Implementierungsleitfaden für die Spam-Quarantäne auf der E-Mail Security Appliance (ESA) und der Security Management Appliance (SMA)

Inhalt

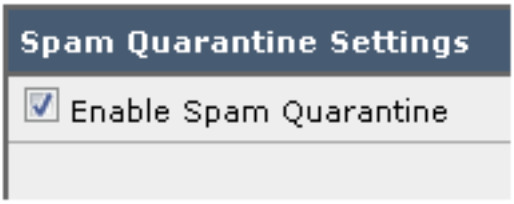
Einführung

In diesem Dokument wird beschrieben, wie Sie die Spam-Quarantäne auf der ESA oder SMA und die zugehörigen Funktionen konfigurieren: Externe Authentifizierung mit LDAP- und Spam-Quarantänenbenachrichtigung.

Vorgehensweise

Lokale Spam-Quarantäne auf der ESA konfigurieren

1. Wählen Sie auf der ESA **Monitor > Spam Quarantine aus**.
2. Aktivieren Sie im Abschnitt Spam-Quarantäneeinstellungen das Kontrollkästchen **Spam-Quarantäne aktivieren**, und legen Sie die gewünschten Quarantäneeinstellungen fest.

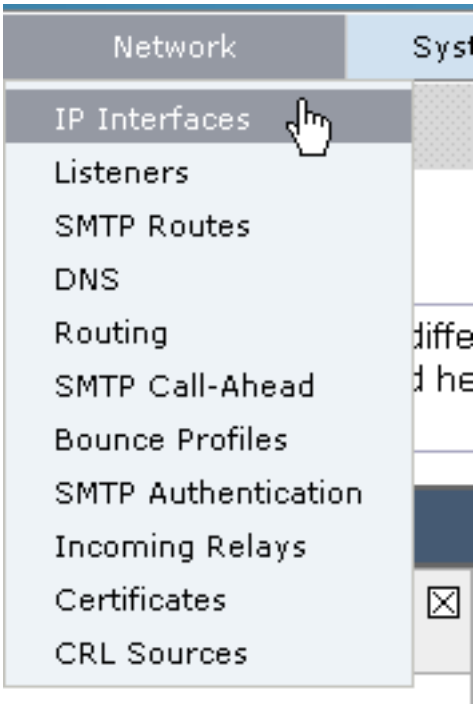


3. Wählen Sie **Sicherheitsdienste > Spam Quarantine aus**.
4. Stellen Sie sicher, dass das Kontrollkästchen **Externe Spam-Quarantäne aktivieren** deaktiviert ist, es sei denn, Sie planen, die externe Spam-Quarantäne zu verwenden (siehe Abschnitt unten).

5. Änderungen senden und bestätigen.

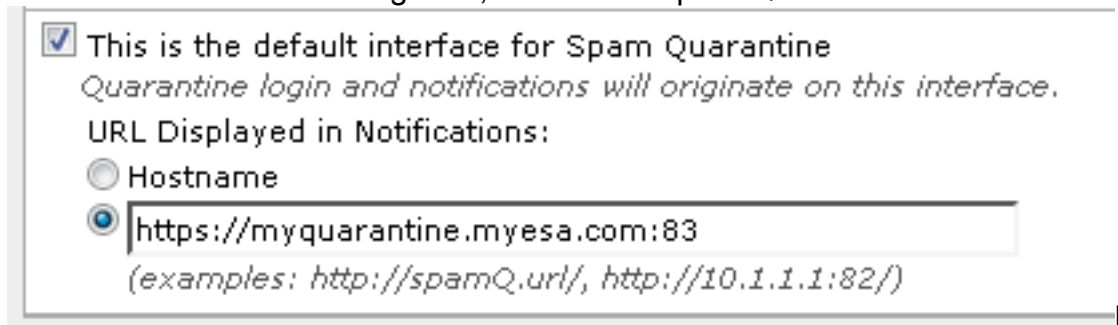
Quarantäne-Ports aktivieren und Quarantäne-URL an der Schnittstelle angeben

1. Wählen Sie **Netzwerk > IP Interfaces (Netzwerk > IP-Schnittstellen)**.



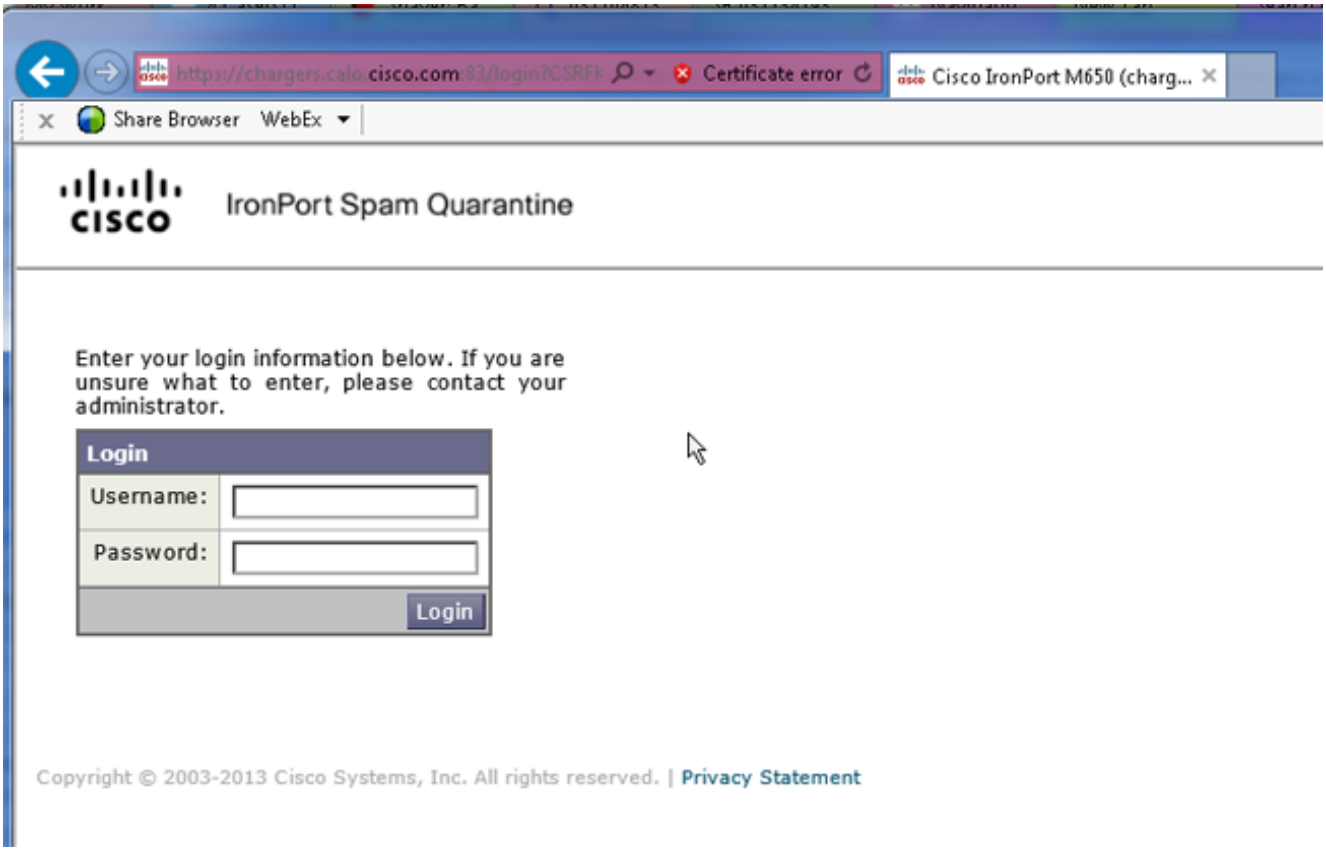
2. Klicken Sie auf den Schnittstellennamen der Schnittstelle, die Sie für den Zugriff auf die Quarantäne verwenden möchten. Aktivieren Sie im Abschnitt "Spam-Quarantäne" die Kontrollkästchen, und geben Sie die Standard-Ports an, oder ändern Sie diese je nach Bedarf:Spam-Quarantäne für HTTPSpam-Quarantäne für HTTPS

3. Aktivieren Sie das Kontrollkästchen **Dies ist die Standardschnittstelle für die Spam-Quarantäne**.
4. Standardmäßig verwendet die Appliance unter "URL in Benachrichtigungen angezeigt" den System-Hostnamen (cli: **sethostname)**, sofern in der zweiten Optionsschaltfläche und im Textfeld nichts anderes angegeben ist. In diesem Beispiel wird die Standardeinstellung für den Hostnamen

angegeben. Sie können eine benutzerdefinierte URL angeben, um auf die Spam-Quarantäne


zuzugreifen. **Hinweis**: Wenn Sie die Quarantäne für den externen Zugriff konfigurieren, benötigen Sie eine auf der Schnittstelle konfigurierte externe IP-Adresse oder eine externe IP-Adresse, die in eine interne IP-Adresse übersetzt ist.Wenn Sie keinen Hostnamen verwenden, können Sie das Optionsfeld Hostname aktivieren, aber trotzdem nur über IP-Adresse auf die Quarantäne zugreifen. Beispiel: https://10.10.10.10:83.

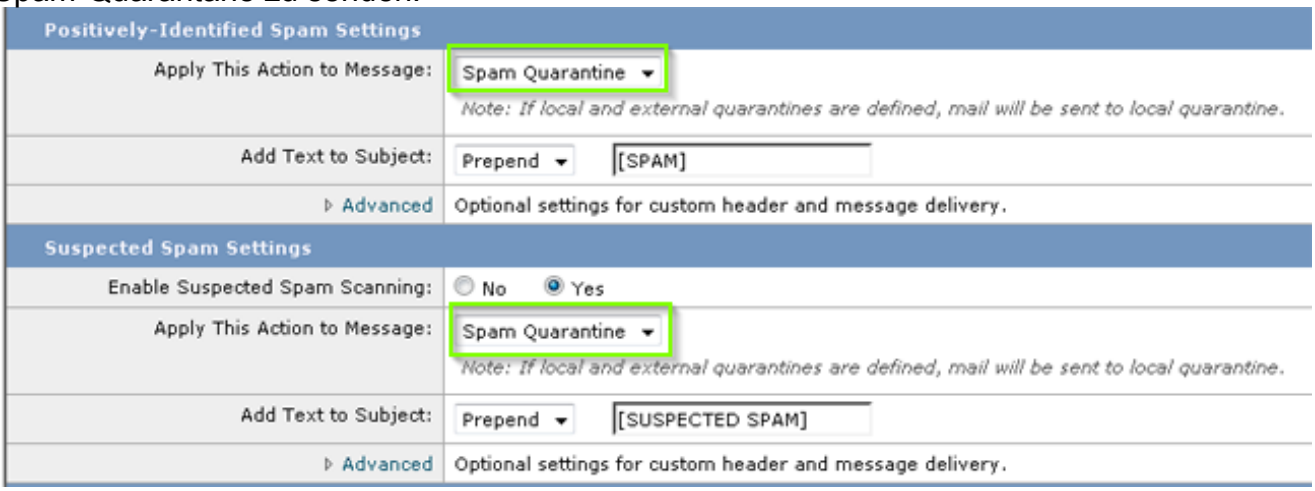
5. Änderungen senden und bestätigen.
6. Validieren. Wenn Sie einen Hostnamen für die Spam-Quarantäne angeben, stellen Sie sicher, dass der Hostname über das interne Domain Name System (DNS) oder einen externen DNS auflösbar ist. DNS löst den Hostnamen in Ihre IP-Adresse auf.Wenn Sie kein Ergebnis erhalten, wenden Sie sich an Ihren Netzwerkadministrator, und greifen Sie wie im vorherigen Beispiel weiter wie im vorherigen Beispiel auf die Quarantäne zu, bis der Host in DNS angezeigt wird.>nslookup quarantäne.mydomain.comNavigieren Sie zu Ihrer zuvor in einem Webbrowser konfigurierten URL, um zu überprüfen, ob Sie auf die Quarantäne zugreifen
können: https://quarantine.mydomain.com:83https://10.10.10.10:83



Konfigurieren der ESA zum Verschieben von Spam und/oder Spam-verdächtigen Nachrichten in die Spam-Quarantäne

Gehen Sie wie folgt vor, um verdächtige Spam- und/oder positiv identifizierte Spam-Nachrichten unter Quarantäne zu stellen:

1. Klicken Sie auf der ESA auf **Mail-Policys > Incoming Mail Policies (E-Mail-Policys > Eingehende Mail-Policys),** und wählen Sie dann die Spalte Anti-Spam für die Standard-Policy (Standard-Policy) aus.
2. Ändern Sie die Aktion von "Positiv Identified Spam" oder "Suspect Spam", um sie an die Spam-Quarantäne zu senden."



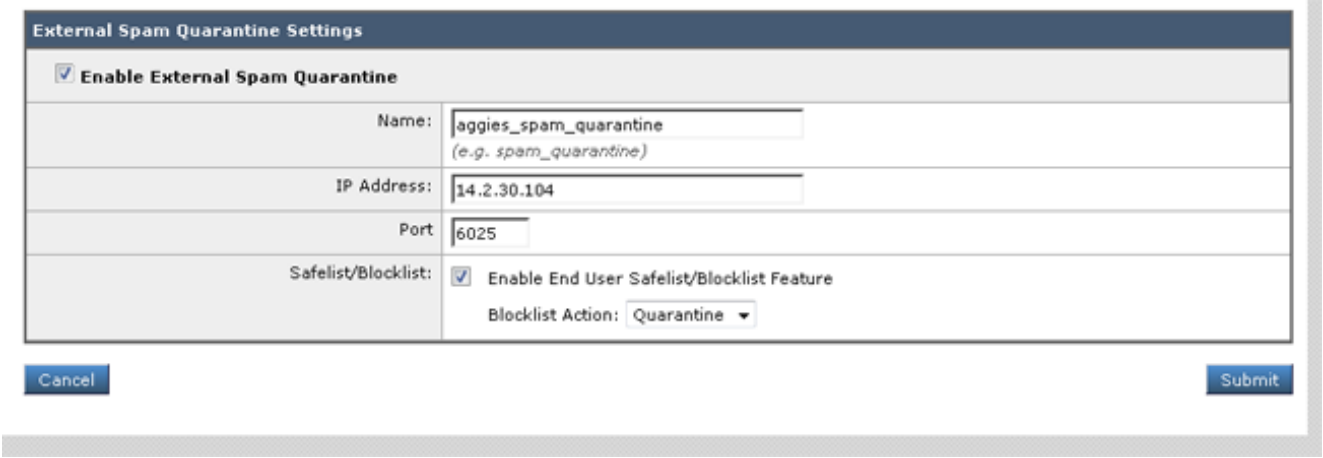
3. Wiederholen Sie den Vorgang für alle anderen ESAs, die Sie möglicherweise für die externe Spam-Quarantäne konfiguriert haben. Wenn Sie diese Änderung auf Cluster-Ebene vorgenommen haben, müssen Sie sie nicht wiederholen, da die Änderung an die anderen Appliances im Cluster weitergeleitet wird.
4. Änderungen senden und bestätigen.

5. An diesem Punkt werden Mails, die ansonsten zugestellt oder verworfen worden wären, unter Quarantäne gestellt.

Konfigurieren Sie die externe Spam-Quarantäne auf der SMA.

Die Schritte zum Konfigurieren der externen Spam-Quarantäne für SMA sind mit einigen Ausnahmen im vorherigen Abschnitt identisch:

1. Auf jeder Ihrer ESA müssen Sie die lokale Quarantäne deaktivieren. Wählen Sie **Monitor > Quarantines aus**.
2. Wählen Sie auf Ihrer ESA **Security Services > Spam Quarantine aus** und klicken Sie auf **Enable External Spam Quarantine**.
3. Zeigen Sie die ESA auf die IP-Adresse Ihrer SMA, und geben Sie den Port an, den Sie verwenden möchten. Der Standardwert ist Port 6025.



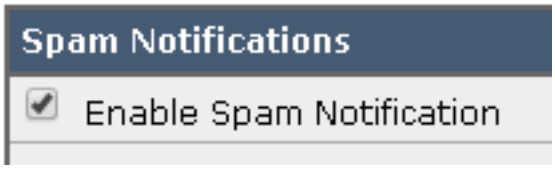
4. Stellen Sie sicher, dass Port 6025 von der ESA zum SMA geöffnet ist. *Dieser Port dient zur Übermittlung von Nachrichten unter Quarantäne von ESA > SMA. Dies kann durch einen Telnet-Test der CLI auf der ESA an Port 6025 validiert werden. Wenn eine Verbindung geöffnet wird und geöffnet bleibt, sollten Sie eingestellt werden.*

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

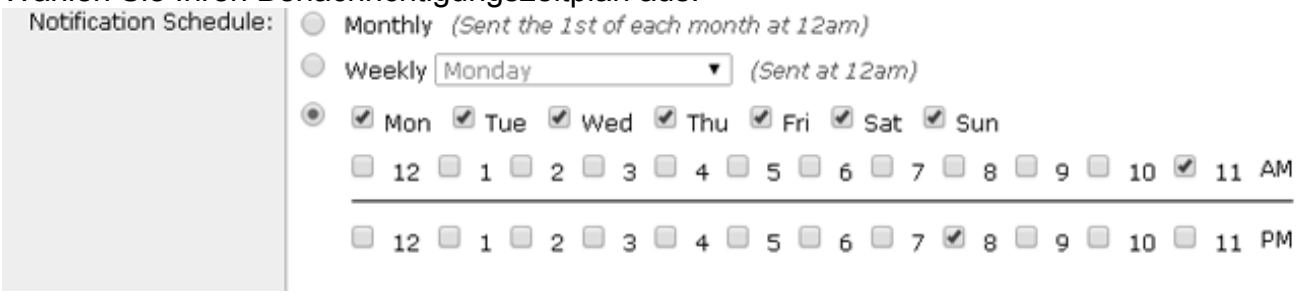
5. Stellen Sie sicher, dass Sie die IP/den Hostnamen für den Zugriff auf die Spam-Quarantäne konfiguriert haben, z. B. unter "Enable Quarantine Ports and Specify a Quarantine URL at the Interface" (Quarantäne-Ports aktivieren und Quarantäne-URL an der Schnittstelle angeben).
6. Überprüfen Sie, ob Nachrichten von Ihren ESAs in die Spam-Quarantäne gelangen. Wenn die Spam-Quarantäne keine Nachrichten anzeigt, kann es auf Port 6025 zu einem Problem mit der Verbindung von ESA > SMA kommen (siehe vorige Schritte).

Spam-Quarantänebenachrichtigung konfigurieren

1. Wählen Sie auf der ESA **Monitor > Spam Quarantine aus**.
2. Auf dem SMA würden Sie zu den Spam-Quarantäne-Einstellungen navigieren, um die gleichen Schritte auszuführen.
3. Klicken Sie auf **Spam Quarantine**.
4. Aktivieren Sie das Kontrollkästchen **Spam-Benachrichtigung aktivieren**.



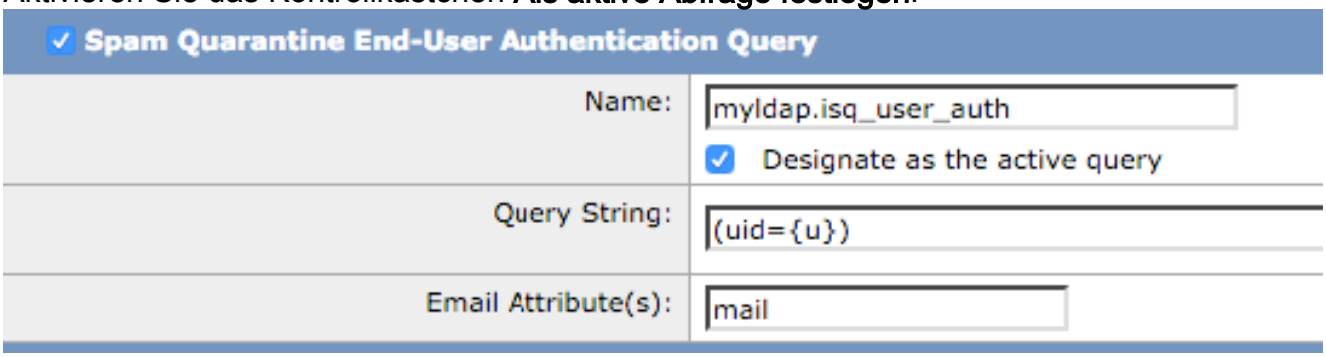
5. Wählen Sie Ihren Benachrichtigungszeitplan aus.



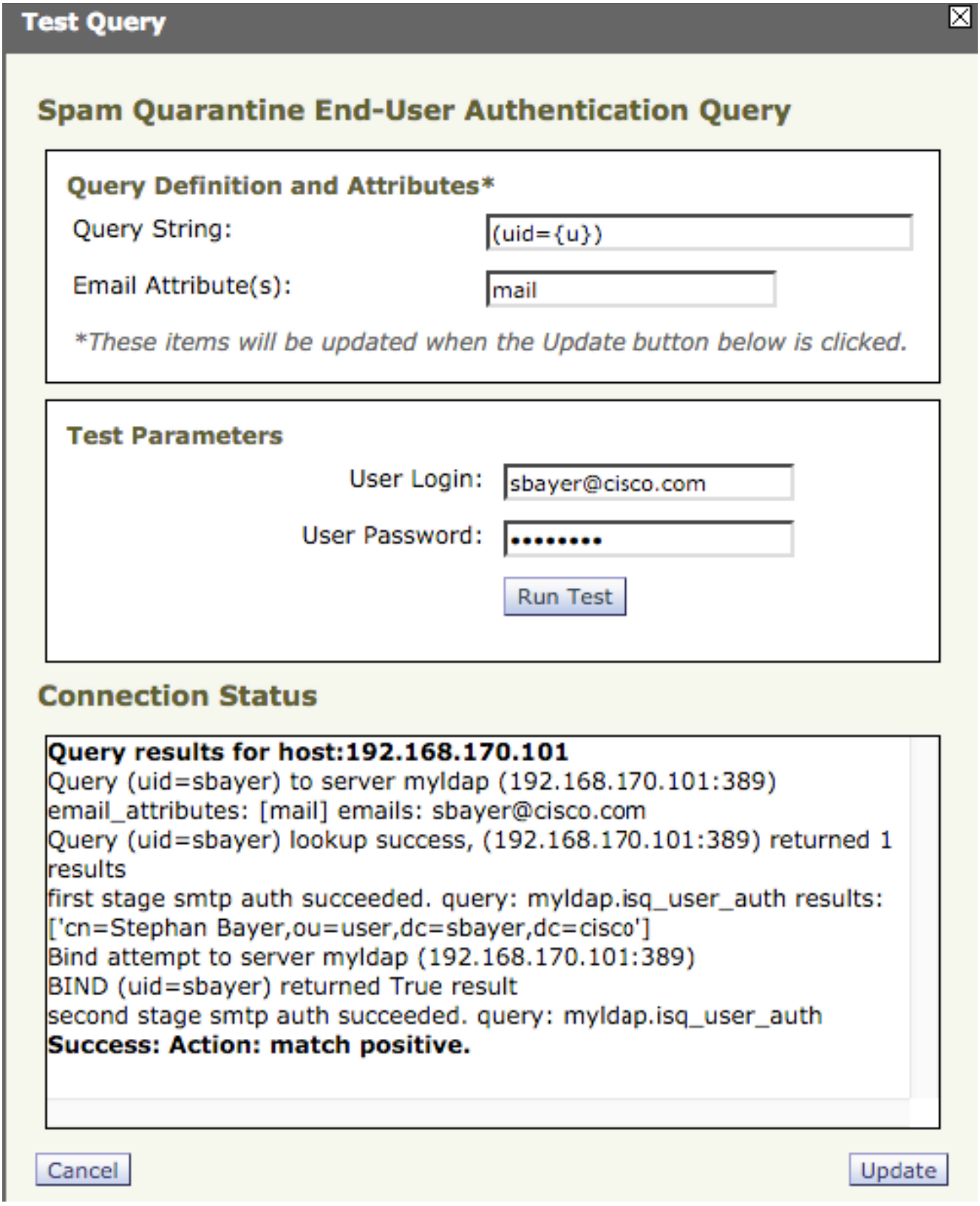
6. Änderungen senden und bestätigen.

Endbenutzer-Spam-Quarantänezugriff über die Endbenutzerauthentifizierungsabfrage für die Spam-Quarantäne konfigurieren

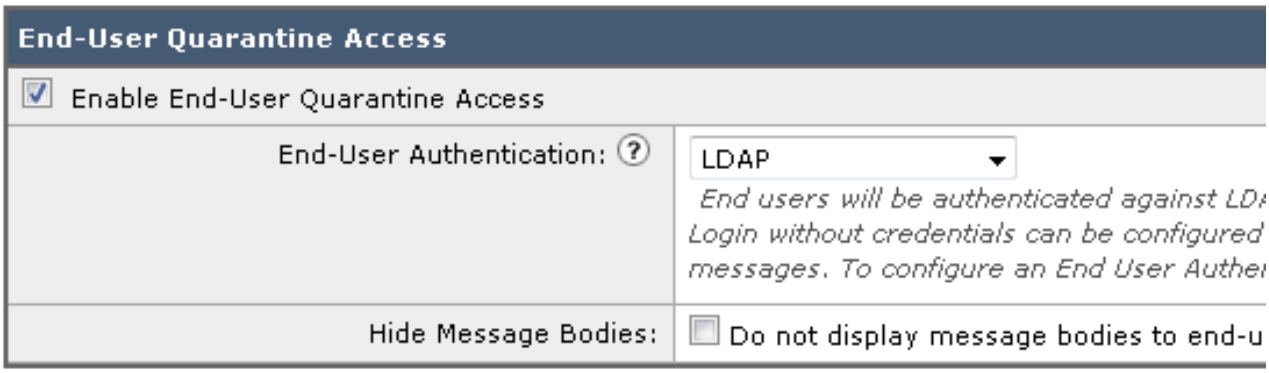
1. Wählen Sie auf dem SMA oder der ESA **Systemverwaltung > LDAP aus**.
2. Öffnen Sie Ihr LDAP-Serverprofil.
3. Um zu überprüfen, ob Sie sich mit einem Active Directory-Konto authentifizieren können, überprüfen Sie, ob die Endbenutzer-Authentifizierungsabfrage für die Spam-Quarantäne aktiviert ist.
4. Aktivieren Sie das Kontrollkästchen **Als aktive Abfrage festlegen**.



5. Klicken Sie auf **Test**, um die Abfrage zu testen. Match Positive bedeutet, dass die Authentifizierung erfolgreich
war:



6. Änderungen senden und bestätigen.
7. Wählen Sie auf der ESA **Monitor > Spam Quarantine aus**. Navigieren Sie auf dem SMA zu den Spam Quarantine-Einstellungen, um die gleichen Schritte auszuführen.
8. Klicken Sie auf **Spam Quarantine**.
9. Aktivieren Sie das Kontrollkästchen **Endbenutzer-Quarantänezugriff aktivieren**.
10. Wählen Sie **LDAP** aus der Dropdown-Liste Endbenutzer-Authentifizierung aus.



11. Änderungen senden und bestätigen.
12. Überprüfen Sie, ob die externe Authentifizierung auf ESA/SMA erfolgt.
13. Navigieren Sie zu Ihrer zuvor in einem Webbrowser konfigurierten URL, um zu überprüfen, ob Sie auf die Quarantäne zugreifen können: https://quarantine.mydomain.com:83 https://10.10.10.10:83
14. Melden Sie sich bei Ihrem LDAP-Konto an. Wenn dies fehlschlägt, überprüfen Sie das LDAP-Profil für die externe Authentifizierung, und aktivieren Sie den Quarantänezugriff für Endbenutzer (siehe vorherige Schritte).

Konfigurieren des administrativen Benutzerzugriffs auf die Spam-Quarantäne

Mit der Vorgehensweise in diesem Abschnitt können Administratoren mit diesen Rollen Nachrichten in der Spam-Quarantäne verwalten: Operator, schreibgeschützter Operator, Helpdesk oder Gastrollen sowie benutzerdefinierte Benutzerrollen, die Zugriff auf die Spam-Quarantäne enthalten.

Benutzer auf Administrator-Ebene, zu denen der Standard-Administrator und der E-Mail-Administrator gehören, können jederzeit auf die Spam-Quarantäne zugreifen und müssen mit diesem Verfahren nicht mit der Spam-Quarantäne-Funktion verknüpft werden.

> **Hinweis**: Benutzer, die nicht auf Administrator-Ebene sind, können zwar auf Nachrichten in der Spam-Quarantäne zugreifen, die Quarantäneeinstellungen jedoch nicht bearbeiten. Benutzer auf Administrator-Ebene können auf Nachrichten zugreifen und die Einstellungen bearbeiten.

Gehen Sie wie folgt vor, um Administratorbenutzer zu aktivieren, die nicht über volle Administratorrechte verfügen, um Nachrichten in der Spam-Quarantäne zu verwalten:

1. Stellen Sie sicher, dass Sie Benutzer erstellt und ihnen eine Benutzerrolle mit Zugriff auf die Spam-Quarantäne zugewiesen haben.
2. Wählen Sie auf der Security Management Appliance **Management Appliance > Centralized Services > Spam Quarantine aus**.
3. Klicken Sie im Bereich "Spam Quarantine Settings" auf **Einstellungen aktivieren oder bearbeiten**.
4. Klicken Sie im Bereich "Administrator Users" (Verwaltung) des Abschnitts "Spam Quarantine-Einstellungen" auf den Auswahllink für Lokale Benutzer, Extern authentifizierte Benutzer oder Benutzerrollen.
5. Wählen Sie die Benutzer aus, denen Sie Zugriff gewähren möchten, um Nachrichten in der

Spam-Quarantäne anzuzeigen und zu verwalten.
6. Klicken Sie auf **OK**.
7. Wiederholen Sie diese Schritte ggf. für die anderen im Abschnitt aufgeführten Benutzertypen (Lokale Benutzer, extern authentifizierte Benutzer oder benutzerdefinierte Benutzerrollen).
8. Senden und bestätigen Sie Ihre Änderungen.