Comprehensive Spam Quarantine Setup Guide on Email Security Appliance (ESA) and Security Management Appliance (SMA)

Contents

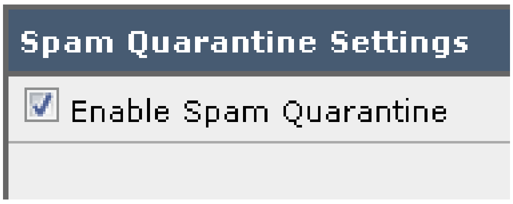
Introduction

This document describes how to configure the spam quarantine on the ESA or SMA and associated features : external authentication with LDAP and spam quarantine notification.

Procedure

Configure Local Spam Quarantine on the ESA

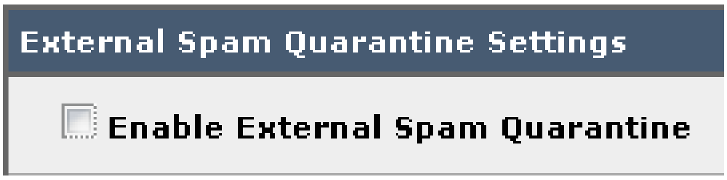
1. On the ESA, choose **Monitor > Spam Quarantine**.
2. In the Spam Quarantine Settings section, check the **Enable Spam Quarantine** check box and set the desired quarantine settings.



Spam Quarantine Settings

☑ Enable Spam Quarantine

3. Choose **Security Services > Spam Quarantine**.
4. Ensure the **Enable External Spam Quarantine** check box is unchecked, unless you plan to use External Spam Quarantine (see section below).



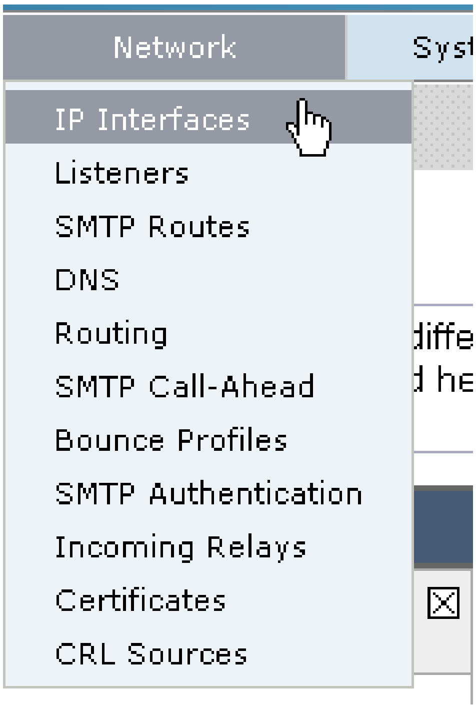
External Spam Quarantine Settings

☐ Enable External Spam Quarantine

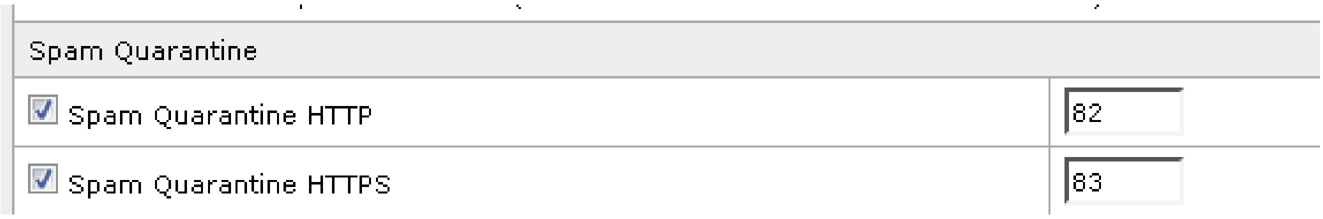
5. Submit and commit changes.

Enable Quarantine Ports and Specify a Quarantine URL at the Interface

1. Choose **Network > IP Interfaces**.



2. Click the interface name of the interface you will use in order to access the quarantine. In the spam quarantine section, check the check boxes and specify default ports or change as required:Spam Quarantine HTTPSpam Quarantine HTTPS

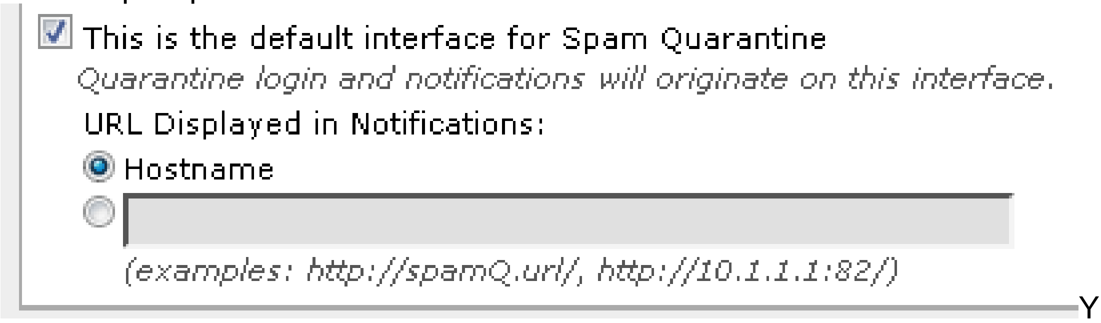


Spam Quarantine

☑ Spam Quarantine HTTP 82

☑ Spam Quarantine HTTPS 83

3. Check the **This is the default interface for Spam Quarantine** check box.
4. Under "URL Displayed in Notifications", by default the appliance uses the system hostname (cli: **sethostname)** unless otherwise specified in the second radio button option and text field. This example specifies the default hostname setting. You can specify a custom URL in order to access your Spam



☑ This is the default interface for Spam Quarantine

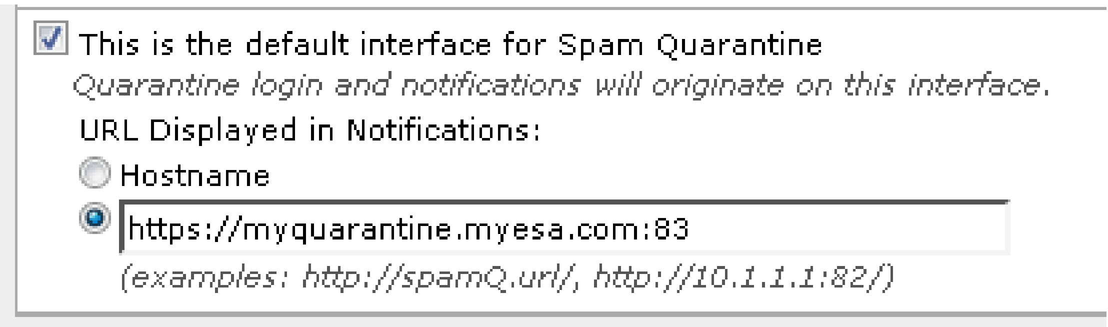
Quarantine login and notifications will originate on this interface.

URL Displayed in Notifications:

● Hostname

○

(examples: http://spamQ.url/, http://10.1.1.1:82/)



☑ This is the default interface for Spam Quarantine

Quarantine login and notifications will originate on this interface.

URL Displayed in Notifications:

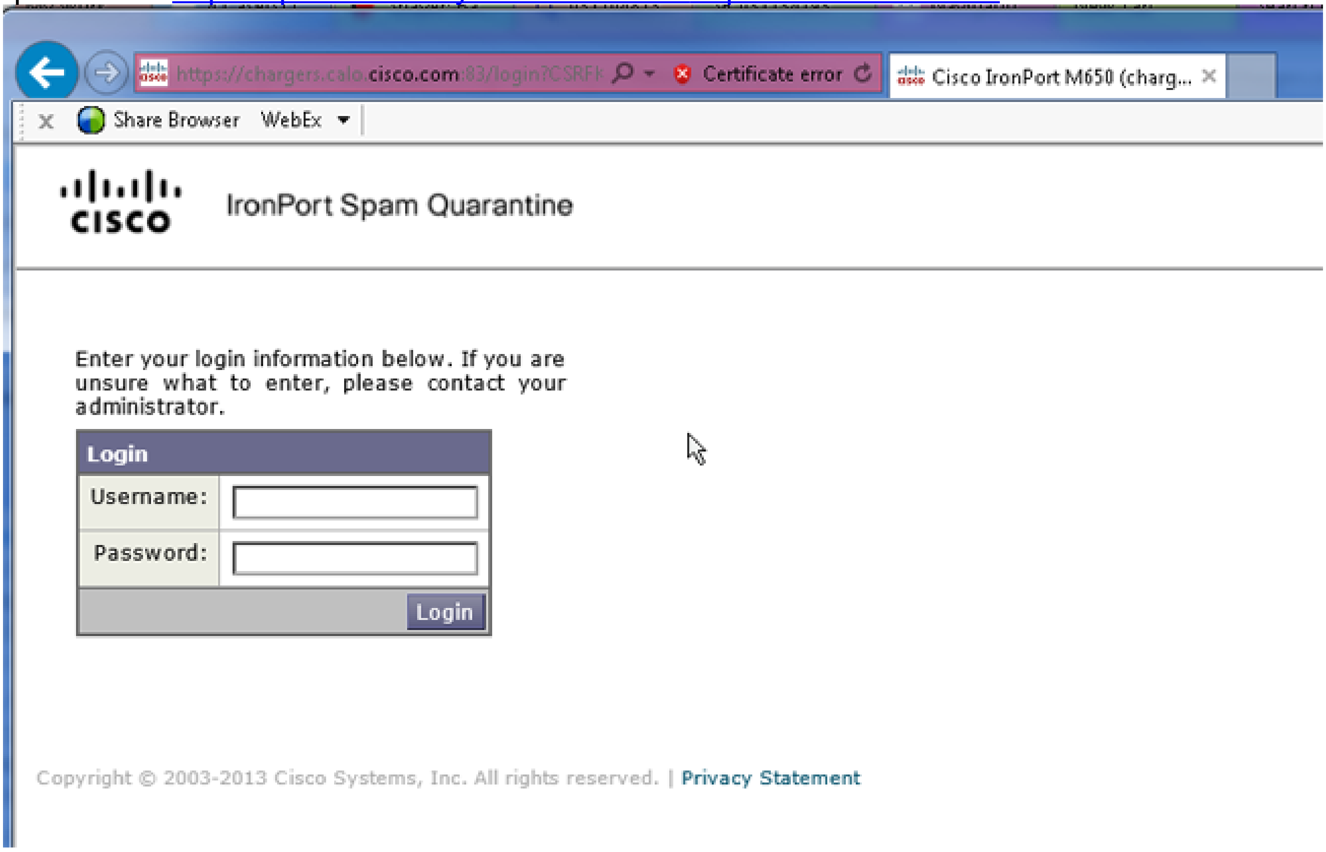
○ Hostname

● https://myquarantine.myesa.com:83

(examples: http://spamQ.url/, http://10.1.1.1:82/)

Quarantine. **Note**: If you configure the quarantine for external access, you will need an external IP address configured on the interface or an external IP that is Network Address Translated to an internal IP.If you do not use a hostname you can keep the Hostname radio button checked, but still access the quarantine by IP address only. For example, https://10.10.10.10:83.

5. Submit and commit changes.
6. Validate. If you specify a hostname for the spam quarantine, ensure the hostname is resolvable via internal Domain Name System (DNS) or external DNS. DNS will resolve the hostname to your IP address.If you do not get a result, check with your Network Administrator and continue to access the Quarantine by IP address like the previous example until the host shows up in DNS.>nslookup quarantine.mydomain.comNavigate to your URL configured previously in a web browser in order to validate that you can access the quarantine: https://quarantine.mydomain.com:83https://10.10.10.10:83



https://chargers.calo.cisco.com:83/login?CSRFk
Certificate error
Cisco IronPort M650 (charg...
Share Browser
WebEx

IronPort Spam Quarantine

Enter your login information below. If you are unsure what to enter, please contact your administrator.

Login	
Username:	
Password:	

Login

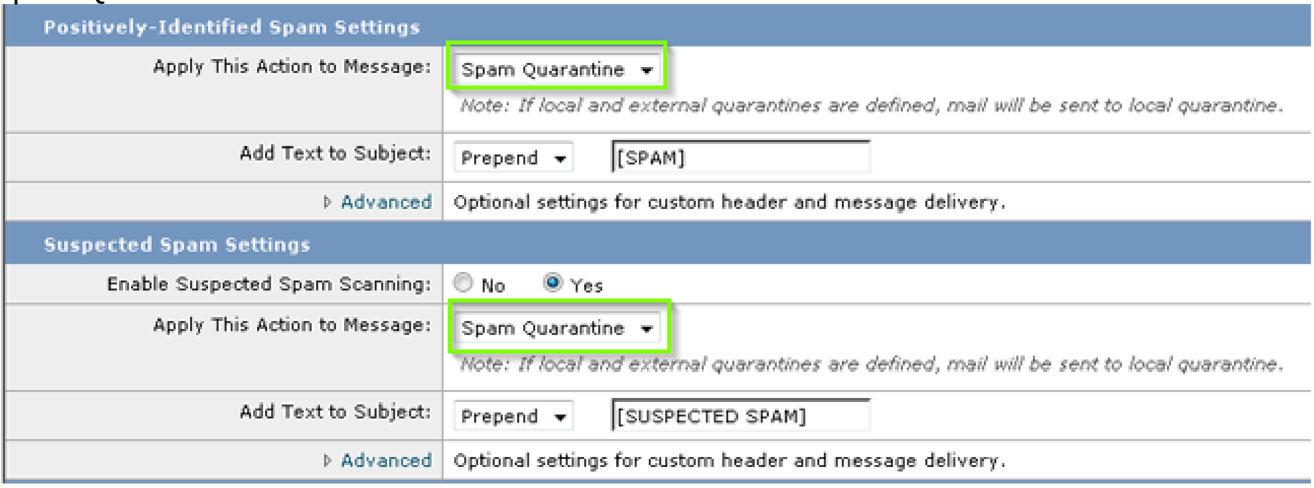
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

Configure the ESA to Move Positive Spam and/or Suspect Spam to Spam Quarantine

In order to quarantine your Suspect Spam and/or Positively Identified Spam messages, complete these steps:

1. On the ESA, click **Mail Policies > Incoming Mail Policies** and then the anti-spam column for the Default Policy.

2. Change the action of either the Positively Identified Spam or Suspect Spam to send to the Spam Quarantine."



Positively-Identified Spam Settings

Apply This Action to Message: Spam Quarantine ▾
Note: If local and external quarantines are defined, mail will be sent to local quarantine.

Add Text to Subject: Prepend ▾ [SPAM]

▹ Advanced Optional settings for custom header and message delivery.

Suspected Spam Settings

Enable Suspected Spam Scanning: ○ No ● Yes

Apply This Action to Message: Spam Quarantine ▾
Note: If local and external quarantines are defined, mail will be sent to local quarantine.

Add Text to Subject: Prepend ▾ [SUSPECTED SPAM]

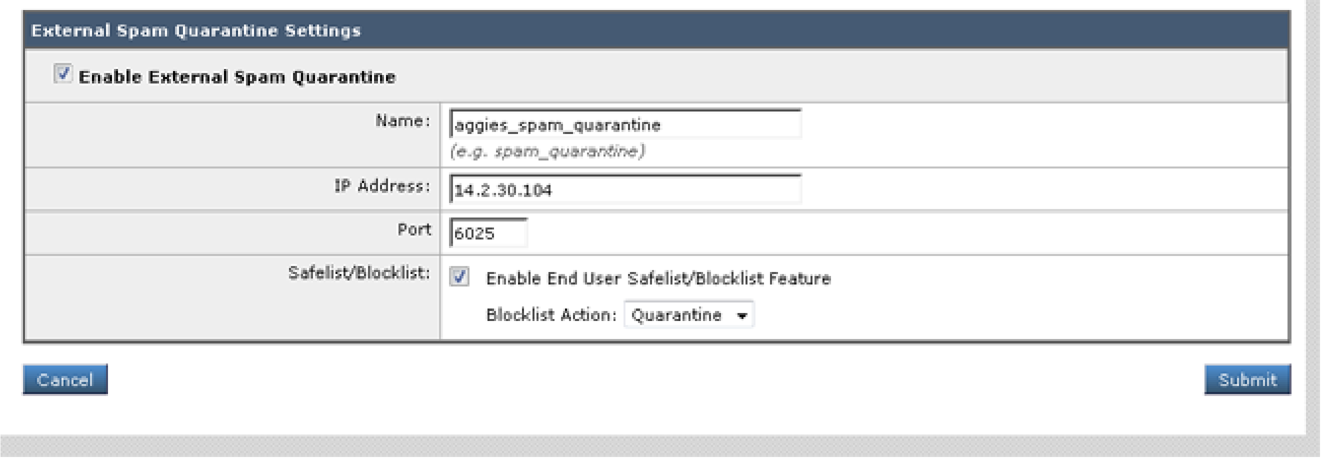
▹ Advanced Optional settings for custom header and message delivery.

3. Repeat the process for any other ESAs you might have configured for External Spam Quarantine. If you made this change at the cluster level you will not have to repeat it as the change will be propogated to the other appliances in the cluster.
4. Submit and commit changes.
5. At this point, mail that would have otherwise been delivered or dropped will get quarantined.

Configure External Spam Quarantine on the SMA

The steps to configure External Spam Quarantine on the SMA are the same as the previous section with a few exceptions:

1. On each of your ESAs, you will need to disable the local quarantine. Choose **Monitor > Quarantines**.
2. On your ESA, choose **Security Services > Spam Quarantine** and click **Enable External Spam Quarantine**.
3. Point the ESA to the IP address of your SMA and specify the port you would like to use. The default is Port 6025.



External Spam Quarantine Settings

☑ **Enable External Spam Quarantine**

Name: aggies_spam_quarantine
(e.g. spam_quarantine)

IP Address: 14.2.30.104

Port 6025

Safelist/Blocklist: ☑ Enable End User Safelist/Blocklist Feature
Blocklist Action: Quarantine ▾

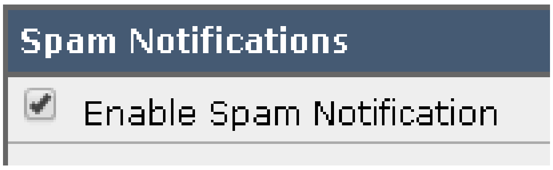
4. Ensure Port 6025 is open from the ESA to the SMA. *This port is for delivery of quarantined messages from ESA > SMA. This can be validated by with a telnet test from the CLI on the ESA on port 6025. If a connection opens and stays open you should be set.*`tarheel.rtp>`

```
telnet 14.2.30.116 6025
Trying 14.2.30.116...
Connected to steelers.rtp.
Escape character is '^]'.
220 steelers.rtp ESMTP
```

5. Ensure you have configured the IP/hostname to access the spam quarantine, such as in "Enable Quarantine Ports and Specify a Quarantine URL at the Interface".
6. Verify that messages arrive to the spam quarantine from your ESAs. If the spam quarantine does not show any messages, there might be an issue with connectivity from ESA > SMA on port 6025 (see previous steps).

Configure Spam Quarantine Notification

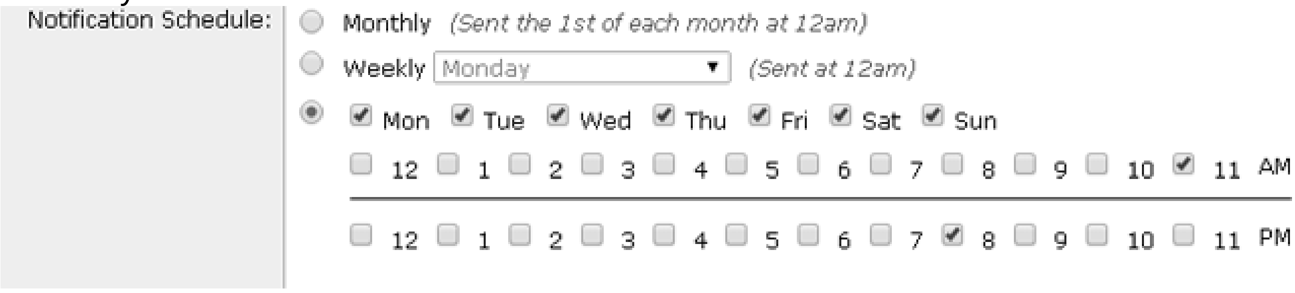
1. On the ESA, choose **Monitor > Spam Quarantine**.
2. On the SMA you would navigate to the Spam Quarantine settings in order to perform the same steps.
3. Click **Spam Quarantine**.
4. Check the **Enable Spam Notification** check box.



Spam Notifications

☑ Enable Spam Notification

5. Choose your notification Schedule.



Notification Schedule:

○ Monthly *(Sent the 1st of each month at 12am)*

○ Weekly Monday ▾ *(Sent at 12am)*

● ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

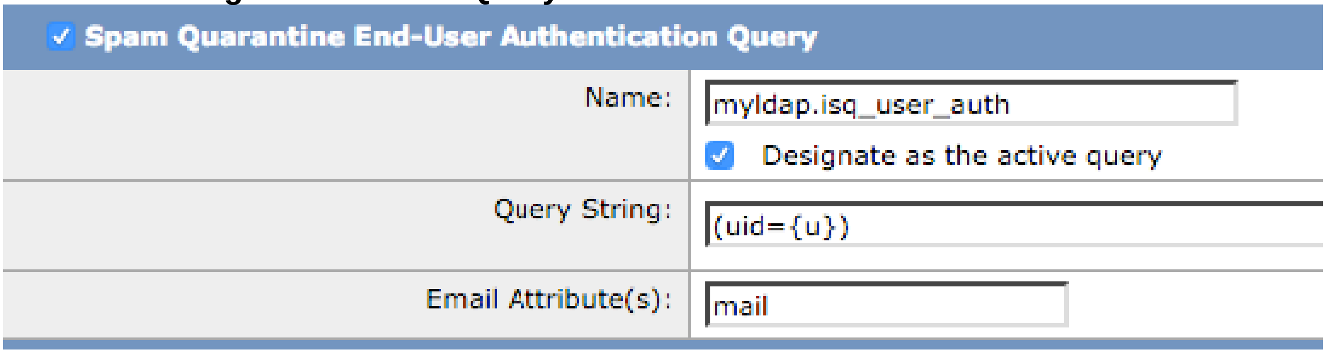
□ 12 □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 ☑ 11 AM

□ 12 □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 ☑ 8 □ 9 □ 10 □ 11 PM

6. Submit and commit changes.

Configure End-User Spam Quarantine Access via Spam Quarantine End-User Authentication Query

1. On the SMA or ESA, choose **System Administration > LDAP**.
2. Open your LDAP Server Profile.
3. In order to verify you are able to authenticate with an Active Directory account, check your Spam Quarantine End-User Authentication Query is enabled.
4. Check the **Designate as Active Query** check box.



☑ Spam Quarantine End-User Authentication Query

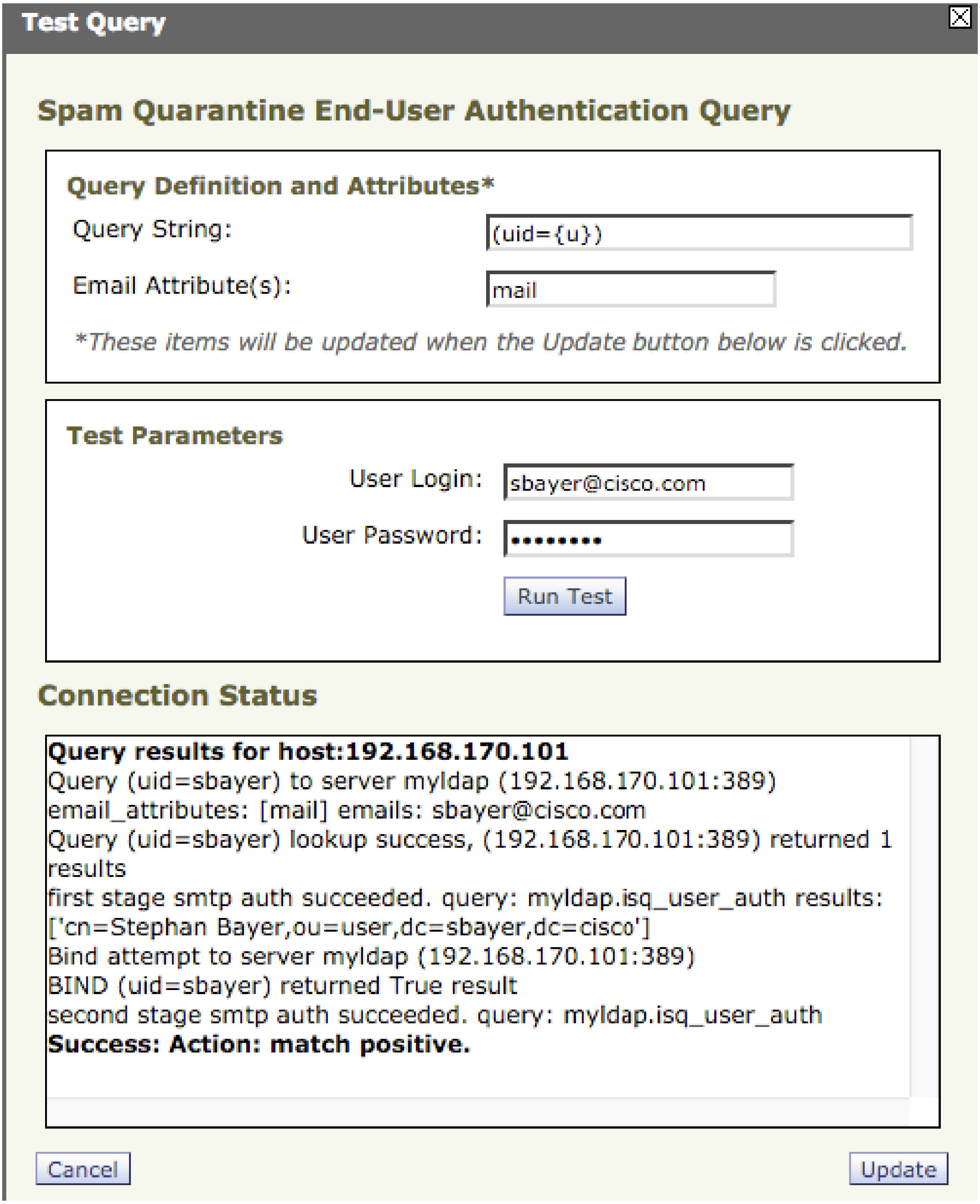
Name: myldap.isq_user_auth

☑ Designate as the active query

Query String: (uid={u})

Email Attribute(s): mail

5. Click **Test** in order to test the query. Match Positive means that the authentication was successful:



Spam Quarantine End-User Authentication Query

Query Definition and Attributes*

Query String: (uid={u})

Email Attribute(s): mail

*These items will be updated when the Update button below is clicked.

Test Parameters

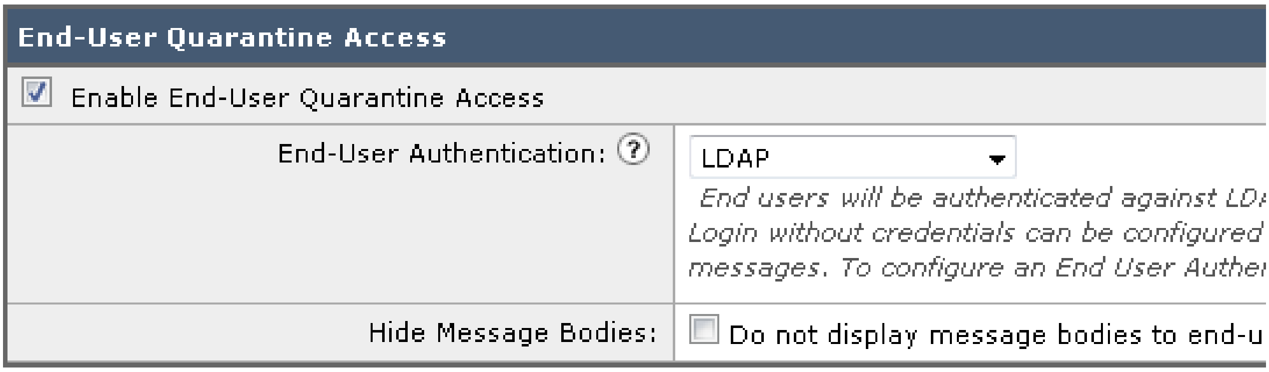
User Login: sbayer@cisco.com

User Password: •••••••••

Connection Status

```
Query results for host:192.168.170.101
Query (uid=sbayer) to server myldap (192.168.170.101:389)
email_attributes: [mail] emails: sbayer@cisco.com
Query (uid=sbayer) lookup success, (192.168.170.101:389) returned 1
results
first stage smtp auth succeeded. query: myldap.isq_user_auth results:
['cn=Stephan Bayer,ou=user,dc=sbayer,dc=cisco']
Bind attempt to server myldap (192.168.170.101:389)
BIND (uid=sbayer) returned True result
second stage smtp auth succeeded. query: myldap.isq_user_auth
Success: Action: match positive.
```

6. Submit and commit changes.
7. On the ESA, choose **Monitor > Spam Quarantine**. On the SMA, navigate to the Spam Quarantine settings in order to perform the same steps.
8. Click **Spam Quarantine**.
9. Check the **Enable End-User Quarantine Access** check box.
10. Choose **LDAP** from the End-User Authentication drop-down list.



End-User Quarantine Access

☑ Enable End-User Quarantine Access

End-User Authentication: LDAP

End users will be authenticated against LD
Login without credentials can be configured
messages. To configure an End User Authe

Hide Message Bodies: □ Do not display message bodies to end-u

11. Submit and commit changes.
12. Validate that External Authentication is on ESA/SMA.
13. Navigate to your URL configured previously in a web browser in order to validate that you can access the quarantine: https://quarantine.mydomain.com:83 https://10.10.10.10:83
14. Log in with your LDAP account. If this fails, check the External authentication LDAP profile and enable End-User Quarantine Access (see previous steps).

Configure Administrative User Access to the Spam Quarantine

Use the procedure in this section in order to allow administrative users with these roles to manage messages in the Spam Quarantine: Operator, Read-Only Operator, Help Desk, or Guestroles, and custom user roles that include access to the Spam Quarantine.

Administrator-level users, which include the default admin user and Email Administrator users, can always access the Spam Quarantine and do not need to be associated with the Spam Quarantine feature using this procedure.

> **Note**: Non-Administrator-level users can access messages in the Spam Quarantine, but they cannot edit the quarantine settings. Administrator-level users can access messages and edit the settings.

In order to enable administrative users who do not have full Administrator privileges to manage messages in the Spam Quarantine, complete these steps:

1. Make sure you have created users and assigned them a user role with access to the Spam Quarantine.
2. On the Security Management appliance, choose **Management Appliance > Centralized Services > Spam Quarantine**.
3. Click **Enable or Edit Settings** in the Spam Quarantine Settings section.
4. In the Administrative Users area of the Spam Quarantine Settings section, click the selection link for Local Users, Externally Authenticated Users, or Custom User Roles.
5. Choose the users to whom you want to grant access to view and manage messages in the Spam Quarantine.
6. Click **OK**.
7. Repeat if needed for each of the other types of Administrative Users listed in the section (Local Users, Externally Authenticated Users, or Custom User Roles).

8. Submit and commit your changes.