

# Configure LDAP Chained Query in the Email Security Appliance

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Procedure](#)

[Verify](#)

[Related Information](#)

## Introduction

This document describes how to enable the Lightweight Directory Access Protocol (LDAP) Chained query option in the Email Security Appliance.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Two (2) or more LDAP profiles are already configured in the Email Security Appliance (ESA). This example uses Domain\_A and Domain\_B as the profiles.
- An active query in the LDAP profiles (this example uses the Accept query).

### Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

The LDAP Chained Query is a feature in the Cisco Email Security Appliance that allows administrators to perform directory lookups across multiple LDAP servers. With this feature, administrators can configure multiple LDAP profiles if a specific domain is hosted on multiple servers. If one server fails or the ESA is unable to retrieve a result for the query, the appliance automatically switches to the next server until a final answer is provided.

## Procedure

1. Log in to the **Cisco Email Security Appliance** with your administrative credentials.



**Secure Email**  
Cloud Gateway C100V  
Version: 14.2.0-616

Username:

Passphrase:

[Login](#)

[Use Single Sign](#)

2. Navigate to the **LDAP** settings page under the **System Administration** menu.

Security Services	Network	System Administration								
<p>"My Dashboard" page by adding report modules for you by default. The Overview page can</p>		<ul style="list-style-type: none"> <li>System Health</li> <li>Trace</li> <li>Alerts</li> <li><b>LDAP</b></li> <li>SAML</li> <li>OpenID Connect</li> <li>SSL Configuration</li> <li>Log Subscriptions</li> <li>Return Addresses</li> <li>Disk Management</li> <li>Cisco Talos Email Status Portal Register</li> </ul>								
<table border="1"> <tr> <td colspan="2"> <input checked="" type="checkbox"/> Overview &gt; Quarantine (Virus)         </td> </tr> <tr> <td>           System Status: Online         </td> <td rowspan="3"> <i>Centralized Services &amp; Quarantines). Please</i> </td> </tr> <tr> <td>           Messages per hour: 0         </td> </tr> <tr> <td>           Work Queue: 0         </td> </tr> <tr> <td colspan="2">           Local Quarantines         </td> </tr> </table>		<input checked="" type="checkbox"/> Overview > Quarantine (Virus)		System Status: Online	<i>Centralized Services &amp; Quarantines). Please</i>	Messages per hour: 0	Work Queue: 0	Local Quarantines		<ul style="list-style-type: none"> <li>Users</li> <li>User Roles</li> <li>Account Settings</li> <li>Time Zone</li> <li>Time Settings</li> <li>Configuration File</li> <li>Feature Key Settings</li> <li>Feature Keys</li> </ul>
<input checked="" type="checkbox"/> Overview > Quarantine (Virus)										
System Status: Online	<i>Centralized Services &amp; Quarantines). Please</i>									
Messages per hour: 0										
Work Queue: 0										
Local Quarantines										
<p>for this section.</p>										

3. Click **Advance**.

## LDAP

**LDAP Server Profiles**

using the Active Directory Wizard. [?](#)

Server Profile	Host Name	Port	Queries
Domain_A	10.10.10.1	3268	Domain_A.accept
Domain_B	10.10.10.2	3268	Domain_B.accept

4. Click **Add Chained Query**.

**LDAP Server Profiles**

using the Active Directory Wizard. [?](#)

Server Profile	Host Name	Port	Queries
Domain_A	10.10.10.1	3268	Domain_A.accept
Domain_B	10.10.10.2	3268	Domain_B.accept

Advanced

**Domain Assignments**

Name	Query Type
Assignment_AB	Accept

**Chained Queries**

5. Specify a name for the chained query, choose the query type to be used, and add the LDAP profiles from the drop-down menus. Then click **Submit**.

## Add Chained Query

Chained Query							
Name:	<input type="text" value="Test"/>						
Query Type:	Accept <span>▼</span>						
Order of Queries:	<table border="1"><thead><tr><th>Order</th><th>Query</th></tr></thead><tbody><tr><td>1</td><td>Domain_A.accept <span>▼</span></td></tr><tr><td>2</td><td>Domain_B.accept <span>▼</span></td></tr></tbody></table>	Order	Query	1	Domain_A.accept <span>▼</span>	2	Domain_B.accept <span>▼</span>
Order	Query						
1	Domain_A.accept <span>▼</span>						
2	Domain_B.accept <span>▼</span>						
Test:	<input type="button" value="Test Query"/>						

**Note:** In this section, you can configure a specific order for the profile lookup.

6. Navigate to the **Listeners** settings in the **Network** tab.

The screenshot shows the Cisco Cloud Gateway C100V interface. The top navigation bar includes 'Monitor', 'Mail Policies', 'Security Services', 'Network', and 'System'. The 'Network' tab is selected, and a dropdown menu is open, showing options like 'IP Interfaces', 'Listeners', 'SMTP Routes', 'DNS', 'Routing', 'SMTP Call-Ahead', 'Bounce Profiles', 'SMTP Authentication', 'Incoming Relays', 'Certificates', 'Cloud Service Settings', and 'CRL Sources'. The 'Listeners' option is highlighted. Below the navigation, the 'Listeners' settings page is displayed, featuring a table with columns for 'Listener Name', 'Interface', 'Port', and 'Host A'. The table contains two entries: 'MailFlow' on 'Data 1' at port 25 with host 'HAT', and 'MailFlow-Ext' on 'Data 2' at port 25 with host 'HAT'. There is also an 'Add Listener...' button and a 'Global Settings' section below the table.

7. Choose a listener to enable the chained query and scroll down to **LDAP Queries**.

The screenshot shows the 'LDAP Queries' settings page. It features a section titled 'LDAP Queries:' followed by the text 'Optional settings for controlling LDAP queries associated with this...'. The page is partially cut off on the right side.

8. Expand the **LDAP queries** option, then expand the **Accept** option, and choose the chained query that was

previously created.

LDAP Queries: Accept

Accept Query: Test

Work Queue

Non-Matching Recipients: Bounce

SMTP Conversation

If the LDAP server is unreachable:

Allow Mail in

Return error code:

Code: 451

Text: Temporary recipient validation error.

Routing

Masquerade

Group

9. Click **Submit** and **commit** the changes.

## Verify

With the earlier configuration, the Email Security Appliance validates recipient addresses with the use of the accept query in both LDAP profiles. First, it queries the Domain\_A profile, and if there is no result, it moves to the next configured profile, in this case, the Domain\_B profile.

To verify if the LDAP chained query option works fine in the Cisco Email Security Appliance, complete these steps:

1. Log in to the Cisco Email Security Appliance with an administrator account.
2. Navigate to the **LDAP** Configuration page under the **System Administration** tab.
3. Click **Test Server(s)** for each server in the chain in order to verify the LDAP servers configured for chained query work properly.
4. Open the Chained query that is to be tested.
5. Click the **Test Query**; test an email recipient hosted in the second profile so the device queries the first profile, fails, and tests the second profile.

## Related Information

- [Cisco Technical Support & Downloads](#)