performs a different query than entering **maillocaladdress**.

Tokens

You can use the following tokens in your LDAP queries:

- {a} username@domainname
- {d} domain
- {dn} distinguished name
- {g} group name
- {u} user name
- {f} MAILFROM: address

Note The {f} token is valid in acceptance queries only.

For example, you might use the following query to accept mail for an Active Directory LDAP server:
(|(mail={a})(proxyAddresses=smtp:{a}))

Note We strongly recommend using the Test feature of the LDAP page (or the **test** subcommand of the **ldapconfig** command) to test all queries you construct and ensure that expected results are returned before you enable LDAP functionality on a listener. See the Testing LDAP Queries, on page 8 for more information.

Spam Quarantine End-User Authentication Queries

End-user authentication queries validate users when they log in to the spam quarantine. The token {u} specifies the user (it represents the user's login name). The token {a} specifies the user's email address. The LDAP query does not strip "SMTP:" from the email address; AsyncOS strips that portion of the address.

Based on the server type, AsyncOS uses one of the following default query strings for the end-user authentication query:

- **Active Directory:** (sAMAccountName={u})
- OpenLDAP: (uid={u})
- **Unknown or Other:** [Blank]

By default, the primary email attribute is **mail**. You can enter your own query and email attributes. To create the query in the CLI, use the isqauth subcommand of the **ldapconfig** command.

Note If you want users to log in with their full email addresses, use (mail=smtp:{a}) for the query string.

Sample Active Directory End-User Authentication Settings

This section shows sample settings for an Active Directory server and the end-user authentication query. This example uses passphrase authentication for the Active Directory server, the default query string for end-user authentication for Active Directory servers, and the mail and proxyAddresses email attributes.

Table 1: Example LDAP Server and Spam Quarantine End-User Authentication Settings: Active Directory

Authentication Method	Use Passphrase (Need to create a low-privilege user to bind for searching, or configure anonymous searching.)
Server Type	Active Directory
Port	3268
Base DN	[Blank]
Connection Protocol	[Blank]
Query String	(sAMAccountName={u})
Email Attribute(s)	mail,proxyAddresses

Sample OpenLDAP End-User Authentication Settings

This section shows sample settings for an OpenLDAP server and the end-user authentication query. This example uses anonymous authentication for the OpenLDAP server, the default query string for end-user authentication for OpenLDAP servers, and the mail and mailLocalAddress email attributes.

Table 2: Example LDAP Server and Spam Quarantine End-User Authentication Settings: OpenLDAP

Authentication Method	Anonymous
Server Type	OpenLDAP
Port	389
Base DN	[Blank] (Some older schemas will want to use a specific Base DN.)
Connection Protocol	[Blank]
Query String	(uid={u})
Email Attribute(s)	mail,mailLocalAddress

Spam Quarantine Alias Consolidation Queries

If you use spam notifications, the spam quarantine alias consolidation query consolidates the email aliases so that recipients do not receive quarantine notices for each alias. For example, a recipient might receive mail for the following email addresses: john@example.com, jsmith@example.com, and john.smith@example.com. When you use alias consolidation, the recipient receives a single spam notification at a chosen primary email address for messages sent to all of the user's aliases.

To consolidate messages to a primary email address, create a query to search for a recipient's alternate email aliases, and then enter the attribute for the recipient's primary email address in the Email Attribute field.

For Active Directory servers, the default query string (which may or may not be different for your deployment) is (|(proxyAddresses={a})(proxyAddresses=smtp:{a})) and the default email attribute is mail . For OpenLDAP servers, the default query string is (mail={a}) and the default email attribute is mail . You can define your own query and email attributes, including multiple attributes separated by commas. If you enter more than one email attribute, Cisco recommends entering a unique attribute that uses a single value, such as mail , as the first email attribute instead of an attribute with multiple values that can change, such as proxyAddresses .

To create the query in the CLI, use the isqalias subcommand of the ldapconfig command.

- Sample Active Directory Alias Consolidation Settings, on page 7
- Sample OpenLDAP Alias Consolidation Settings, on page 8

Sample Active Directory Alias Consolidation Settings

This section shows sample settings for an Active Directory server and the alias consolidation query. This example uses anonymous authentication for the Active Directory server, a query string for alias consolidation for Active Directory servers, and the mail email attribute.

Table 3: Example LDAP Server and Spam Quarantine Alias Consolidation Settings: Active Directory

Authentication Method	Anonymous
Server Type	Active Directory
Port	3268

Authentication Method	Anonymous
Base DN	[Blank]
Connection Protocol	Use SSL
Query String	(|(mail={a})(mail=smtp:{a}))
Email Attribute	mail

Sample OpenLDAP Alias Consolidation Settings

This section shows sample settings for an OpenLDAP server and the alias consolidation query. This example uses anonymous authentication for the OpenLDAP server, a query string for alias consolidation for OpenLDAP servers, and the mail email attribute.

Table 4: Example LDAP Server and Spam Quarantine Alias Consolidation Settings: OpenLDAP

Authentication Method	Anonymous
Server Type	OpenLDAP
Port	389
Base DN	[Blank] (Some older schemas will want to use a specific Base DN.)
Connection Protocol	Use SSL
Query String	(mail={a}))
Email Attribute	mail

Testing LDAP Queries

Use the Test Query button on the Add/Edit LDAP Server Profile page (or the ldaptest command in the CLI) to test your queries. AsyncOS displays details about each stage of the query connection test. For example, whether the first stage SMTP authorization succeeded or failed, and whether the BIND match returned a true or false result.

The ldaptest command is available as a batch command, for example:

ldaptest LDAP.isqalias foo@cisco.com

The variable names you enter for queries are *case-sensitive* and must match your LDAP implementation to work correctly. For example, entering mailLocalAddress for the email attribute performs a different query than entering maillocaladdress .

To test a query, you must enter the test parameters and click Run Test. The results appear in the Test Connection field. If an end-user authentication query succeeds, a result of "Success: Action: match positive" is displayed. For alias consolidation queries, a result of "Success: Action: alias consolidation" is displayed, along with the email address for the consolidated spam notifications. If a query fails, AsyncOS displays a reason for the failure, such as no matching LDAP records were found, or the matching record did not contain the email

attribute. If you use multiple LDAP servers, the Cisco Content Security appliance tests the query on each LDAP server.

Domain-Based Queries

Domain-based queries are LDAP queries that are grouped by type and associated with a domain. You might want to use domain-based queries if different LDAP servers are associated with different domains, but you need to run queries for all your LDAP servers for end-user quarantine access. For example, a company called Bigfish owns the domains Bigfish.com, Redfish.com, and Bluefish.com, and it maintains a different LDAP server for employees associated with each domain. Bigfish can use a domain-based query to authenticate end-users against the LDAP directories of all three domains.

To use a domain-based query to control end-user access or notifications for the spam quarantine, complete the following steps:

Procedure

Step 1 Create an LDAP server profile for each domain you want to use in the domain-based query. In each server profile, configure the queries you want to use in the domain-based query. For more information, see Creating the LDAP Server Profile, on page 2.

Step 2 Create the domain-based query. When you create the domain-based query, you select queries from each server profile, and designate the domain-based query as an active query for the spam quarantine. For more information about creating the query, see Creating a Domain-Based Query, on page 9.

Step 3 Enable end-user access or spam notifications for the spam quarantine. For more information, see Setting Up End-User Access to the Spam Quarantine via Web Browser.

Creating a Domain-Based Query

Procedure

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > LDAP**.

Step 3 On the LDAP page, click **Advanced**.

Step 4 Enter a name for the domain-based query.

Step 5 Select the query type.

Note
When you create a domain-based query, you specify a single query type. After you select a query type, the query field drop-down lists contain the appropriate queries from the LDAP server profiles.

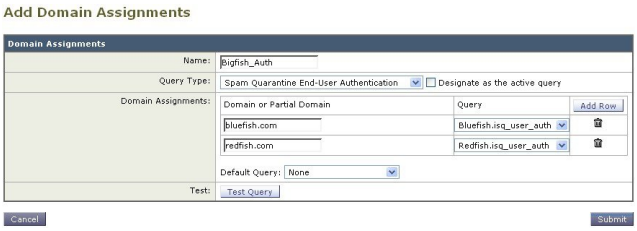
Step 6 In the Domain Assignments field, enter a domain.

Step 7 Select a query to associate with the domain.

Step 8 Add a row and select a query for each domain in the domain-based query.

Step 9 Enter a default query to run if all other queries fail. If you do not want to enter a default query, select **None**.

Figure 1: Example Domain-based Query



Step 10 Test the query by clicking the Test Query button and entering a user login and passphrase or an email address to test in the Test Parameters fields. The results appear in the Connection Status field.

Step 11 Check the **Designate as the active query** checkbox if you want the spam quarantine to use the domain-based query.

Note
The domain-based query becomes the active LDAP query for the specified query type. For example, if the domain-based query is used for end-user authentication, it becomes the active end-user authentication query for the spam quarantine.

Step 12 Click **Submit** and then click **Commit** to commit your changes.

Note
To do the same configuration on the command line interface, type the `advanced` subcommand of the `ldapconfig` command at the command line prompt.

Chain Queries

A chain query is a series of LDAP queries that AsyncOS runs in succession. AsyncOS runs each query in the series each query in the "chain" until the LDAP server returns a positive response or the final query returns a negative response or fails. Chain queries can be useful if entries in LDAP directories use different attributes to store similar (or the same) values. For example, departments in an organization might use different types of LDAP directories. The IT department might use OpenLDAP while the Sales department uses Active Directory. To ensure that queries run against both types of LDAP directories, you can use chain queries.

To use a chain query to control end-user access or notifications for the spam quarantine, complete the following steps:

Procedure

Step 1 Create an LDAP server profile for each query you want to use in the chain queries. For each of the server profiles, configure the queries you want to use for a chain query. For more information, see Creating the LDAP Server Profile, on page 2.

Step 2 Create the chain query and designate it as an active query for the spam quarantine. For more information, see Creating a Chain Query, on page 11.

Step 3 Enable LDAP end-user access or spam notifications for the spam quarantine. For more information about the spam quarantine, see Setting Up the Centralized Spam Quarantine.

Creating a Chain Query

Tip You can also use the advanced subcommand of the ldapconfig command in the CLI.

Procedure

Step 1 [New Web Interface Only] On the Security Management appliance, click to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > LDAP > LDAP Server**.

Step 3 From the LDAP Server Profiles page, click **Advanced**.

Step 4 Click **Add Chained Query**.

Step 5 Enter a name for the chain query.

Step 6 Select the query type.

When you create a chain query, all of its component queries have the same query type. After you select a query type, the query field drop-down lists display the appropriate queries from the LDAP.

Step 7 Select the first query in the chain.

The Cisco Content Security appliance runs the queries in the order you configure them. If you add multiple queries to the chain query, you might want to order them so that general queries follow granular queries.

Figure 2: Example Chain Query

Step 8 Test the query by clicking the Test Query button and entering a user login and passphrase or an email address in the Test Parameters fields. The results appear in the Connection Status field.

Step 9 Check the **Designate as the active quer**y check box if you want the spam quarantine to use the domain query.

Note
The chain query becomes the active LDAP query for the specified query type. For example, if the chain query is used for end-user authentication, it becomes the active end-user authentication query for the spam quarantine.

Step 10 Submit and commit your changes.

Note
To do the same configuration on the command line interface, type the `advanced` subcommand of the `ldapconfig` command at the command line prompt.

Configuring AsyncOS to Work With Multiple LDAP Servers

When you configure an LDAP server profile, you can configure the Cisco Content Security appliance to connect to a list of multiple LDAP servers. If you use multiple LDAP servers, they need to contain the same information, have the same structure, and use the same authentication information. Third-party products exist that can consolidate the records.

You configure the Cisco Content Security appliance to connect to redundant LDAP servers to use the following features:

- **Failover**. If the Cisco Content Security appliance cannot connect to an LDAP server, it connects to the next server in the list.
- **Load Balancing**. The Cisco Content Security appliance distributes connections across the list of LDAP servers when it performs LDAP queries.

You can configure redundant LDAP servers on the Management Appliance > System Administration > LDAP page or by using the CLI ldapconfig command.

Testing Servers and Queries

Use the Test Server(s) button on the Add (or Edit) LDAP Server Profile page (or the test subcommand in the CLI) to test the connection to an LDAP server. If you use multiple LDAP servers, AsyncOS tests each server and displays individual results for each server. AsyncOS will also test the query on each LDAP server and display the individual results.

Failover

To ensure an LDAP server is available to that resolve queries, you can configure the LDAP profile for failover. If the connection to the LDAP server fails, or the query returns an error for which it is appropriate to do so, the appliance attempts to query the next LDAP server specified in the list.

The Cisco Content Security appliance attempts to connect to the first server in the list of LDAP servers for a specified period of time. If the appliance cannot connect to the first LDAP server in the list, or the query returns an error, the appliance attempts to connect to the next LDAP server in the list. By default, the appliance always attempts to connect to the first server in the list, and it attempts to connect to each subsequent server in the order they are listed. To ensure that the Cisco Content Security appliance connects to the primary LDAP server by default, enter it as the first server in the list of LDAP servers.

Note Only attempts to query a specified LDAP server fail over. Attempts to query referral or continuation servers associated with the specified LDAP server do not fail over.

If the Cisco Content Security appliance connects to a second or subsequent LDAP server, it remains connected to that server for a specified period of time. At the end of this period, the appliance attempts to reconnect to the first server in the list.

Configuring the Cisco Content Security Appliance for LDAP Failover

Procedure

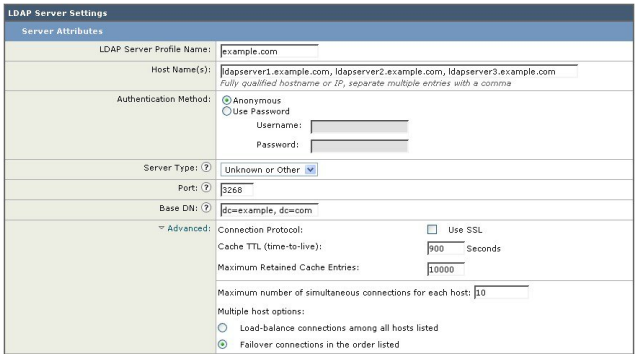
Step 1 [New Web Interface Only] On the Security Management appliance, click to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > LDAP**.

Step 3 Select the LDAP server profile you want to edit.

In the following example, the LDAP server name is example.com.

Figure 3: Example LDAP Failover Configuration



Step 4 In the Hostname text field, type the LDAP Servers; for example **ldapserver.example.com**.

Step 5 In the Maximum number of simultaneous connections for each host text field, type the maximum number of connections.

In this example the maximum number of connections is **10**.

Step 6 Click on the radio button next to **Failover connections in the order list**.

Step 7 Configure other LDAP options as necessary.

Step 8 Submit and commit the changes.

Load Balancing

To distribute LDAP connections among a group of LDAP servers, you can configure your LDAP profile for load balancing.

When you use load balancing, the Cisco Content Security appliance distributes connections among the LDAP servers listed. If a connection fails or times out, the appliance determines which LDAP servers are available and reconnects to available servers. The appliance determines the number of simultaneous connections to establish based on the maximum number of connections you configure.

If one of the listed LDAP servers does not respond, the appliance distributes the connection load among the remaining LDAP servers.

Configuring the Cisco Content Security Appliance for Load Balancing

Procedure

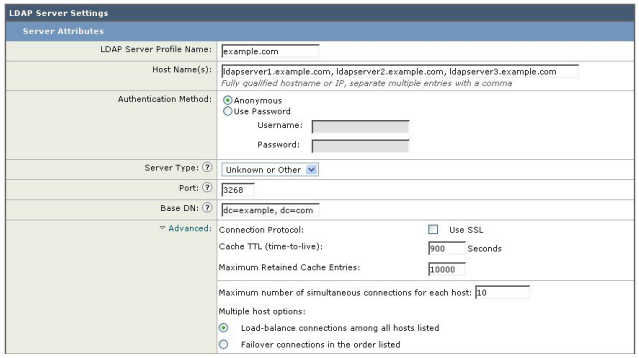
Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > LDAP**.

Step 3 Select the LDAP server profile you want to edit

In the following example, the LDAP server name is example.com.

Figure 4: Example Loadbalancing Configuration



Step 4 In the Hostname text field, type the LDAP Servers; for example **ldapserver.example.com**.

Step 5 In the Maximum number of simultaneous connections for each host text field, type the maximum number of connections.

In this example the maximum number of connections is **10**.

Step 6 Click on the radio button next to **Load balance connections among all hosts**.

Step 7 Configure other LDAP options as necessary.

Step 8 Submit and commit the changes.

Configuring External Authentication of Administrative Users Using LDAP

You can configure the Cisco Content Security appliance to use an LDAP directory on your network to authenticate administrative users by allowing them to log in to the appliance with their LDAP user names and passphrases.

Procedure

Step 1 **Configure the LDAP Server Profile.** See Creating the LDAP Server Profile, on page 2.

Step 2 **Create a query to find user accounts.** In an LDAP server profile, in the External Authentication Queries section, create a query to search for user accounts in the LDAP directory. See User Accounts Query for Authenticating Administrative Users , on page 15.

Step 3 **Create group membership queries.** Create a query to determine if a user is a member of a directory group, and create a separate query to find all members of a group. For more information, see Group Membership Queries for Authenticating Administrative Users , on page 16 and the documentation or online help for your Email Security appliance.

Note
Use the **Test Queries** button in the External Authentication Queries section of the page (or the ldaptest command) to verify that your queries return the expected results. For related information, see Testing LDAP Queries, on page 8.

Step 4 **Set up external authentication to use the LDAP server.** Enable the appliance to use the LDAP server for user authentication and assign user roles to the groups in the LDAP directory. For more information, see Enabling External Authentication of Administrative Users , on page 17 and the "Adding Users" in the documentation or online help for your Email Security appliance.

User Accounts Query for Authenticating Administrative Users

To authenticate external users, AsyncOS uses a query to search for the user record in the LDAP directory and the attribute that contains the user's full name. Depending on the server type you select, AsyncOS enters a default query and a default attribute. You can choose to have your appliance deny users with expired accounts if you have attributes defined in RFC 2307 in your LDAP user records (**shadowLastChange**, **shadowMax**, and **shadowExpire**). The base DN is required for the domain level where user records reside.

The following table shows the default query string and full user name attribute that AsyncOS uses when it searches for a user account on an Active Directory server.

Table 5: Default Query String for Active Directory Server

Server Type	Active Directory
Base DN	[blank] (You need to use a specific base DN to find the user records.)
Query String	(&(objectClass=user)(sAMAccountName={u}))
Attribute containing the user's full name	displayName

The following table shows the default query string and full user name attribute that AsyncOS uses when it searches for a user account on an OpenLDAP server.

Table 6: Default Query String for Open LDAP Server

Server Type	OpenLDAP
Base DN	[blank] (You need to use a specific base DN to find the user records.)
Query String	(&(objectClass=posixAccount)(uid={u}))
Attribute containing the user's full name	gecos

Group Membership Queries for Authenticating Administrative Users

You can associate LDAP groups with user roles for accessing the appliance.

AsyncOS also uses a query to determine if a user is a member of a directory group and a separate query to find all members of a group. Membership in a directory group membership determines the user's permissions within the system. When you enable external authentication on the Management Appliance > System Administration > Users page in the GUI (or userconfig in the CLI), you assign user roles to the groups in your LDAP directory. User roles determine the permissions that users have in the system, and for externally authenticated users, the roles are assigned to directory groups instead of individual users. For example, you can assign users in the IT directory group the Administrator role and users in the Support directory group to the Help Desk User role.

If a user belongs to multiple LDAP groups with different user roles, AsyncOS grants the user the permissions for the most restrictive role. For example, if a user belongs to a group with Operator permissions and a group with Help Desk User permissions, AsyncOS grants the user the permissions for the Help Desk User role.

When you configure the LDAP profile to query for group membership, enter the base DN for the directory level where group records can be found, the attribute that holds the group member's user name, and the attribute that contains the group name. Based on the server type that you select for your LDAP server profile, AsyncOS enters default values for the user name and group name attributes, as well default query strings.

Note For Active Directory servers, the default query string to determine if a user is a member of a group is (&(objectClass=group)(member={u})). However, if your LDAP schema uses distinguished names in the "memberof" list instead of user names, you can use {dn} instead of {u}.

The following table shows the default query strings and attributes that AsyncOS uses when it searches for group membership information on an Active Directory server.

Table 7: Default Query String and Attributes for Active Directory Server

Query String	Active Directory
Base DN	[blank] (You need to use a specific base DN to find the group records.)
Query string to determine if a user is a member of a group	(&(objectClass=group)(member={u})) **Note** If your LDAP schema uses distinguished names in the member of list instead of user names, you can replace {u} with {dn}
Query string to determine all members of a group	(&(objectClass=group)(cn={g}))
Attribute that holds each member's user name (or a DN for the user's record)	member
Attribute that contains the group name	cn

The following table shows the default query strings and attributes that AsyncOS uses when it searches for group membership information on an OpenLDAP server.

Table 8: Default Query String and Attributes for Open LDAP Server

Query String	OpenLDAP
Base DN	[blank] (You need to use a specific base DN to find the group records.)
Query string to determine if a user is a member of a group	(&(objectClass=posixGroup)(memberUid={u}))
Query string to determine all members of a group	(&(objectClass=posixGroup)(cn={g}))
Attribute that holds each member's user name (or a DN for the user's record)	memberUid
Attribute that contains the group name	cn

Enabling External Authentication of Administrative Users

After you configure the LDAP server profile and queries, you can enable external authentication using LDAP:

Procedure

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > Users** page.

Step 3 Click **Enable**.

Step 4 Select the **Enable External Authentication** check box.

Step 5 Select **LDAP** for the authentication type.

Step 6 Select the LDAP external authentication query that authenticates users.

Step 7 Enter the number of seconds that the appliance waits for a response from the server before timing out.

Step 8 Enter the name of a group from the LDAP directory that you want the appliance to authenticate, and select the role for the users in the group.

Step 9 Optionally, click **Add Row** to add another directory group. Repeat steps 7 and 8 for each directory group that the appliance authenticates.

Step 10 Submit and commit your changes.