郵件安全裝置(ESA)和安全管理裝置(SMA)上的綜合垃圾郵件隔離區設定指南

目錄

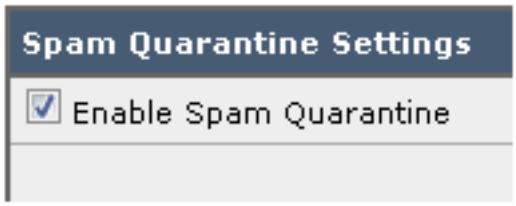
簡介

本文檔介紹如何在ESA或SMA上配置垃圾郵件隔離區及相關功能：使用LDAP和垃圾郵件隔離通知進行外部身份驗證。

程式

在ESA上配置本地垃圾郵件隔離區

1. 在ESA上，選擇**Monitor > Spam Quarantine**。
2. 在Spam Quarantine Settings部分，選中**Enable Spam Quarantine**覈取方塊並設定所需的隔離設定。

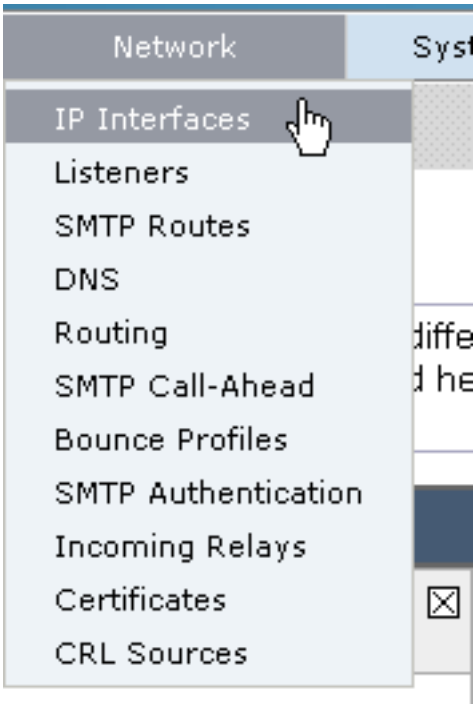


3. 選擇**Security Services > Spam Quarantine**。
4. 確保取消選中**啟用外部垃圾郵件隔離**覈取方塊，除非您計畫使用外部垃圾郵件隔離（請參閱下面的部分）。

5. 提交和提交更改。

在介面上啟用隔離埠並指定隔離URL

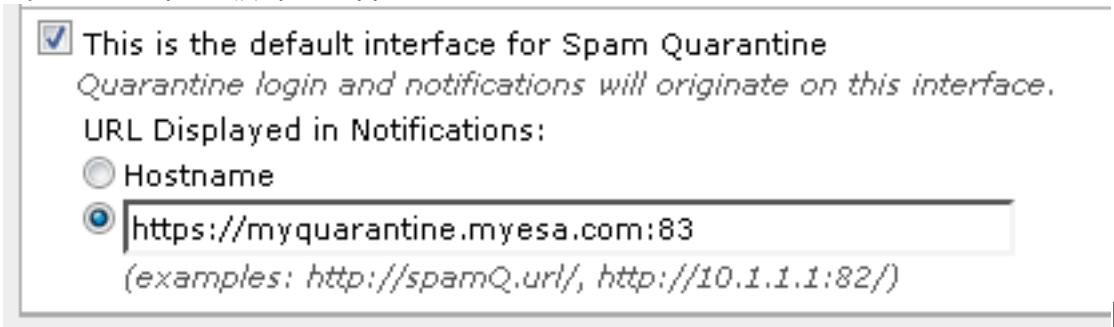
1. 選擇**Network > IP Interfaces**。



2. 按一下將用於訪問隔離區的介面的介面名稱。 在垃圾郵件隔離區部分，選中覈取方塊，然後指定預設埠或根據需要進行更改：垃圾郵件隔離區HTTP垃圾郵件隔離區HTTPS

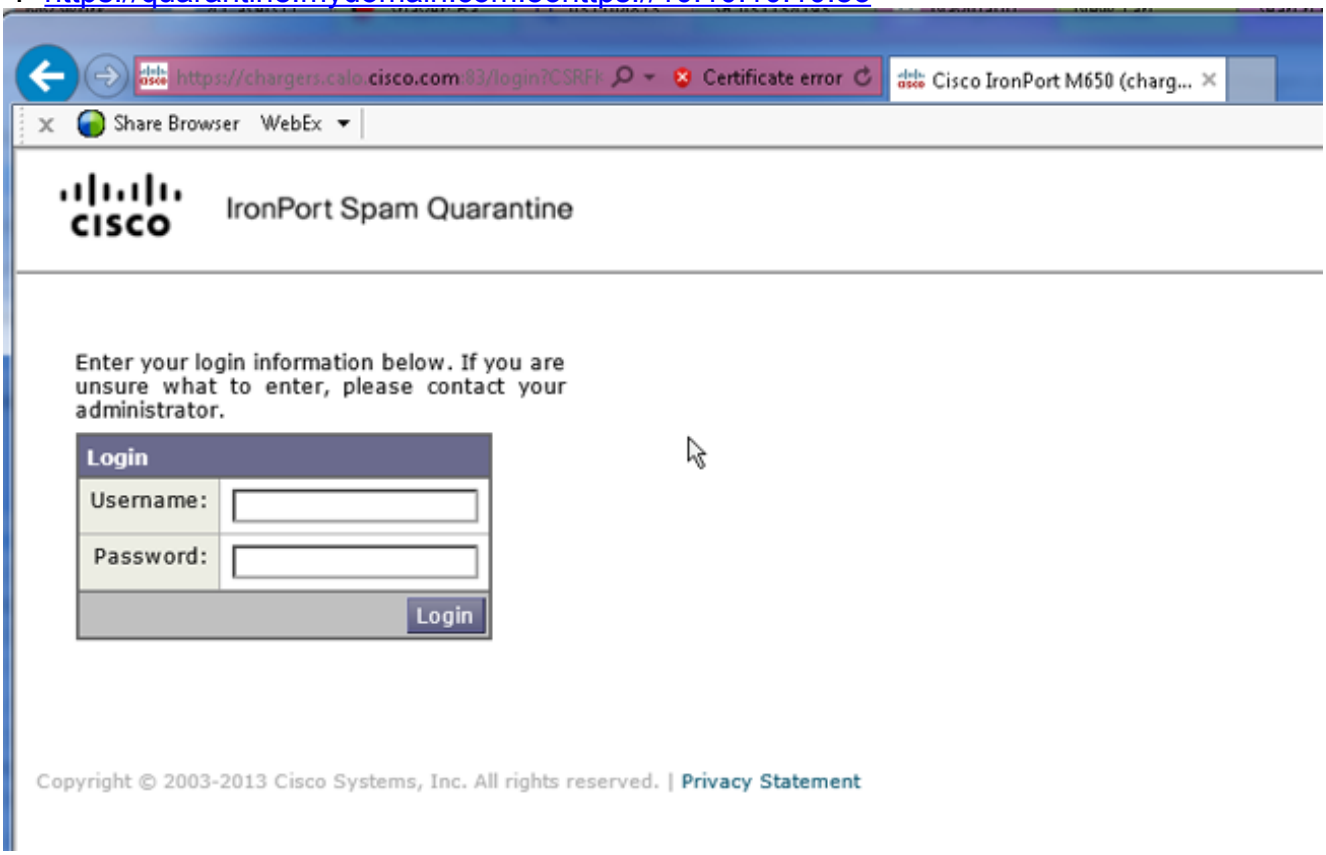
3. 選中**This is the default interface for Spam Quarantine**覈取方塊。
4. 在「通知中顯示的URL」下，裝置預設使用系統主機名(cli: **sethostname)**，除非第二個單選按鈕選項和文本欄位中另外指定。 此示例指定預設主機名設定。

您可以指定自定義URL以訪問垃圾郵件隔離區。



附註：如果為外部訪問配置隔離區，則需要在介面上配置外部IP地址或將網路地址轉換為內部IP的外部IP。如果不使用主機名，則可以保持選中「主機名」單選按鈕，但仍只能通過IP地址訪問隔離區。例如，https://10.10.10.10:83。

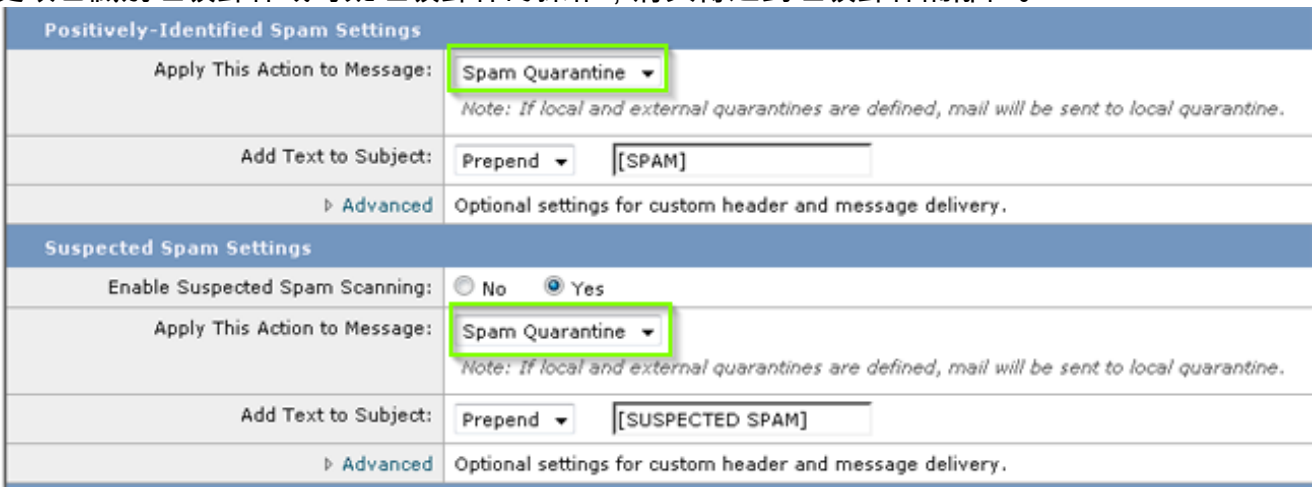
5. 提交和提交更改。
6. 驗證。 如果為垃圾郵件隔離區指定主機名，請確保可以通過內部域名系統(DNS)或外部DNS解析主機名。DNS會將主機名解析為IP地址。如果您沒有獲得結果，請諮詢網路管理員，然後繼續像上例一樣訪問通過IP地址隔離，直到主機出現在DNS中。>nslookup quarantine.mydomain.com導航到先前在Web瀏覽器中配置的URL，以驗證是否可以訪問隔離區
：https://quarantine.mydomain.com:83https://10.10.10.10:83



將ESA配置為將陽性垃圾郵件和/或可疑垃圾郵件移動到垃圾郵件隔離區

若要隔離可疑垃圾郵件和/或識別為肯定垃圾郵件，請完成以下步驟：

1. 在ESA上，按一下**Mail Policies > Incoming Mail Policies**，然後按一下Default Policy的反垃圾郵件列。
2. 更改已識別垃圾郵件或可疑垃圾郵件的操作，將其傳送到垃圾郵件隔離區。



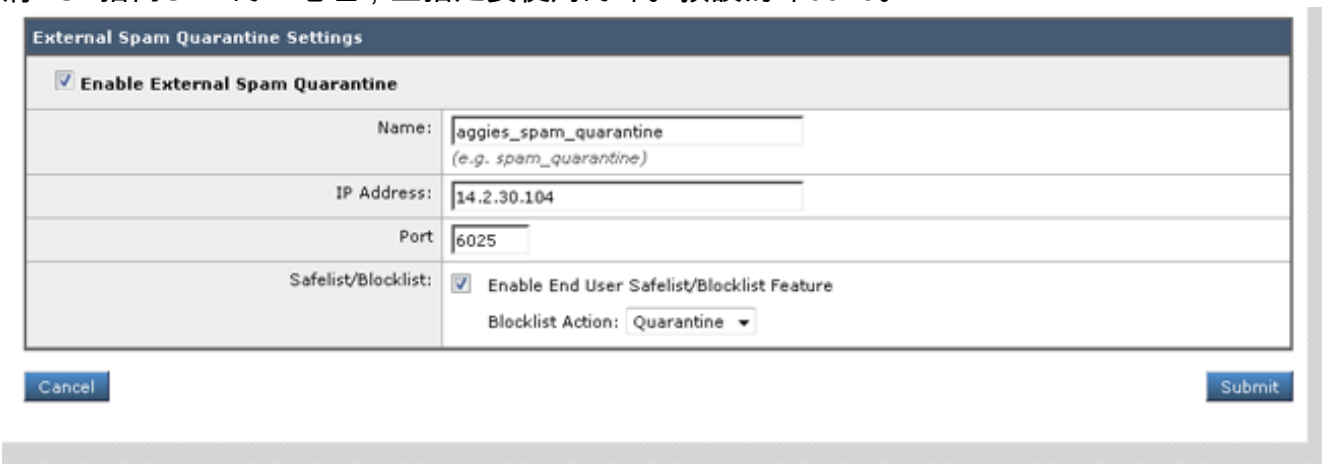
3. 對您可能為外部垃圾郵件隔離區配置的任何其他ESA重複此過程。如果在群集級別進行了此更

改，則不必重複此更改，因為更改將傳播到群集中的其他裝置。
4. 提交和提交更改。
5. 此時，本應已送達或已丟棄的郵件將被隔離。

在SMA上配置外部垃圾郵件隔離區

在SMA上配置外部垃圾郵件隔離區的步驟與上一節相同，但有一些例外：

1. 在每個ESA上，您需要禁用本地隔離。選擇**Monitor > Quarantines**。
2. 在ESA上，選擇**Security Services > Spam Quarantine**，然後按一下**Enable External Spam Quarantine**。
3. 將ESA指向SMA的IP地址，並指定要使用的埠。預設為埠6025。



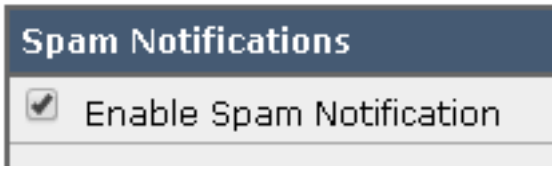
4. 確保從ESA到SMA開啟埠6025。*此埠用於傳遞來自ESA > SMA的隔離郵件。 可以通過從ESA埠6025上的CLI使用telnet測試來驗證這一點。如果連線開啟並且保持開啟狀態，則應該進行設定。*

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

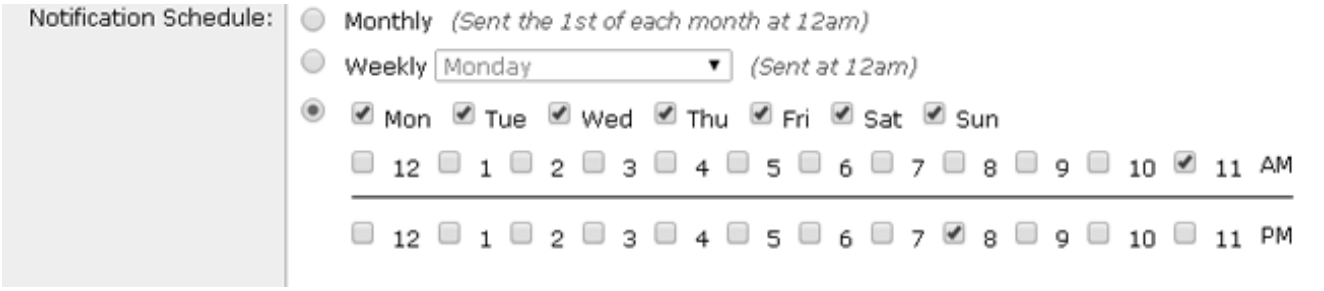
5. 確保已配置IP/主機名以訪問垃圾郵件隔離區，如在「啟用隔離區埠並在介面上指定隔離URL」中。
6. 驗證郵件是否從您的ESA到達垃圾郵件隔離區。如果垃圾郵件隔離區未顯示任何郵件，則埠6025上來自ESA > SMA的連線可能存在問題（請參閱前面的步驟）。

配置垃圾郵件隔離區通知

1. 在ESA上，選擇**Monitor > Spam Quarantine**。
2. 在SMA上，您可以導航到垃圾郵件隔離區設定，以便執行相同的步驟。
3. 按一下**Spam Quarantine**。
4. 選中**Enable Spam Notification**覈取方塊。



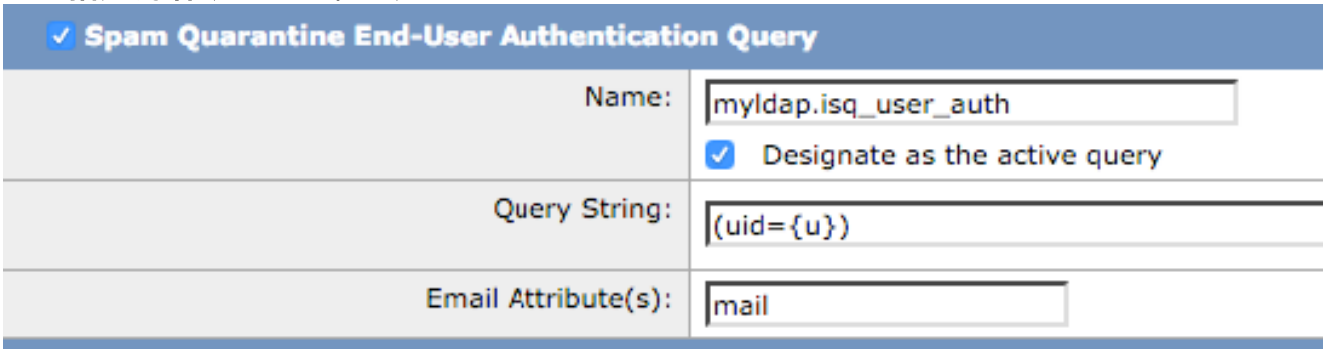
5. 選擇通知計畫。



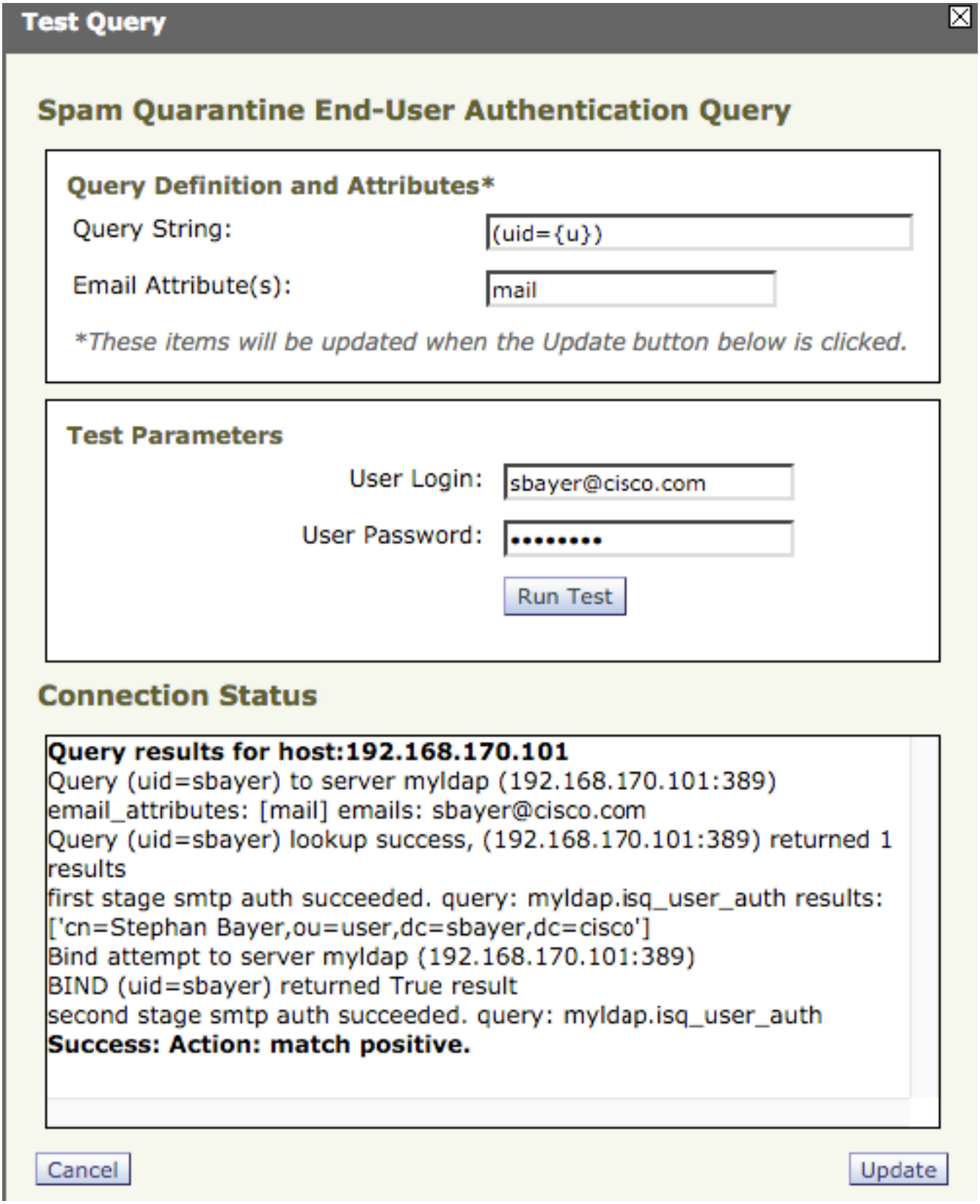
6. 提交和提交更改。

通過垃圾郵件隔離區終端使用者身份驗證查詢配置終端使用者垃圾郵件隔離區訪問

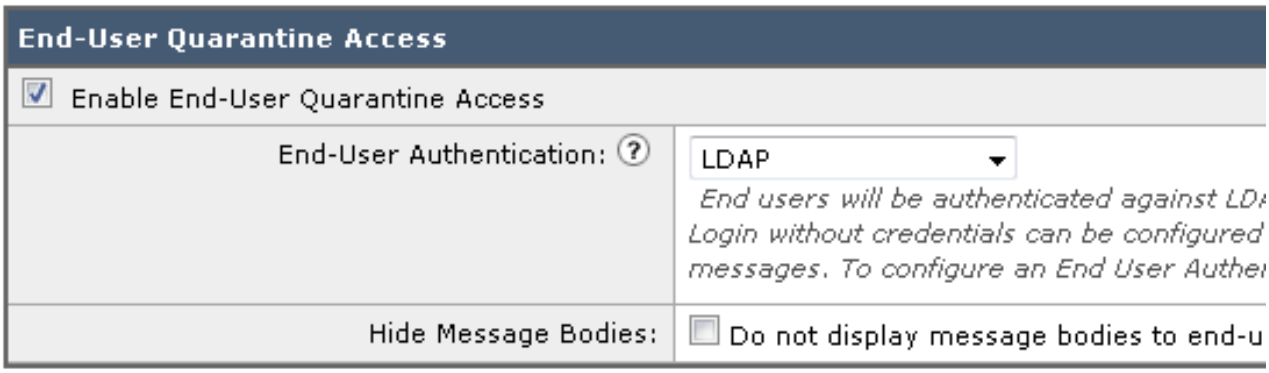
1. 在SMA或ESA上，選擇**System Administration > LDAP**。
2. 開啟LDAP伺服器配置檔案。
3. 若要驗證您能否使用Active Directory帳戶進行身份驗證，請檢查是否啟用垃圾郵件隔離區終端使用者身份驗證查詢。
4. 選中**指定為活動查**詢覈取方塊。



5. 按一下**測試**以測試查詢。 Match Positive表示驗證成功
：



6. 提交和提交更改。
7. 在ESA上，選擇**Monitor > Spam Quarantine**。 在SMA上，導航到垃圾郵件隔離區設定，以便執行相同步驟。
8. 按一下**Spam Quarantine**。
9. 選中**Enable End-User Quarantine Access**覈取方塊。
10. 從End-User Authentication下拉選單中選擇**LDAP**。



11. 提交和提交更改。
12. 驗證外部身份驗證是否在ESA/SMA上。
13. 導航到先前在Web瀏覽器中配置的URL，以驗證是否可訪問隔離區：
    https://quarantine.mydomain.com:83
    https://10.10.10.10:83
14. 使用您的LDAP帳戶登入。如果失敗，請檢查外部身份驗證LDAP配置檔案並啟用終端使用者隔離訪問（請參閱前面的步驟）。

配置對垃圾郵件隔離區的管理使用者訪問許可權

使用本節中的步驟可允許具有這些角色的管理使用者管理垃圾郵件隔離區中的郵件：操作員、只讀操作員、服務檯或訪客角色以及包含垃圾郵件隔離區訪問許可權的自定義使用者角色。

管理員級使用者（包括預設管理員使用者和電子郵件管理員使用者）始終可以訪問垃圾郵件隔離區，無需使用此過程與垃圾郵件隔離區功能相關聯。

> **附註**：非管理員級使用者可以訪問垃圾郵件隔離區中的郵件，但不能編輯隔離區設定。管理員級使用者可以訪問消息並編輯設定。

要使沒有完全管理員許可權的管理使用者能夠管理垃圾郵件隔離區中的郵件，請完成以下步驟：

1. 確保您已建立使用者並為其分配具有垃圾郵件隔離區訪問許可權的使用者角色。
2. 在安全管理裝置上，選擇**管理裝置>集中服務>垃圾郵件隔離區**。
3. 按一下「垃圾郵件隔離區設定」部分中的**啟用或編輯設定**。
4. 在「垃圾郵件隔離區設定」部分的「管理使用者」區域中，按一下「本地使用者」、「外部身份驗證使用者」或「自定義使用者角色」的選擇連結。
5. 選擇要授予其訪問許可權的使用者，以檢視和管理垃圾郵件隔離區中的郵件。
6. 按一下「OK」（確定）。
7. 如果需要，請為部分中列出的其他型別的管理使用者（本地使用者、外部身份驗證使用者或自定義使用者角色）重複此操作。
8. 提交並提交更改。