LDAP Queries

This chapter contains the following sections:

Overview of LDAP Queries

It is recommended that you avoid changing LDAP settings on Cloud Email Security appliances .

If you store user information within LDAP directories in your network infrastructure — for example, in Microsoft Active Directory, SunONE Directory Server, or OpenLDAP directories — you can configure the appliance to query your LDAP servers to accept, route, and authenticate messages. You can configure the appliance to work with one or multiple LDAP servers.

The following section provides an overview on the types of LDAP queries you can perform; how LDAP works with the appliance to authenticate, accept, and route messages; and how to configure your appliance to work with LDAP.

Related Topics

- Understanding LDAP Queries, on page 2
- Understanding How LDAP Works with AsyncOS, on page 3
- Configuring the Cisco IronPort Appliance to Work with an LDAP Server, on page 4
- Creating LDAP Server Profiles to Store Information About the LDAP Server, on page 4
- Testing LDAP Servers, on page 6
- Enabling LDAP Queries to Run on a Particular Listener, on page 6
- Enhanced Support for Microsoft Exchange 5.5, on page 9

Understanding LDAP Queries

If you store user information within LDAP directories in your network infrastructure, you can configure the appliance to query your LDAP server for the following purposes:

- **Acceptance Queries**. You can use your existing LDAP infrastructure to define how the recipient email address of incoming messages (on a public listener) should be handled. For more information, see Using Acceptance Queries For Recipient Validation, on page 18.
- **Routing (Aliasing).** You can configure the appliance to route messages to the appropriate address and/or mail host based upon the information available in LDAP directories on your network. For more information, see Using Routing Queries to Send Mail to Multiple Target Addresses, on page 19.
- **Certificate Authentication.** You can create a query that checks the validity of a client certificate in order to authenticate an SMTP session between the user's mail client and the appliance . For more information, see Checking the Validity of a Client Certificate.
- **Masquerading**. You can masquerade Envelope Senders (for outgoing mail) and message headers (for incoming mail, such as To:, Reply To:, From: or CC:). For more information about masquerading, see Using Masquerading Queries to Rewrite the Envelope Sender, on page 20.
- **Group Queries**. You can configure the appliance to perform actions on messages based on the groups in the LDAP directory. You do this by associating a group query with a message filter. You can perform any message action available for message filters on messages that match the defined LDAP group. For more information, see Using Group LDAP Queries to Determine if a Recipient is a Group Member, on page 22.
- **Domain-based Queries**. You can create domain-based queries to allow the appliance to perform different queries for different domains on a single listener. When the appliance runs the domain-based queries, it determines the query to use based on the domain, and it queries the LDAP server associated with that domain.
- **Chain Queries.** You can create a chain query to enable the appliance to perform a series of queries in sequence. When you configure a chain query, the appliance runs each query in sequence until the LDAP appliance returns a positive result. For chained routing queries, the appliance re-runs the same configured chain query in sequence for each rewritten email address.
- **Directory Harvest Prevention**. You can configure the appliance to combat directory harvest attacks using your LDAP directories. You can configure directory harvest prevention during the SMTP conversation or within the work queue. If the recipient is not found in the LDAP directory, you can configure the system to perform a delayed bounce or drop the message entirely. Consequently, spammers are not able to differentiate between valid and invalid email addresses. See Using LDAP For Directory Harvest Attack Prevention, on page 27.
- **SMTP Authentication**. AsyncOS provides support for SMTP authentication. SMTP Auth is a mechanism for authenticating clients connected to an SMTP server. You can use this functionality to enable users at your organization to send mail using your mail servers even if they are connecting remotely (e.g. from

home or while traveling). For more information, see Configuring AsyncOS for SMTP Authentication, on page 30.

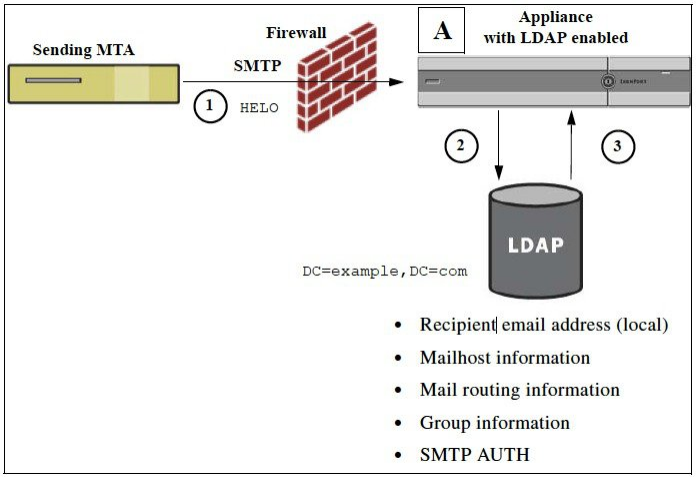
- **External Authentication**. You can configure your appliance to use your LDAP directory to authenticate users logging in to the appliance . For more information, see Configuring External LDAP Authentication for Users, on page 37.
- **Spam Quarantine End-User Authentication**. You can configure your appliance to validate users when they log in to the end-user quarantine. For more information, see Authenticating End-Users of the Spam Quarantine, on page 40.
- **Spam Quarantine Alias Consolidation**. If you use email notifications for spam, this query consolidates the end-user aliases so that end-users do not receive quarantine notices for each aliased email address. For more information, see Spam Quarantine Alias Consolidation Queries, on page 41.

Understanding How LDAP Works with AsyncOS

When you work with LDAP directories, the appliance can be used in conjunction with an LDAP directory server to accept recipients, route messages, and/or masquerade headers. LDAP group queries can also be used in conjunction with message filters to create rules for handling messages as they are received by the appliance .

The following figure demonstrates how the appliance works with LDAP:

Figure 1: LDAP Configuration



1. The sending MTA sends a message to the public listener “A” via SMTP.
2. The appliance queries the LDAP server defined via the **System Administration > LDAP** page (or by the global **`ldapconfig`** command).
3. Data is received from the LDAP directory, and, depending on the queries defined on the **System Administration > LDAP** page (or in the **`ldapconfig`** command) that are used by the listener:
   - the message is routed to the new recipient address, or dropped or bounced
   - the message is routed to the appropriate mailhost for the new recipient
   - From:, To:, and CC: message headers are re-written based upon the query
   - further actions as defined by **`rcpt-to-group`** or **`mail-from-group`** message filter rules (used in conjunction with configured group queries).

Note You can configure your appliance to connect to multiple LDAP servers. When you do this, you can configure the LDAP profile settings for load-balancing or failover. For more information about working with multiple LDAP servers, see Configuring AsyncOS To Work With Multiple LDAP Servers, on page 44.

Configuring the Cisco IronPort Appliance to Work with an LDAP Server

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

Step 1 **Configure LDAP server profiles**. The server profile contains information to enable AsyncOS to connect to the LDAP server (or servers), such as:

- the name of the server (s) and port to send queries,
- the base DN, and
- the authentication requirements for binding to the server

For more information about configuring a server profile, see Creating LDAP Server Profiles to Store Information About the LDAP Server, on page 4.

When you configure the LDAP server profile, you can configure AsyncOS to connect to one or multiple LDAP servers.

For information about configuring AsyncOS to connect to multiple servers, see Configuring AsyncOS To Work With Multiple LDAP Servers, on page 44.

Step 2 **Configure the LDAP query**. You configure the LDAP queries on the LDAP server profile. The query you configure should be tailored to your particular LDAP implementation and schema.

For information on the types of LDAP queries you can create, see Understanding LDAP Queries, on page 2.

For information on writing queries, see Working with LDAP Queries, on page 11.

Step 3 **Enable the LDAP server profile on a public listener or on a private listener**. You must enable the LDAP server profile on a listener to instruct the listener to run the LDAP query when accepting, routing, or sending a message.

For more information, see Enabling LDAP Queries to Run on a Particular Listener, on page 6.

Note When you configure a group query, you need to take additional steps to configure AsyncOS to work with the LDAP server. For information on configuring a group query, see Using Group LDAP Queries to Determine if a Recipient is a Group Member, on page 22. When you configure an end-user authentication or spam notification consolidation query, you must enable LDAP end-user access to the Spam Quarantine. For more information on the Spam Quarantine, see the Spam Quarantine chapter.

Creating LDAP Server Profiles to Store Information About the LDAP Server

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

Step 1 On the **System Administration > LDAP** page, click **Add LDAP Server Profile.**

Step 2 Enter a name for the server profile.

Step 3 Enter the host name for the LDAP server.

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 44.

Step 4 Select an authentication method. You can use anonymous authentication or specify a username and passphrase.

Step 5 Select the LDAP server type: Active Directory, OpenLDAP, or Unknown or Other.

Step 6 Enter a port number.

The default port is 3268 without SSL and 3269 with SSL for Active Directory or any Unknown / Other server types.

The default port is 389 without SSL and 636 with SSL, for Open LDAP server types.

Step 7 Enter a Base DN (distinguishing name) for the LDAP server.

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

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

Step 8 Select whether to use SSL when communicating with the LDAP server.

Step 9 Under Advanced, enter cache time-to-live. This value represents the amount of time to retain caches.

Step 10 Enter the maximum number of retained cache entries.

Note This cache is maintained per LDAP server. If you are configuring more than one LDAP servers, you must set a smaller LDAP cache value for better performance. Also, if the memory usage of various processes in the appliance is high, increasing this value may reduce the system performance.

Step 11 Enter the 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.

  Note The maximum number of simultaneous connections includes LDAP connections used for LDAP queries. However, the appliance may open more connections if you use LDAP authentication for the Spam Quarantine.

- You can configure the maximum time (in seconds) for which the connections to the LDAP server must persist before the connections reset. Choose a value between 60 and 86400.

Step 12 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 6.

Step 13 Create queries by marking the checkbox and completing the fields. You can select Accept, Routing, Masquerade, Group, SMTP Authentication, External Authentication, Spam Quarantine End-User Authentication, and Spam Quarantine Alias Consolidation.

Note To allow the appliance to run LDAP queries when you receive or send messages, you must enable the LDAP query on the appropriate listener. For more information, see Enabling LDAP Queries to Run on a Particular Listener, on page 6.

Step 14 Test a query 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**. For more information, see Testing LDAP Servers, on page 6.

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 15 Submit and commit your changes.

Note Although the number of server configurations is unlimited, you can configure only one recipient acceptance, one routing, one masquerading, and one group 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.

Enabling LDAP Queries to Run on a Particular Listener

To allow the appliance to run LDAP queries when you receive or send messages, you must enable the LDAP query on the appropriate listener.

Related Topics

- Configuring Global Settings for LDAP Queries, on page 6
- Example of Creating an LDAP Server Profile, on page 7
- Enabling LDAP Queries on a Public Listener, on page 8
- Enabling LDAP Queries on a Private Listener, on page 8

Configuring Global Settings for LDAP Queries

The LDAP global settings define how the appliance handles all LDAP traffic.

Step 1 On the **System Administration > LDAP** page, click **Edit Settings**.

Step 2 Select the IP interface to use for LDAP traffic. The appliance automatically chooses an interface by default.

Step 3 Select the TLS certificate to use for the LDAP interface (TLS certificates added via the **Network > Certificates** page or the `certconfig` command in the CLI are available in the list, see Overview of Encrypting Communication with Other MTAs).

Step 4 Select appropriate option, if you want to validate the LDAP server certificate.

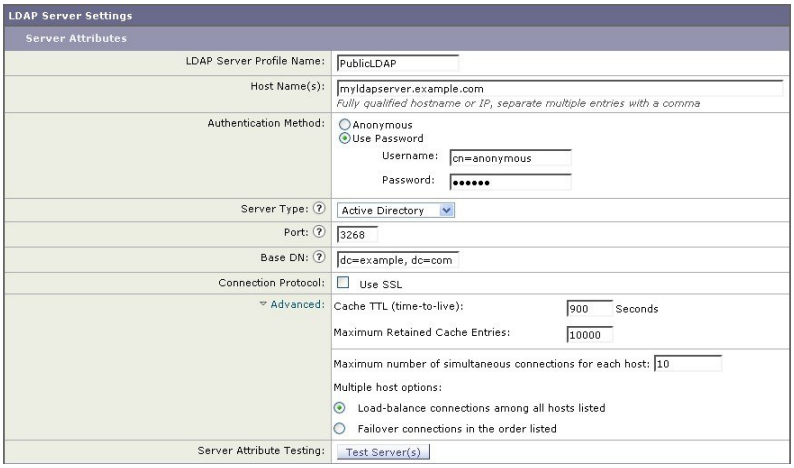
Step 5 Submit and commit your changes.

Example of Creating an LDAP Server Profile

In the following example, the System Administration > LDAP page is used to define an LDAP server for the appliance to bind to, and queries for recipient acceptance, routing, and masquerading are configured.

Note There is a 60 second connection attempt time-out for LDAP connections (which covers the DNS lookup, the connection itself, and, if applicable, the authentication bind for the appliance itself). After the first failure, AsyncOS immediately starts trying other hosts in the same server (if you specified more than one in the comma separated list). If you only have one host in the server, AsyncOS continues attempting to connect to it.

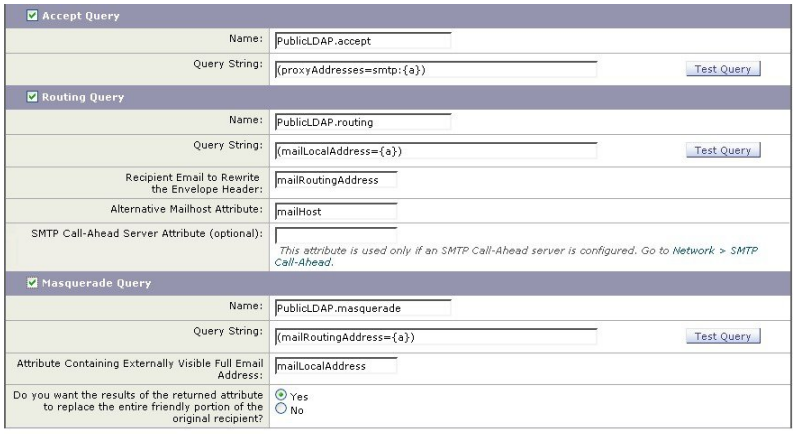
Figure 2: Configuring an LDAP Server Profile (1 of 2)



First, the nickname of "PublicLDAP" is given for the myldapserver.example.com LDAP server. The number of connections is set to 10 (the default), and the multiple LDAP server (hosts) load balance option is left as the default. You can specify multiple hosts here by providing a comma separated list of names. Queries are directed to port 3268 (the default). SSL is not enabled as the connection protocol for this host. The base DN of example.com is defined (dc=example,dc=com). The cache time-to-live is set to 900 seconds, the maximum number of cache entries is 10000, and the authentication method is set to passphrase.

Queries for recipient acceptance, mail routing, and masquerading are defined. Remember that query names are case-sensitive and must match exactly in order to return the proper results.

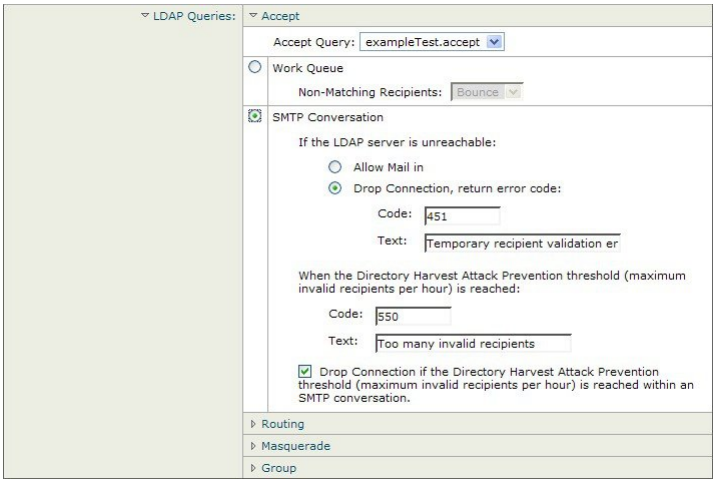
Figure 3: Configuring an LDAP Server Profile (2 of 2)



Enabling LDAP Queries on a Public Listener

In this example, the public listener “InboundMail” is updated to use LDAP queries for recipient acceptance. Further, recipient acceptance is configured to happen during the SMTP conversation (for more information, see Using Acceptance Queries For Recipient Validation, on page 18 for more information).

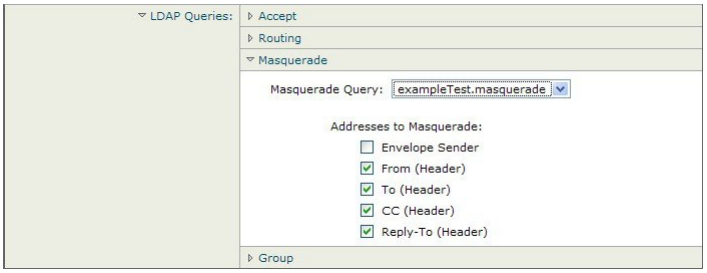
Figure 4: Enabling Acceptance and Routing Queries on a Listener



Enabling LDAP Queries on a Private Listener

In this example, the private listener “OutboundMail” is updated to use LDAP queries for masquerading. The masqueraded fields include: From, To, CC, and Reply-To.

Figure 5: Enabling a Masquerading Query on a Listener



Enhanced Support for Microsoft Exchange 5.5

AsyncOS includes a configuration option to provide support for Microsoft Exchange 5.5. If you use a later version of Microsoft Exchange, you do not need to enable this option. When configuring an LDAP server, you can elect to enable Microsoft Exchange 5.5 support by answering "y" when prompted in the `ldapconfig -> edit -> server -> compatibility` subcommand (this is only available via the CLI):

```
mail3.example.com> ldapconfig

Current LDAP server configurations:

1. PublicLDAP: (ldapexample.com:389)


Choose the operation you want to perform:

- NEW - Create a new server configuration.

- EDIT - Modify a server configuration.

- DELETE - Remove a server configuration.


[]> edit

Enter the name or number of the server configuration you wish to edit.

[]> 1

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

Choose the operation you want to perform:

- SERVER - Change the server for the query.

- LDAPACCEPT - Configure whether a recipient address should be accepted or
bounced/dropped.

- LDAPROUTING - Configure message routing.

- MASQUERADE - Configure domain masquerading.
```

```
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.

- SMTPAUTH - Configure SMTP authentication.

[]> server

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com


Microsoft Exchange 5.5 Compatibility Mode: Disabled

Choose the operation you want to perform:

- NAME - Change the name of this configuration.

- HOSTNAME - Change the hostname used for this query.

- PORT - Configure the port.

- AUTHTYPE - Choose the authentication type.

- BASE - Configure the query base.

- COMPATIBILITY - Set LDAP protocol compatibility options.

[]> compatibility
Would you like to enable Microsoft Exchange 5.5 LDAP compatibility mode? (This is not
recommended for versions of Microsoft Exchange later than 5.5, or other LDAP servers.)


[N]> y

Do you want to configure advanced LDAP compatibility settings? (Typically not required)

[N]>

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

Microsoft Exchange 5.5 Compatibility Mode: Enabled (attribute "objectClass")

Choose the operation you want to perform:

- NAME - Change the name of this configuration.

- HOSTNAME - Change the hostname used for this query.

- PORT - Configure the port.

- AUTHTYPE - Choose the authentication type.

- BASE - Configure the query base.
```

```
- COMPATIBILITY - Set LDAP protocol compatibility options.

[]>
```

Working with LDAP Queries

You create an entry in the LDAP server profile for each type of LDAP query you want to perform. When you create LDAP queries, you must enter the query syntax for your LDAP server. Please note that the queries you construct should be tailored and specific to your particular implementation of LDAP directory services, particularly if you have extended your directory with new object classes and attributes to accommodate the unique needs of your directory.

Related Topics

- Types of LDAP Queries, on page 11
- Base Distinguishing Name (DN), on page 12
- LDAP Query Syntax, on page 12
- Secure LDAP (SSL), on page 13
- Routing Queries, on page 13
- Allowing Clients to Bind to the LDAP Server Anonymously , on page 13
- Testing LDAP Queries, on page 16
- Troubleshooting Connections to LDAP Servers, on page 17

Types of LDAP Queries

- **Acceptance queries**. For more information, see Using Acceptance Queries For Recipient Validation, on page 18.
- **Routing queries**. For more information, see Using Routing Queries to Send Mail to Multiple Target Addresses, on page 19.
- **Certificate Authentication queries.** For more information, see Checking the Validity of a Client Certificate.
- **Masquerading queries**. For more information, see Using Masquerading Queries to Rewrite the Envelope Sender, on page 20.
- **Group queries**. For more information, see Using Group LDAP Queries to Determine if a Recipient is a Group Member, on page 22.
- **Domain-based queries**. For more information, see Using Domain-based Queries to Route to a Particular Domain, on page 25.
- **Chain queries**. For more information, see Using Chain Queries to Perform a Series of LDAP Queries, on page 26.

You can also configure queries for the following purposes:

- **Directory harvest prevention**. For more information, see Understanding LDAP Queries, on page 2.
- **SMTP authentication.** For more information, see Configuring AsyncOS for SMTP Authentication, on page 30.
- **External authentication**. For more information, Configuring External LDAP Authentication for Users, on page 37.
- **Spam quarantine end-user authentication query.** For more information, see Authenticating End-Users of the Spam Quarantine, on page 40.

- **Spam quarantine alias consolidation query.** For more information, see Spam Quarantine Alias Consolidation Queries, on page 41.

The search queries you specify are available to all listeners you configure on the system.

Base Distinguishing Name (DN)

The root level of the directory is called the base. The name of the base is the DN (distinguishing name). The base DN format for Active Directory (and the standard as per RFC 2247) has the DNS domain translated into domain components (dc=). For example, example.com's base DN would be: dc=example, dc=com. Note that each portion of the DNS name is represented in order. This may or may not reflect the LDAP settings for your configuration.

If your directory contains multiple domains you may find it inconvenient to enter a single BASE for your queries. In this case, when configuring the LDAP server settings, set the base to NONE. This will, however, make your searches inefficient.

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**.

Related Topics

- Tokens:, on page 12

Tokens:

You can use the following tokens in your LDAP queries:

- {a} username@domainname
- {d} domainname
- {dn} distinguished name
- {g} groupname
- {u} username
- {f} MAIL FROM: 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 Cisco Systems strongly recommends 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 Testing LDAP Queries, on page 16 for more information.

Secure LDAP (SSL)

You can use instruct AsyncOS to use SSL when communicating with the LDAP server. If you configure your LDAP server profile to use SSL:

- AsyncOS will use the LDAPS certificate configured via certconfig in the CLI (see Creating a Self-Signed Certificate).

  You may have to configure your LDAP server to support using the LDAPS certificate.
- If an LDAPS certificate has not been configured, AsyncOS will use the demo certificate.

Routing Queries

There is no recursion limit for LDAP routing queries; the routing is completely data driven. However, AsyncOS does check for circular reference data to prevent the routing from looping infinitely.

Allowing Clients to Bind to the LDAP Server Anonymously

You may need to configure your LDAP directory server to allow for anonymous queries. (That is, clients can bind to the server anonymously and perform queries.) For specific instructions on configuring Active Directory to allow anonymous queries, see the "Microsoft Knowledge Base Article - 320528" at the following URL:

```
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B320528
```

Alternately, you can configure one "user" dedicated solely for the purposes of authenticating and performing queries instead of opening up your LDAP directory server for anonymous queries from any client.

A summary of the steps is included here, specifically:

- How to set up Microsoft Exchange 2000 server to allow "anonymous" authentication.
- How to set up Microsoft Exchange 2000 server to allow "anonymous bind."
- How to set up AsyncOS to retrieve LDAP data from a Microsoft Exchange 2000 server using both "anonymous bind" and "anonymous" authentication.

Specific permissions must be made to a Microsoft Exchange 2000 server in order to allow "anonymous" or "anonymous bind" authentication for the purpose of querying user email addresses. This can be very useful when an LDAP query is used to determine the validity of an income email message to the SMTP gateway.

Related Topics

- Anonymous Authentication Setup, on page 14
- Anonymous Bind Setup for Active Directory, on page 15
- Notes for Active Directory Implementations, on page 16

Anonymous Authentication Setup

The following setup instructions allow you to make specific data available to unauthenticated queries of Active Directory and Exchange 2000 servers in the Microsoft Windows Active Directory. If you wish to allow "anonymous bind" to the Active Directory, see Anonymous Bind Setup for Active Directory, on page 15.

Step 1 Determine required Active Directory permissions.

Using the ADSI Edit snap-in or the LDP utility, you must modify the permissions to the attributes of the following Active Directory objects:

- The root of the domain naming context for the domain against which you want to make queries.
- All OU and CN objects that contain users against which you wish to query email information.

The following table shows the required permissions to be applied to all of the needed containers.

User Object	Permissions	Inheritance	Permission Type
Everyone	List Contents	Container Objects	Object
Everyone	List Contents	Organizational Unit Objects	Object
Everyone	Read Public Information	User Objects	Property
Everyone	Read Phone and Mail Options	User Objects	Property

Step 2 Set Active Directory Permissions

- Open ADSIEdit form the Windows 2000 Support Tools.
- Locate the **Domain Naming Context** folder. This folder has the LDAP path of your domain.
- Right click the **Domain Naming Context** folder, and then click **Properties**.
- Click **Security**.
- Click **Advanced**.
- Click **Add**.
- Click the **User Object** Everyone, and then click **OK**.
- Click the **Permission Type** tab.
- Click **Inheritance** from the **Apply onto** box.
- Click to select the Allow check box for the **Permission** permission.

Step 3 Configure the Cisco Messaging Gateway

Use `ldapconfig` on the Command Line Interface (CLI) to create an LDAP server entry with the following information.

- Hostname of an Active Directory or Exchange server
- Port 3268
- Base DN matching the root naming context of the domain
- Authentication type Anonymous

Anonymous Bind Setup for Active Directory

The following setup instructions allow you to make specific data available to anonymous bind queries of Active Directory and Exchange 2000 servers in the Microsoft Windows Active Directory. Anonymous bind of an Active Directory server will send the username anonymous with a blank passphrase.

Note If a passphrase is sent to an Active Directory server while attempting anonymous bind, authentication may fail.

Step 1 Determine required Active Directory permissions.

Using the ADSI Edit snap-in or the LDP utility, you must modify the permissions to the attributes of the following Active Directory objects.

- The root of the domain naming context for the domain against which you want to make queries.
- All OU and CN objects that contain users against which you wish to query email information.

The following table shows the required permissions to be applied to all of the needed containers.

User Object	Permissions	Inheritance	Permission Type
ANONYMOUS LOGON	List Contents	Container Objects	Object
ANONYMOUS LOGON	List Contents	Organizational Unit Objects	Object
ANONYMOUS LOGON	Read Public Information	User Objects	Property
ANONYMOUS LOGON	Read Phone and Mail Options	User Objects	Property

Step 2 Set Active Directory Permissions

- Open ADSIEdit form the Windows 2000 Support Tools.
- Locate the **Domain Naming Context** folder. This folder has the LDAP path of your domain.
- Right click the **Domain Naming Context** folder, and then click **Properties**.
- Click **Security**.
- Click **Advanced**.
- Click **Add**.
- Click the **User Object** ANONYMOUS LOGON, and then click **OK**.
- Click the **Permission Type** tab.
- Click **Inheritance** from the **Apply** onto box.
- Click to select the **Allow** check box for the **Permission** permission.

Step 3 Configure the Cisco Messaging Gateway

Use the **System Administration** > **LDAP** page (or `ldapconfig` in the CLI) to create an LDAP server entry with the following information.

- Hostname of an Active Directory or Exchange server
- Port 3268
- Base DN matching the root naming context of the domain

- Authentication type passphrase based using cn=anonymous as the user with a blank passphrase

Notes for Active Directory Implementations

- Active Directory servers accept LDAP connections on ports 3268 and 389. The default port for accessing the global catalog is port 3268.
- Active Directory servers accept LDAPS connections on ports 636 and 3269. Microsoft supports LDAPS on Windows Server 2003 and higher.
- The appliance should connect to a domain controller that is also a global catalog so that you can perform queries to different bases using the same server.
- Within Active Directory, you may need to grant read permissions to the group "Everyone" to directory objects to yield successful queries. This includes the root of the domain naming context.
- Generally, the value of the mail attribute entry in many Active Directory implementations has a matching value "ProxyAddresses" attribute entry.
- Microsoft Exchange environments that are aware of each other within the infrastructure can usually route mail between each other without involving a route back to the originating MTA.

Testing LDAP Queries

Use the Test Query button on the Add/Edit LDAP Server Profile page (or the `test` sub command in the CLI) of each query type to test the query to the LDAP server you configured. In addition to displaying the result, AsyncOS also displays the details on each stage of the query connection test. You can test each of the query types.

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

```
ldaptest LDAP.ldapaccept foo@ironport.com
```

If you entered multiple hosts in the Host Name field of the LDAP server attributes, the appliance tests the query on each LDAP server.

Table 1: Testing LDAP Queries

Query type	If a recipient matches (PASS)...	If a recipient does not match (FAIL)...
Recipient Acceptance (Accept, `ldapaccept`)	Accept the message.	Invalid Recipient: Conversation or delayed bounce or drop the message per listener settings. DHAP: Drop.
Routing (Routing, `ldaprouting`)	Route based on the query settings.	Continue processing the message.
Masquerade (Masquerade, `masquerade`)	Alter the headers with the variable mappings defined by the query.	Continue processing the message.
Group Membership (Group, `ldapgroup`)	Return "true" for message filter rules.	Return "false" for message filter rules.

Query type	If a recipient matches (PASS)...	If a recipient does not match (FAIL)...
SMTP Auth (SMTP Authentication, `smtpauth`)	A passphrase is returned from the LDAP server and is used for authentication; SMTP Authentication occurs.	No passphrase match can occur; SMTP Authentication attempts fail.
External Authentication (`externalauth`)	Individually returns a “match positive” for the bind, the user record, and the user’s group membership.	Individually returns a “match negative” for the bind, the user record, and the user’s group membership.
Spam Quarantine End-User Authentication (`isqauth`)	Returns a “match positive” for the end-user account.	No passphrase match can occur; End-User Authentication attempts fail.
Spam Quarantine Alias Consolidation (`isqalias`)	Returns the email address that the consolidated spam notifications will be sent to.	No consolidation of spam notifications can occur.

Note 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`**. Cisco Systems strongly recommends using the test subcommand of the ldapconfig command to test all queries you construct and ensure the proper results are returned.

Troubleshooting Connections to LDAP Servers

If the LDAP server is unreachable by the appliance, one of the following errors will be shown:

- `Error: LDAP authentication failed: <LDAP Error "invalidCredentials" [0x31]>`
- `Error: Server unreachable: unable to connect`
- `Error: Server unreachable: DNS lookup failure`

Note that a server may be unreachable because the wrong port was entered in the server configuration, or the port is not opened in the firewall. LDAP servers typically communicate over port 3268 or 389. Active Directory uses port 3268 to access the global catalog used in multi-server environments (See the “Firewall Information” appendix for more information.) In AsyncOS 4.0, the ability to communicate to the LDAP server via SSL (usually over port 636) was added. For more information, see Secure LDAP (SSL), on page 13.

A server may also be unreachable because the hostname you entered cannot be resolved.

You can use the Test Server(s) 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. For more information, see Testing LDAP Servers, on page 6.

If the LDAP server is unreachable:

- If LDAP Accept or Masquerading or Routing is enabled on the work queue, mail will remain within the work queue.
- If LDAP Accept is not enabled but other queries (group policy checks, etc.) are used in filters, the filters evaluate to false.

Using Acceptance Queries For Recipient Validation

You can use your existing LDAP infrastructure to define how the recipient email address of incoming messages (on an public listener) should be handled. Changes to user data in your directories are updated the next time the appliance queries the directory server. You can specify the size of the caches and the amount of time the appliance stores the data it retrieves.

Note You may wish to bypass LDAP acceptance queries for special recipients (such as administrator@example.com). You can configure this setting from the Recipient Access Table (RAT). For information about configuring this setting, see the "Configuring the Gateway to Receive Email" chapter.

Related Topics

- Sample Acceptance Queries, on page 18
- Configuring Acceptance Queries for Lotus Notes, on page 19

Sample Acceptance Queries

The following table shows sample acceptance queries.

Table 2: Example LDAP Query Strings for Common LDAP Implementations: Acceptance

Query for:	Recipient validation

OpenLDAP	`(mailLocalAddress={a})`
	`(mail={a})`
	`(mailAlternateAddress={a})`

Microsoft Active Directory Address Book **Microsoft Exchange**	`(|(mail={a})(proxyAddresses=smtp:{a}))`

SunONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

Lotus NotesLotus Domino	`(|(|(mail={a})(uid={u}))(cn={u}))` `(|(ShortName={u})(InternetAddress={a})(FullName={u}))`

You can also validate on the username (Left Hand Side). This is useful if your directory does not contain all the domains you accept mail for. Set the Accept query to (uid={u}).

Configuring Acceptance Queries for Lotus Notes

Note that there is a potential complication with LDAPACCEPT and Lotus Notes. If Notes LDAP contains a person with attributes like these:

```
mail=juser@example.com

cn=Joe User

uid=juser

cn=123456

location=New Jersey
```

Lotus accepts email for this person for various different forms of email addresses, other than what is specified, such as "Joe_User@example.com" — which do not exist in the LDAP directory. So AsyncOS may not be able to find all of the valid user email addresses for that user.

One possible solution is to try to publish the other forms of addresses. Please contact your Lotus Notes administrator for more details.

Using Routing Queries to Send Mail to Multiple Target Addresses

AsyncOS supports alias expansion (LDAP routing with multiple target addresses). AsyncOS replaces the original email message with a new, separate message for each alias target (for example, recipient@yoursite.com might be replaced with new separate messages to newrecipient1@hotmail.com and recipient2@internal.yourcompany.com, etc.). Routing queries are sometimes known as aliasing queries on other mail processing systems.

Related Topics

- Sample Routing Queries, on page 19

Sample Routing Queries

Table 3: Example LDAP Query Strings for Common LDAP Implementations: Routing

Query for:	Route to another mailhost
OpenLDAP	`(mailLocalAddress={a})`
Microsoft Active Directory Address Book **Microsoft Exchange**	May not be applicable

Query for:	Route to another mailhost

SunONE Directory Server	`(mail={a})`
	`(mailForwardingAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailRoutingAddress={a})`
	`(otherMailbox={a})`
	`(rfc822Mailbox={a})`

a. Active Directory implementations can have multiple entries for the `proxyAddresses` attribute, but because AD formats this attribute value as `smtp:user@domain.com`, that data cannot be used for LDAP routing/alias expansion. Each target address must be in a separate `attribute:value` pair. Microsoft Exchange environments that are aware of each other within the infrastructure can usually route mail between each other without involving a route back to the originating MTA.

Related Topics

- Routing: MAILHOST and MAILROUTINGADDRESS, on page 20

Routing: MAILHOST and MAILROUTINGADDRESS

For Routing queries, the value of MAILHOST cannot be an IP address; it must be a resolvable hostname. This usually requires the use of an Internal DNSconfig.

MAILHOST is optional for the routing query. MAILROUTINGADDRESS is mandatory if MAILHOST is not set.

Using Masquerading Queries to Rewrite the Envelope Sender

Masquerading is a feature that rewrites the Envelope Sender (also known as the sender, or MAIL FROM) and the To:, From:, and/or CC: headers on email based on queries you construct. A typical example implementation of this feature is “Virtual Domains,” which allows you to host multiple domains from a single site. Another typical implementation is “hiding” your network infrastructure by “stripping” the subdomains from strings in email headers.

Related Topics

- Sample Masquerading Queries , on page 20
- Masquerading “Friendly Names”, on page 21

Sample Masquerading Queries

Table 4: Example LDAP Query Strings for Common LDAP Implementation: Masquerading

Query for:	Masquerade
OpenLDAP	`(mailRoutingAddress={a})`
Microsoft Active Directory Address Book	`(proxyaddresses=smtp:{a})`

Query for:	Masquerade

SunONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

Masquerading "Friendly Names"

In some user environments, an LDAP directory server schema may store a "friendly name" in addition to a mail routing address or a local mail address. AsyncOS allows you to masquerade Envelope Senders (for outgoing mail) and message headers (for incoming mail, such as To:, Reply To:, From: or CC:) with this "friendly address" — even if the friendly address contains special characters that are not normally permitted in a valid email address (for example, quotation marks, spaces, and commas).

When using masquerading of headers via an LDAP query, you now have the option to configure whether to replace the entire friendly email string with the results from the LDAP server. Note that even with this behavior enabled, only the user@domain portion will be used for the Envelope Sender (the friendly name is illegal).

As with the normal LDAP masquerading, if empty results (zero length or entire white space) are returned from the LDAP query, no masquerading occurs.

To enable this feature, answer "y" to the following question when configuring an LDAP-based masquerading query for a listener (LDAP page or `ldapconfig` command):

```
Do you want the results of the returned attribute to replace the entire
friendly portion of the original recipient? [N]
```

For example, consider the following example LDAP entry:

Attribute	Value
mailRoutingAddress	admin\@example.com
mailLocalAddress	joe.smith\@example.com
mailFriendlyAddress	"Administrator for example.com," <joe.smith\@example.com>

If this feature is enabled, an LDAP query of (mailRoutingAddress={a}) and a masquerading attribute of (mailLocalAddress) would result in the following substitutions:

Original Address (From, To, CC, Reply-to)	Masqueraded Headers	Masqueraded Envelope Sender
admin@example.com	From: "Administrator for example.com," <joe.smith@example.com>	MAIL FROM: <joe.smith@example.com>

Using Group LDAP Queries to Determine if a Recipient is a Group Member

You can define a query to your LDAP servers to determine if a recipient is a member of a group as defined by your LDAP directory.

Step 1 Create a message filter that uses a rcpt-to-group or mail-from-group rule to act upon the message.

Step 2 Then, use the **System Administration** > **LDAP** page (or the **`ldapconfig`** command) to define the LDAP server for the appliance to bind to and configure a query for a group membership.

Step 3 Use the **Network** > **Listeners** page (or the **`listenerconfig -> edit -> ldapgroup`** subcommand) to enable the group query for the listener.

What to do next

Related Topics

- Sample Group Queries , on page 22
- Configuring a Group Query, on page 22

Sample Group Queries

Table 5: Example LDAP Query Strings for Common LDAP Implementation: Group

Query for:	Group
OpenLDAP	OpenLDAP does not support the memberOf attribute by default. Your LDAP Administrator may add this attribute or a similar attribute to the schema.
Microsoft Active Directory	`(&(memberOf={g})(proxyAddresses=smtp:{a}))`
SunONE Directory Server	`(&(memberOf={g})(mailLocalAddress={a}))`

For example, suppose that your LDAP directory classifies members of the “Marketing” group as ou=Marketing . You can use this classification to treat messages sent to or from members of this group in a special way. Step 1 creates a message filter to act upon the message, and Steps 2 and 3 enable the LDAP lookup mechanism.

Configuring a Group Query

In the following example, mail from members of the Marketing group (as defined by the LDAP group “Marketing”) will be delivered to the alternate delivery host `marketingfolks.example.com` .

Step 1 First, a message filter is created to act upon messages that match positively for group membership. In this example, a filter is created that uses the `mail-from-group` rule. All messages whose Envelope Sender is found to be in the LDAP group "marketing-group1" will be delivered with an alternate delivery host (the filters `alt-mailhost` action).

The group membership field variable (groupName) will be defined in step 2. The group attribute "groupName" is defined with the value `marketing-group1` .

```
mail3.example.com> filters


Choose the operation you want to perform:

- NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.

MarketingGroupfilter:

if (mail-from-group == "marketing-group1") {

alt-mailhost ('marketingfolks.example.com');}

.

1 filters added.

Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]>
```

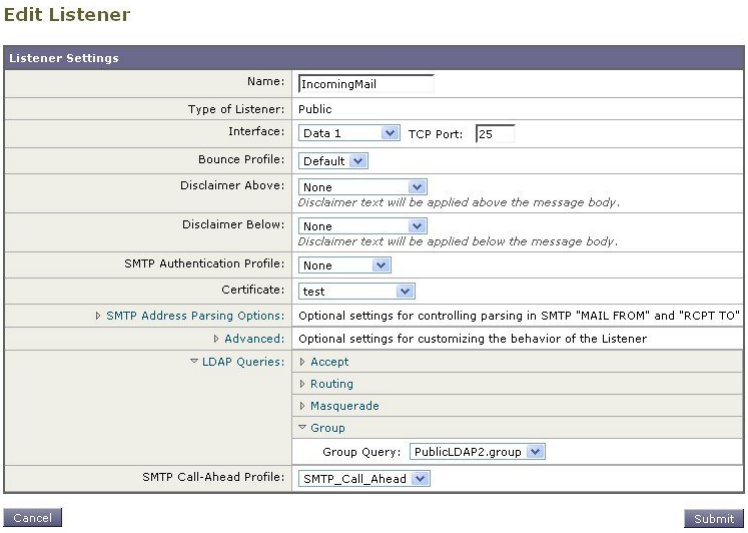
For more information on the `mail-from-group` and `rcpt-to-group` message filter rules, see Message Filter Rules.

Step 2 Next, the Add LDAP Server Profile page is used to define an LDAP server for the appliance to bind to, and an initial query for a group membership is configured.

Step 3 Next, the public listener "InboundMail" is updated to use LDAP queries for group routing. The Edit Listener page is used to enable the LDAP query specified above.

As a result of this query, messages accepted by the listener trigger a query to the LDAP server to determine group membership. The PublicLDAP2.group query was defined previously via the **System Administration > LDAP** page.

Figure 6: Specifying a Group Query on a Listener



Step 4 Submit and commit your changes.

Example: Using a Group Query to Skip Spam and Virus Checking

Because message filters occurs early in the pipeline, you can use a group query to skip virus and spam checking for specified groups. For example, you want your IT group to receive all messages and to skip spam and virus checking. In your LDAP record, you create a group entry that uses the DN as the group name. The group name consists of the following DN entry:

cn=IT, ou=groups, o=sample.com

You create an LDAP server profile with the following group query:

(&(memberOf={g})(proxyAddresses=smtp:{a}))

You then enable this query on a listener so that when a message is received by the listener, the group query is triggered.

To skip virus and spam filtering for members of the IT group, you create the following message filter to check incoming messages against LDAP groups.

```
[]> - NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.

IT_Group_Filter:

if (rcpt-to-group == "cn=IT, ou=groups, o=sample.com"){
```

```
skip-spamcheck();

skip-viruscheck();

deliver();

}

.
1 filters added.
```

Note The rcpt-to-group in this message filter reflects the DN entered as the group name: cn=IT, ou=groups, o=sample.com. Verify that you use the correct group name in the message filter to ensure that your filter matches the name in your LDAP directory.

Messages accepted by the listener trigger a query to the LDAP server to determine group membership. If the message recipient is a member of the IT group, the message filter skips both virus and spam checking and delivers the message to the recipient. To enable the filter to check the results of the LDAP query, you must create the LDAP query on the LDAP server and enable the LDAP query on a listener.

Using Domain-based Queries to Route to a Particular Domain

Domain-based queries are LDAP queries grouped by type, associated with a domain, and assigned to a particular listener. You might want to use domain-based queries if you have different LDAP servers associated with different domains but you want to run queries for all your LDAP servers on the same listener. For example, the company "MyCompany" purchases company "HisCompany" and company "HerCompany" MyCompany maintains its domain, MyCompany.example.com as well as domains for HisCompany.example.com and HerCompany.example.com, and it maintains a different LDAP server for employees associated with each domain. To accept mail for all three of these domains, MyCompany creates domain-based queries. This allows MyCompany.example.com to accept emails for Mycompany.example.com, HisCompany.example.com, and HerCompany.example.com on the same listener.

Step 1 Create a server profile for each of the domains you want to use in the domain-based queries. For each of the server profiles, configure the queries you want to use for a domain-based query (acceptance, routing, etc.). For more information, see Creating LDAP Server Profiles to Store Information About the LDAP Server, on page 4.

Step 2 Create the domain-based query. When you create the domain-based query, you select queries from each server profile, and enable the appliance to determine which query to run based on the domain in the Envelope To field. For more information about creating the query, see Creating a Domain-Based Query, on page 26.

Step 3 Enable the domain-based query on the public or private listener. For more information about configuring listeners, see the "Configuring the Gateway to Receive Mail" chapter.

Note You can also enable domain-based queries for LDAP end-user access or spam notifications for the Spam Quarantine. For more information, see the Spam Quarantine chapter.

What to do next

Related Topics

Creating a Domain-Based Query

You create a domain-based query from the System Administration > LDAP > LDAP Server Profiles page.

Step 1 From the LDAP Server Profiles page, click **Advanced**.

Step 2 Click **Add Domain Assignments.**

Step 3 Enter a name for the domain-based query.

Step 4 Select the query type.

Note When you create domain-based queries, you cannot select different types of queries. Once you select a query type, the appliance populates the query field with queries of that type from the available server profiles.

Step 5 In the Domain Assignments field, enter a domain.

Step 6 Select a query to associate with the domain.

Step 7 Continue to add rows until you have added all the domains to your query.

Step 8 You can enter a default query to run if all other queries fail. If you do not want to enter a default query, select **None**.

Step 9 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 10 Optionally, if you use the {f} token in an acceptance query, you can add an envelope sender address to the test query.

Note Once you create the domain-based query, you need to associate it with a public or private listener.

Step 11 Submit and commit your changes.

Using Chain Queries to Perform a Series of LDAP Queries

A chain query is a series of LDAP queries that the appliance attempts to run in succession. The appliance attempts to run each query in the "chain" until the LDAP server returns a positive response (or the final query in the "chain" returns a negative response or fails). For chained routing queries, the appliance re-runs the same configured chain query in sequence for each rewritten email address. Chain queries can be useful if entries in your LDAP directory use different attributes to store similar (or the same) values. For example, you might have used the attributes maillocaladdress and mail to store user email addresses. To ensure that your queries run against both these attributes, you can use chain queries.

Step 1 Create server profiles for each of the queries 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 LDAP Server Profiles to Store Information About the LDAP Server, on page 4.

Step 2 Create the chain query. For more information, see Creating a Chain Query, on page 27.

Step 3 Enable the chain query on the public or private listener. For more information about configuring listeners, see the "Configuring the Gateway to Receive Mail" chapter.

Note You can also enable domain-based queries for LDAP end-user access or spam notifications for the Spam Quarantine. For more information, see the Spam Quarantine chapter.

What to do next

Related Topics

- Creating a Chain Query, on page 27

Creating a Chain Query

You create a chain query from the System Administration > LDAP > LDAP Server Profiles page.

Step 1 From the LDAP Server Profiles page, click **Advanced**.

Step 2 Click **Add Chain Query**.

Step 3 Add a name for the chain query.

Step 4 Select the query type.

When you create chain queries, you cannot select different types of queries. Once you select a query type, the appliance populates the query field with queries of that type from available server profiles.

Step 5 Select a query to add to the chain query.

The appliance runs the queries in the order you configure them. Therefore, if you add multiple queries to the chain query, you might want to order the queries so that more specific queries are followed by more general queries.

Step 6 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 7 Optionally, if you use the {f} token in an acceptance query, you can add an envelope sender address to the test query.

Note Once you create the chain query, you need to associate it with a public or private listener.

Step 8 Submit and commit your changes.

Using LDAP For Directory Harvest Attack Prevention

Directory Harvest Attacks occur when a malicious sender attempts to send messages to recipients with common names, and the email gateway responds by verifying that a recipient has a valid mailbox at that location. When performed on a large scale, malicious senders can determine who to send mail to by “harvesting” these valid addresses for spamming.

The appliance can detect and prevent Directory Harvest Attack (DHA) when using LDAP acceptance validation queries. You can configure LDAP acceptance to prevent directory harvest attacks within the SMTP conversation or within the work queue.

Related Topics

- Directory Harvest Attack Prevention within the SMTP Conversation, on page 28

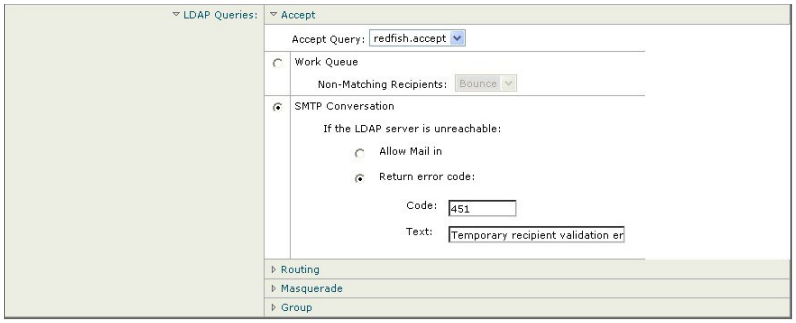
• Directory Harvest Attack Prevention within the Work Queue, on page 29

Directory Harvest Attack Prevention within the SMTP Conversation

You can prevent DHAs by entering only domains in the Recipient Access Table (RAT), and performing the LDAP acceptance validation in the SMTP conversation.

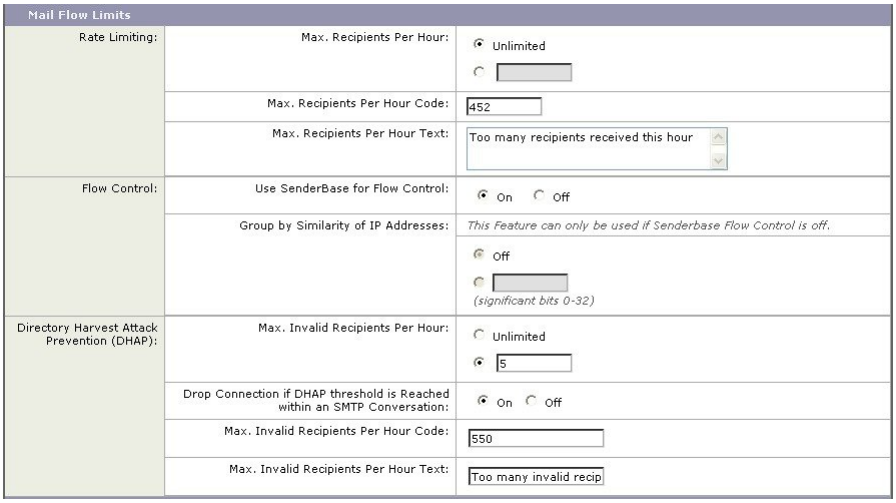
To drop messages during the SMTP conversation, configure an LDAP server profile for LDAP acceptance. Then, configure the listener to perform an LDAP accept query during the SMTP conversation.

Figure 7: Configuring the Acceptance Query in the SMTP Conversation



Once you configure LDAP acceptance queries for the listener, you must configure DHAP settings in the mail flow policy associated with the listener.

Figure 8: Configuring the Mail Flow Policy to Drop Connections in the SMTP Conversation



In the mail flow policy associated with the listener, configure the following Directory Harvest Attack Prevention settings:

- **Max. Invalid Recipients Per hour**. The maximum number of invalid recipients per hour this listener will receive from a remote host. This threshold represents the total number of RAT rejections combined with the total number of messages to invalid LDAP recipients dropped in the SMTP conversation or bounced in the work queue. For example, you configure the threshold as five, and the counter detects two RAT rejections and three dropped messages to invalid LDAP recipients. At this point, the appliance determines that the threshold is reached, and the connection is dropped. By default, the maximum number

of recipients per hour for a public listener is 25. For a private listener, the maximum number of recipients per hour is unlimited by default. Setting it to "Unlimited" means that DHAP is not enabled for that mail flow policy.

- **Drop Connection if DHAP Threshold is reached within an SMTP conversation**. Configure the appliance to drop the connection if the Directory Harvest Attack Prevention threshold is reached.
- **Max. Recipients Per Hour Code**. Specify the code to use when dropping connections. The default code is 550.
- **Max. Recipients Per Hour Text**. Specify the text to use for dropped connections. The default text is "Too many invalid recipients."

If the threshold is reached, the Envelope Sender of the message does not receive a bounce message when a recipient is invalid.

Directory Harvest Attack Prevention within the Work Queue

You can prevent most DHAs by entering only domains in the Recipient Access Table (RAT), and performing the LDAP acceptance validation within the work queue. This technique prevents the malicious senders from knowing if the recipient is valid during the SMTP conversation. (When acceptance queries are configured, the system accepts the message and performs the LDAP acceptance validation within the work queue.) However, the Envelope Sender of the message will still receive a bounce message if a recipient is not valid.

Related Topics

- Configuring Directory Harvest Prevention in the Work Queue, on page 29

Configuring Directory Harvest Prevention in the Work Queue

To prevent Directory Harvest Attacks, you first configure an LDAP server profile, and enable LDAP Accept. Once you have enabled LDAP acceptance queries, configure the listener to use the accept query, and to bounce mail for non-matching recipients:

Next, configure the Mail Flow Policy to define the number of invalid recipient addresses the system will allow per sending IP address for a specific period of time. When this number is exceeded, the system will identify this condition as a DHA and send an alert message. The alert message will contain the following information:

```
LDAP: Potential Directory Harvest Attack from host=('IP-address', 'domain_name
'), dhap_limit=n, sender_group=sender_group,


listener=listener_name, reverse_dns=(reverse_IP_address, 'domain_name
', 1), sender=envelope_sender, rcpt=envelope_recipients
```

The system will bounce the messages up to the threshold you specified in the mail flow policy and then it will silently accept and drop the rest, thereby informing legitimate senders that an address is bad, but preventing malicious senders from determining which receipts are accepted.

This invalid recipients counter functions similarly to the way Rate Limiting is currently available in AsyncOS: you enable the feature and define the limit as part of the mail flow policy in a public listener's HAT (including the default mail flow policy for the HAT).

You can also configure this in the command-line interface using the `listenerconfig` command.

This feature is also displayed when editing any mail flow policy in the GUI, providing that LDAP queries have been configured on the corresponding listener:

Entering a number of invalid recipients per hour enables DHAP for that mail flow policy. By default, 25 invalid recipients per hour are allowed for public listeners. For private listeners, the maximum invalid recipients per hour is unlimited by default. Setting it to “Unlimited” means that DHAP is not enabled for that mail flow policy.

Configuring AsyncOS for SMTP Authentication

AsyncOS provides support for SMTP authentication. SMTP Auth is a mechanism for authenticating clients connected to an SMTP server.

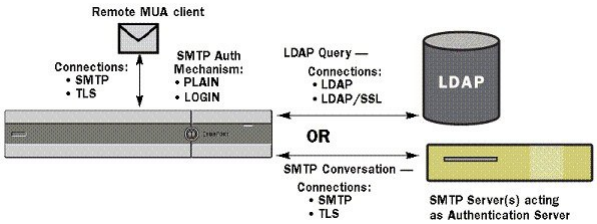
The practical use of this mechanism is that users at a given organization are able to send mail using that entity’s mail servers even if they are connecting remotely (e.g. from home or while traveling). Mail User Agents (MUAs) can issue an authentication request (challenge/response) when attempting to send a piece of mail.

Users can also use SMTP authentication for outgoing mail relays. This allows the appliance to make a secure connection to a relay server in configurations where the appliance is not at the edge of the network.

AsyncOS supports two methods to authenticate user credentials:

- You can use an LDAP directory.
- You can use a different SMTP server (SMTP Auth forwarding and SMTP Auth outgoing).

Figure 9: SMTP Auth Support: LDAP Directory Store or SMTP Server



Configured SMTP Authentication methods are then used to create SMTP Auth profiles via the smtpauthconfig command for use within HAT mail flow policies (see Enabling SMTP Authentication on a Listener, on page 34).

Related Topics

- Configuring SMTP Authentication, on page 30
- Configuring an SMTP Authentication Query, on page 32
- SMTP Authentication via Second SMTP Server (SMTP Auth with Forwarding), on page 32
- SMTP Authentication with LDAP, on page 33
- Authenticating SMTP Sessions Using Client Certificates, on page 36
- Outgoing SMTP Authentication, on page 36
- Logging and SMTP Authentication, on page 37

Configuring SMTP Authentication

If you are going to authenticate with an LDAP server, select the SMTPAUTH query type on the Add or Edit LDAP Server Profile pages (or in the **`ldapconfig`** command) to create an SMTP Authentication query. For each LDAP server you configure, you can configure a SMTPAUTH query to be used as an SMTP Authentication profile.

There are two kinds of SMTP authentication queries: LDAP bind and passphrase as attribute. When you use passphrase as attribute, the appliance will fetch the passphrase field in the LDAP directory. The passphrase may be stored in plain text, encrypted, or hashed. When you use LDAP bind, the appliance attempts to log into the LDAP server using the credentials supplied by the client.

Related Topics

- Specifying a Passphrase as Attribute, on page 31

Specifying a Passphrase as Attribute

The convention in OpenLDAP, based on RFC 2307, is that the type of coding is prefixed in curly braces to the encoded passphrase (for example, "{SHA}5en6G6MezRroT3XKqkdPOmY/BfQ="). In this example, the passphrase portion is a base64 encoding of a plain text passphrase after application of SHA.

The appliance negotiates the SASL mechanism with the MUA before getting the passphrase, and the appliance and the MUA decide on what method (LOGIN, PLAIN, MD5, SHA, SSHA, and CRYPT SASL mechanisms are supported). Then, the appliance queries the LDAP database to fetch a passphrase. In LDAP, the passphrase can have a prefix in braces.

- If there is no prefix, the appliance assumes that the passphrase was stored in LDAP in plaintext.
- If there is a prefix, the appliance will fetch the hashed passphrase, perform the hash on the username and/or passphrase supplied by the MUA, and compare the hashed versions. The appliance supports SHA1 and MD5 hash types based on the RFC 2307 convention of prepending the hash mechanism type to the hashed passphrase in the passphrase field.
- Some LDAP servers, like the OpenWave LDAP server, do not prefix the encrypted passphrase with the encryption type; instead, they store the encryption type as a separate LDAP attribute. In these cases, you can specify a default SMTP AUTH encryption method the appliance will assume when comparing the passphrase with the passphrase obtained in the SMTP conversation.

The appliance takes an arbitrary username from the SMTP Auth exchange and converts that to an LDAP query that fetches the clear or hashed passphrase field. It will then perform any necessary hashing on the passphrase supplied in the SMTP Auth credentials and compare the results with what it has retrieved from LDAP (with the hash type tag, if any, removed). A match means that the SMTP Auth conversation shall proceed. A failure to match will result in an error code.

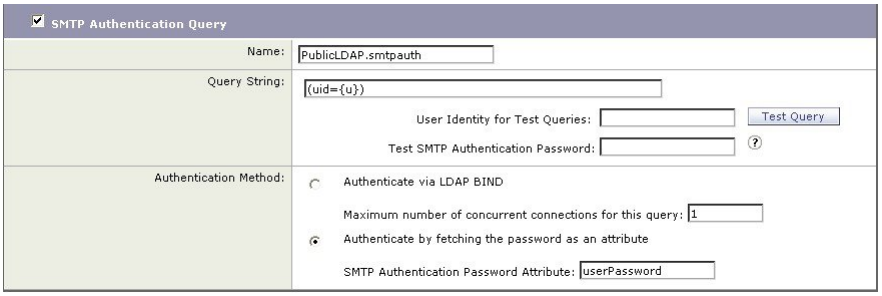
Configuring an SMTP Authentication Query

Table 6: SMTP Auth LDAP Query Fields

Name	A name for the query.
Query String	You can select whether to authenticate via LDAP bind or by fetching the passphrase as an attribute. **Bind**: Attempt to log into the LDAP server using the credentials supplied by the client (this is called an LDAP bind). Specify the maximum number of concurrent connections to be used by the SMTP Auth query. This number should not exceed the number specified in the LDAP server attributes above. Note, to avoid large number of session time-outs for bind authentication, increase the maximum number of concurrent connections here (typically nearly all of the connections can be assigned to SMTP Auth). A new connection is used for each bind authentication. The remainder of the connections are shared by the other LDAP query types. **Passphrase as Attribute**: To authenticate by fetching passphrases, specify the passphrase in the SMTP Auth passphrase attribute field below. Specify the LDAP query to use for either kind of authentication.Active Directory example query: (&(samaccountname={u})(objectCategory=person)(objectClass=user))
SMTP Auth Passphrase Attribute	If you have selected “Authenticate by fetching the passphrase as an attribute,” you can specify the passphrase attribute here.

In the following example, the System Administration > LDAP page is used to edit the LDAP configuration named “PublicLDAP” to include an SMTPAUTH query. The query string (uid={u}) is constructed to match against userPassword attribute.

Figure 10: SMTP Authentication Query



When an SMTPAUTH profile has been configured, you can specify that the listener uses that query for SMTP authentication.

SMTP Authentication via Second SMTP Server (SMTP Auth with Forwarding)

You can configure the appliance to verify the username and passphrase that have been provided to another SMTP authenticated conversation with a different SMTP server.

The authenticating server is not the server that transfers mail; rather, it only responds to SMTP Authentication requests. When authentication has succeeded, the SMTP transfer of mail with the dedicated mail server can

proceed. This feature is sometimes referred to as “SMTP Authentication with forwarding” because only the credentials are forwarded (or “proxied”) to another SMTP server for authentication.

Step 1 Choose **Network > SMTP Authentication**.

Step 2 Click **Add Profile..**.

Step 3 Enter a unique name for the SMTP authentication profile.

Step 4 For the **Profile Type**, select **Forward**.

Step 5 Click **Next**.

Step 6 Enter the hostname/IP address and port of the forwarding server. Select a forwarding interface to use for forwarding authentication requests. Specify the number of maximum simultaneous connections. Then, you can configure whether TLS is required for connections from the appliance to the forwarding server You can also select a SASL method to use (PLAIN or LOGIN), if available. This selection is configured for each forwarding server.

Step 7 Submit and commit your changes.

Step 8 After creating the authentication profile, you can enable the profile on a listener. See Enabling SMTP Authentication on a Listener, on page 34 for more information.

SMTP Authentication with LDAP

To create an LDAP-based SMTP Authentication profile, you must have previously created an SMTP Authentication query in conjunction with an LDAP server profile using the System Administration > LDAP page. You can then use this profile to create an SMTP Authentication profile. For more information about creating an LDAP profile, see Understanding LDAP Queries, on page 2.

Step 1 Choose **Network > SMTP Authentication**.

Step 2 Click **Add Profile**.

Step 3 Enter a unique name for the SMTP authentication profile.

Step 4 For the Profile Type, select **LDAP**.

Step 5 Click **Next**.

Step 6 Select the LDAP query you would like to use for this authentication profile.

Step 7 Select a default encryption method from the drop-down menu. You can select from SHA, Salted SHA, Crypt, Plain, or MD5. If your LDAP servers prefix an encrypted passphrase with the encryption type, leave ‘None’ selected. If your LDAP server saves the encryption type as a separate entity (OpenWave LDAP servers, for example), then select an encryption method from the menu. The default encryption setting will not be used if the LDAP query is using bind.

Step 8 Click **Finish**.

Step 9 Submit and commit your changes.

Step 10 After creating the authentication profile, you can enable the profile on a listener. See Enabling SMTP Authentication on a Listener, on page 34 for more information.

What to do next

Related Topics

Enabling SMTP Authentication on a Listener

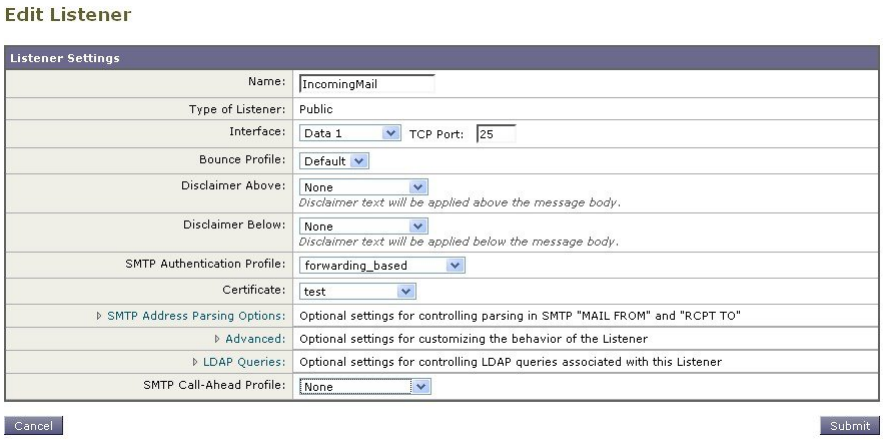
After using the **Network > SMTP Authentication** page to create an SMTP authentication "profile" that specifies the type of SMTP authentication you want to perform (LDAP-based or SMTP forwarding-based), you must associate that profile with a listener using the **Network > Listeners** page (or the **`listenerconfig`** command).

Note An authenticated user is granted RELAY connection behavior within their current Mail Flow Policy.

You may specify more than one forwarding server in a profile. SASL mechanisms CRAM-MD5 and DIGEST-MD5 are not supported between the appliance and a forwarding server.

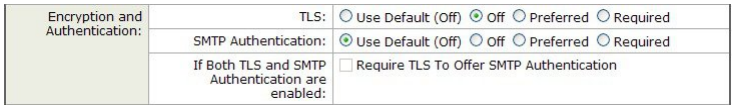
In the following example, the listener "InboundMail" is edited to use the SMTPAUTH profile configured via the Edit Listener page:

Figure 11: Selecting an SMTP Authentication Profile via the Edit Listener page



Once a listener is configured to use the profile, the Host Access Table default settings can be changed so that the listener allows, disallows, or requires SMTP Authentication:

Figure 12: Enabling SMTP Authentication on a Mail Flow Policy



Number	Description
1.	The SMTP Authentication field provides listener-level control for SMTP authentication. If you select "No," authentication will not be enabled on the listener, regardless of any other SMTP authentication settings you configure.
2.	If "Required" is selected in the second prompt (SMTP Authentication:), no AUTH keyword will be issued until TLS is negotiated (after the client issues a second EHLO command).

Related Topics

- SMTP Authentication and HAT Policy Settings, on page 35
- HAT Delayed Rejection, on page 35

SMTP Authentication and HAT Policy Settings

Because senders are grouped into the appropriate sender group before the SMTP Authentication negotiation begins, Host Access Table (HAT) settings, are not affected. When a remote mail host connects, the appliance first determines which sender group applies and imposes the Mail Policy for that sender group. For example, if a remote MTA “suspicious.com” is in your SUSPECTLIST sender group, the THROTTLE policy will be applied, regardless of the results of “suspicious.com’s” SMTPAUTH negotiation.

However, senders that do authenticate using SMTPAUTH are treated differently than “normal” senders. The connection behavior for successful SMTPAUTH sessions changes to “RELAY,” effectively bypassing the Recipient Access Table (RAT) and LDAPACCEPT. This allows the sender to relay messages through the appliance . As stated, any Rate Limiting or throttling that applies will remain in effect.

HAT Delayed Rejection

When HAT Delayed Rejection is configured, connections that would get dropped based on the HAT Sender Group and Mail Flow Policy configuration can still authenticate successfully and get the RELAY mail flow policy granted.

Configure whether to perform HAT rejection at the message recipient level.By default, HAT rejected connections will be closed with a banner message at the start of the SMTP conversation.

When an email is rejected due to HAT “Reject” settings, AsyncOS can perform the rejection at the message recipient level (RCPT TO), rather than at the start of the SMTP conversation. Rejecting messages in this way delays the message rejection and bounces the message, allowing AsyncOS to retain more detailed information about the rejected messages. For example, you can see the mail from address and each recipient address of the message which is blocked. Delaying HAT rejections also makes it less likely that the sending MTA will perform multiple retries.

When you enable HAT delayed rejection, the following behavior occurs:

- The MAIL FROM command is accepted, but no message object is created.
- All RCPT TO commands are rejected with text explaining that access to send e-mail is refused.
- If the sending MTA authenticates with SMTP AUTH, they are granted a RELAY policy and are allowed to deliver mail as normal.

You can configure delayed rejection using the `listenerconfig --> setup` CLI command. This behavior is disabled by default.

The following table shows how to configure delayed rejection for HAT.

```
example.com> listenerconfig


Currently configured listeners:

1. listener1 (on main, 172.22.138.17) QMQP TCP Port 628 Private

2. listener2 (on main, 172.22.138.17) SMTP TCP Port 25 Private


Choose the operation you want to perform:

- NEW - Create a new listener.
```

```
- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.


[]> setup

Enter the global limit for concurrent connections to be allowed across all listeners.

[300]>


[...]


By default HAT rejected connections will be closed with a banner
message at the start of the SMTP conversation. Would you like to do the rejection at the
message recipient level instead for more detailed logging of rejected mail?

[N]> y

Do you want to modify the SMTP RCPT TO reject response in this case?

[N]> y

Enter the SMTP code to use in the response. 550 is the standard code.

[550]> 551

Enter your custom SMTP response. Press Enter on a blank line to finish.

Sender rejected due to local mail policy.

Contact your mail admin for assistance.
```

Authenticating SMTP Sessions Using Client Certificates

The appliance supports the use of client certificates to authenticate SMTP sessions between the appliance and users' mail clients.

When creating an SMTP authentication profile, you select the Certificate Authentication LDAP query to use for verifying the certificate. You can also specify whether the appliance falls back to the SMTP AUTH command to authenticate the user if a client certificate isn't available.

If your organization uses client certificates to authenticate users, you have the option of using the SMTP Authentication query to check whether a user who doesn't have a client certificate can send mail as long as their record specifies that it's allowed.

Outgoing SMTP Authentication

SMTP Authentication can also be used to provide validation for an outbound mail relay, using a username and passphrase. Create an 'outgoing' SMTP authentication profile and then attach the profile to an SMTP route for the ALL domain. On each mail delivery attempt, the appliance will log on to the upstream mail relay

with the necessary credentials. SMTP authentication supports the following authorization protocols: PLAIN and LOGIN.

Step 1 Create an outgoing SMTP authentication profile.

a. Choose **Network > SMTP Authentication**.
b. Click **Add Profile**.
c. Enter a unique name for the SMTP authentication profile.
d. For the Profile Type, select **Outgoing**.
e. Click **Next**.
f. Enter an authentication username and passphrase for the authentication profile.
g. Click **Finish**.

Step 2 Configure SMTP routes to use the outgoing SMTP authentication profile that you created in Step 1.

a. Choose **Network > SMTP Routes**.
b. Click the **All Other Domains** link in the **Receiving Domain** column of the table.
c. Enter the name of the Destination Host for the SMTP route. This is the hostname of your external mail relay used to deliver outgoing mail.
d. Select the outgoing SMTP authentication profile from the drop-down menu.
e. Submit and commit your changes.

Logging and SMTP Authentication

The following events will be logged in the mail logs when the SMTP Authentication mechanism (either LDAP-based, SMTP forwarding server based, or SMTP outgoing) is configured on the appliance :

- [Informational] Successful SMTP Authentication attempts — including the user authenticated and the mechanism used. (No plaintext passphrases will be logged.)
- [Informational] Unsuccessful SMTP Authentication attempts — including the user authenticated and the mechanism used.
- [Warning] Inability to connect to the authentication server — including the server name and the mechanism.
- [Warning] A time-out event when the forwarding server (talking to an upstream, injecting appliance) times out while waiting for an authentication request.

Configuring External LDAP Authentication for Users

You can configure the appliance to use an LDAP directory on your network to authenticate users by allowing them to log in with their LDAP usernames and passphrases. After you configure the authentication queries for the LDAP server, enable the appliance to use external authentication on the **System Administration > Users** page in the GUI (or use the `userconfig` command in the CLI).

Step 1 **Create a query to find user accounts.** In an LDAP server profile, create a query to search for user accounts in the LDAP directory.

Step 2 **Create group membership queries.** Create a query to determine if a user is a member of a directory group.

Step 3 **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 "Adding Users" in the "Distributing Administrative Tasks" chapter.

Note Use the Test Query button on the LDAP page (or the `ldaptest` command) to verify that your queries return the expected results. For more information, see Testing LDAP Queries, on page 16.

What to do next

Related Topics

- User Accounts Query, on page 38
- Group Membership Queries, on page 39

User Accounts Query

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 username attribute that AsyncOS uses when it searches for a user account on an Active Directory server.

Table 7: Default User Account Query String and Attribute: Active Directory

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 username attribute that AsyncOS uses when it searches for a user account on an OpenLDAP server.

Table 8: Default User Account Query String and Attribute: OpenLDAP

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

AsyncOS also uses a query to determine if a user is a member of a directory group. Membership in a directory group membership determines the user's permissions within the system. When you enable external authentication on the 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 username, and the attribute that contains the group name. Based on the server type that you select for your LDAP server profile, AysncOS enters default values for the username 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 usernames, 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 9: Default Group Membership Query Strings and Attribute: Active Directory

Server Type	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 memberOf list instead of usernames, you can replace {u} with {dn} .
Attribute that holds each member's username (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 10: Default Group Membership Query Strings and Attributes: OpenLDAP

Server Type	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}))
Attribute that holds each member's username (or a DN for the user's record)	memberUid
Attribute that contains the group name	cn

Authenticating End-Users of the Spam Quarantine

Spam quarantine 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.

If you want the Spam Quarantine to use an LDAP query for end-user access, check the "Designate as the active query" check box. If there is an existing active query, it is disabled. When you open the **System Administration > LDAP** page, an asterisk (*) is displayed next to the active queries.

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 proxyAddresses for Active Directory servers and mail for OpenLDAP servers. You can enter your own query and email attributes. To create the query from the CLI, use the isqauth subcommand of the ldapconfig command.

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

Related Topics

- Sample Active Directory End-User Authentication Settings, on page 41
- Sample OpenLDAP Alias Consolidation Settings, on page 43
- Configuring End-User Access to the Spam Quarantine

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 mail and proxyAddresses email attributes, and the default query string for end-user authentication for Active Directory servers.

Table 11: 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 mail and mailLocalAddress email attributes, and the default query string for end-user authentication for OpenLDAP servers.

Table 12: 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.

If you want the Spam Quarantine to use an LDAP query for spam notifications, check the "Designate as the active query" check box. If there is an existing active query, it is disabled. When you open the System Administration > LDAP page, an asterisk (*) is displayed next to the active queries.

For Active Directory servers, the default query string 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.

Related Topics

- Sample Active Directory Alias Consolidation Settings, on page 42
- Sample OpenLDAP Alias Consolidation Settings, on page 43

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

Authentication Method	**Anonymous**
Server Type	Active Directory
Port	3268
Base DN	[Blank]
Connection Protocol	Use SSL

Query String	`(`
	`|(mail={a})(mail=smtp:{a})`
	`)`

Email Attribute	mail

Note This example is for representational purposes only. Queries and OU or tree settings may vary depending on the environment and configuration.

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 14: 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

Note This example is for representational purposes only. Queries and OU or tree settings may vary depending on the environment and configuration.

Sample User Distinguished Name Settings

This section shows sample settings for an Active Directory server and the user distinguished name query. This example uses anonymous authentication for the Active Directory server and a query string for user distinguished name retrieval for Active Directory servers.

Table 15: Example LDAP Server and Spam Quarantine Alias Consolidation Settings: Active Directory

Authentication Method	Anonymous
Server Type	Active Directory
Port	3268
Base DN	[Blank]
Connection Protocol	Use SSL
Query String	`(proxyAddresses=smtp:{a})`

Note This example is for representational purposes only. Queries and OU or tree settings may vary depending on the environment and configuration.

Configuring AsyncOS To Work With Multiple LDAP Servers

When you configure an LDAP profile, you can configure the appliance to connect to a list of multiple LDAP servers. To use multiple LDAP servers, you must configure LDAP servers to contain the same information, use the same structure, and use the same authentication information. (third party products exist that can consolidate the records).

When you configure the appliance to connect to redundant LDAP servers, you can configure the LDAP configuration for failover or load balancing.

You can use multiple LDAP servers to achieve the following results:

- **Failover**. When you configure the LDAP profile for failover, the appliance fails over to the next LDAP server in the list if it cannot connect to the first LDAP server.
- **Load Balancing**. When you configure the LDAP profile for load balancing, the appliance distributes connections across the list of LDAP servers when it performs LDAP queries.

You can configure redundant LDAP servers from the System Administration > LDAP page or from the CLI ldapconfig command.

Performing Recipient Verification and Resolving Group Queries using Azure AD Domain Services

To perform recipient verification and resolve group queries using Azure AD Domain Services, see the Configuring Azure AD DS documentation at https://docs.ces.cisco.com/docs/using-azure-ad-ds-with-ces#lockdown-secure-ldap-access-over-the-internet

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.

Related Topics

- Failover, on page 44
- Load Balancing, on page 45

Failover

To ensure that LDAP queries are resolved, you can configure your LDAP profile for failover. If the connection to the LDAP server fails, or the query returns certain error codes (for example, Unavailable or Busy), the appliance attempts to query the next LDAP server specified in the list.

The 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 certain error codes

(for example, Unavailable or Busy), 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 appliance connects to your primary LDAP server by default, ensure that you enter it as the first server in your list of LDAP servers.

If the appliance connects to a second or subsequent LDAP server, it remains connected to that server until it reaches a timeout period. After it reaches the timeout, it attempts to reconnect to the first server in the list.

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.

Related Topics

- Configuring the Appliance for LDAP Failover, on page 45

Configuring the Appliance for LDAP Failover

To configure the appliance for LDAP failover, complete the following steps in the GUI:

Step 1 From System Administration > LDAP, select the LDAP server profile you want to edit.

Step 2 From the LDAP server profile, configure the following settings:

Number	Description
1	List LDAP Servers.
2	Configure Maximum Connections.

Step 3 Configure other LDAP settings 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 configure your LDAP profile for load balancing, the 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.

Reliance Topics

- Configuring the Appliance for Load Balancing, on page 46

Configuring the Appliance for Load Balancing

Step 1 From **System Administration > LDAP**, select the LDAP server profile you want to edit.

Step 2 From the LDAP server profile, configure the following settings:

Number	Description
1	List LDAP Servers
2	Configure Maximum Connections

Step 3 Configure other LDAP settings and commit the changes.