ESA(Email Security Appliance) 및 SMA(Security Management Appliance)에 대한 포괄적인 스팸 격리 설정 가이드

목차

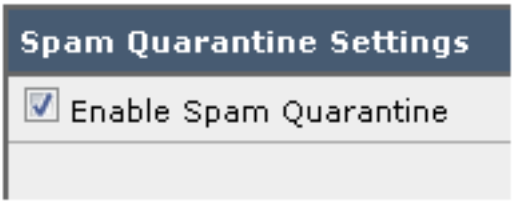
소개

이 문서에서는 ESA 또는 SMA에서 스팸 격리를 구성하는 방법과 관련 기능에 대해 설명합니다 .LDAP 및 스팸 격리 알림을 통한 외부 인증

절차

ESA에서 로컬 스팸 격리 구성

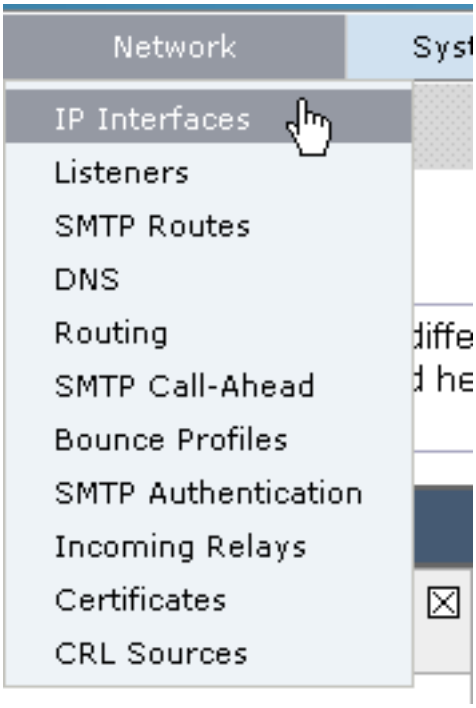
1. ESA에서 Monitor(모니터링) **> Spam Quarantine(스팸 격리)을** 선택합니다.
2. Spam Quarantine Settings(스팸 격리 설정) 섹션에서 **Enable Spam Quarantine(스팸 격리 활성화**) 확인란을 선택하고 원하는 격리 설정을 설정합니다.



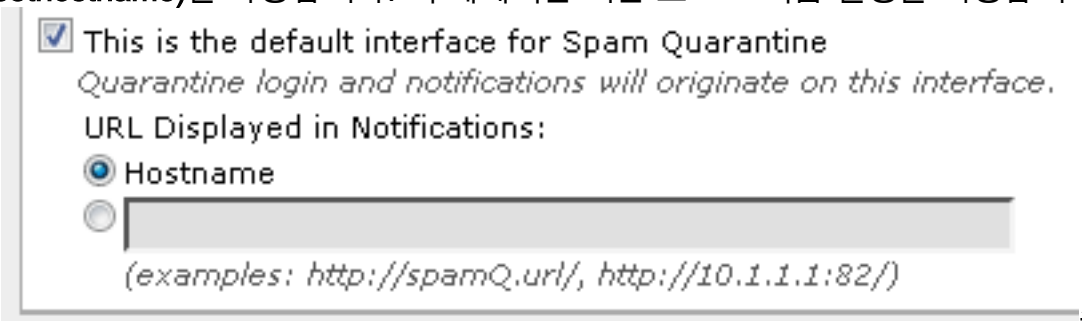
3. Security **Services(보안 서비스) > Spam Quarantine(스팸 격리)을 선택합니다**.
4. External Spam **Quarantine(외부 스팸 격리**)을 사용하려는 경우가 아니면 Enable External Spam Quarantine(외부 스팸 격리 활성화) 확인란을 선택하지 않았는지 확인합니다(아래 섹션 참조).

5. 변경 사항을 제출하고 커밋합니다.

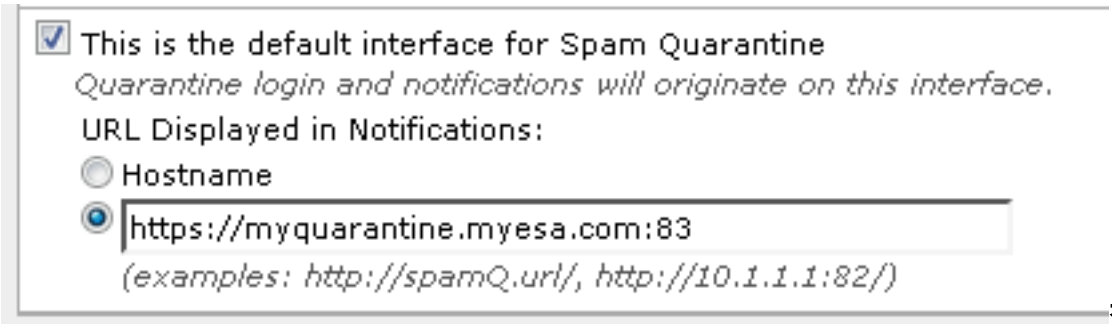
격리 포트 활성화 및 인터페이스에서 격리 URL 지정

1. Network **> IP Interfaces를 선택합니다**.


2. 격리에 액세스하기 위해 사용할 인터페이스의 인터페이스 이름을 클릭합니다. 스팸 격리 섹션에서 확인란을 선택하고 기본 포트를 지정하거나 필요에 따라 변경합니다.스팸 쿼런틴 HTTP스팸 쿼런틴 HTTPS

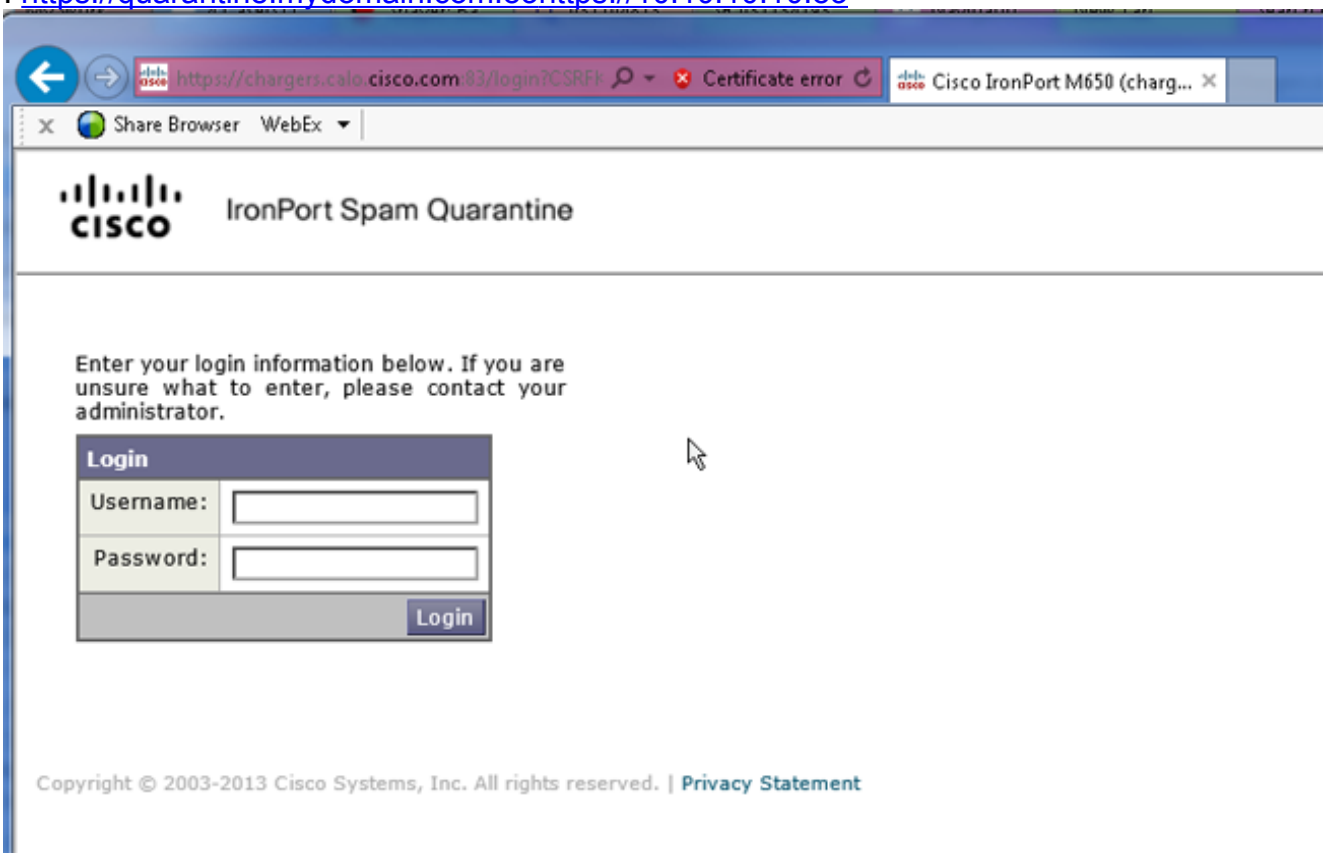

3. This **is the default interface for Spam Quarantine** 확인란**을** 선택합니다.
4. "URL Displayed in Notifications(알림에 표시되는 URL)"에서 어플라이언스는 두 번째 라디오 버튼 옵션 및 텍스트 필드에 달리 지정되지 않는 한 기본적으로 시스템 호스트 이름(cli: **sethostname)**을 사용합니다. 이 예에서는 기본 호스트 이름 설정을 지정합니다


. 스팸 격리에 액세스하기 위해 사용자 지정 URL을 지정할 수 있습니다



참고:외부 액세스를 위한 격리를 구성하는 경우 인터페이스에 구성된 외부 IP 주소 또는 내부 IP로 변환된 네트워크 주소인 외부 IP가 필요합니다.호스트 이름을 사용하지 않을 경우 Hostname 라디오 버튼을 선택할 수 있지만 여전히 IP 주소로만 격리에 액세스할 수 있습니다.예: https://10.10.10.10:83입니다.

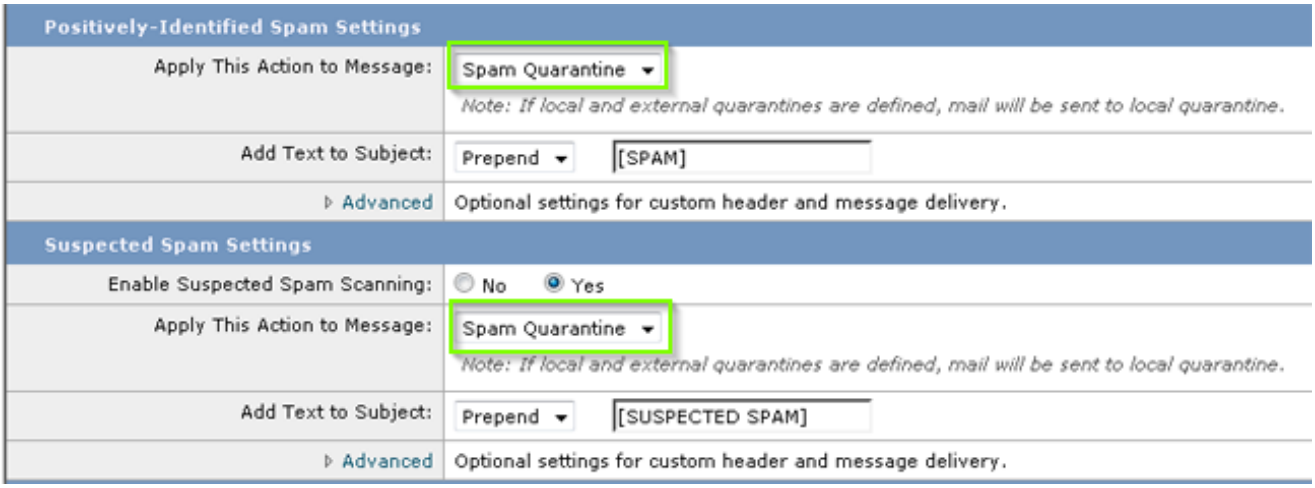
5. 변경 사항을 제출하고 커밋합니다.
6. 검증. 스팸 격리에 대한 호스트 이름을 지정하는 경우 내부 DNS(Domain Name System) 또는 외부 DNS를 통해 호스트 이름을 확인할 수 있는지 확인합니다.DNS는 호스트 이름을 IP 주소로 확인합니다.결과를 얻지 못한 경우 네트워크 관리자에게 문의하여 호스트가 DNS에 나타날 때까지 이전 예와 같이 IP 주소로 쿼런틴에 계속 액세스합니다.>nslookup quarantine.mydomain.com격리에 액세스할 수 있는지 확인하기 위해 이전에 웹 브라우저에서 구성한 URL로 이동합니다
. https://quarantine.mydomain.com:83https://10.10.10.10:83



ESA를 구성하여 스팸 판정 및/또는 의심스런 스팸을 스팸 격리로 이동

의심되는 스팸 및/또는 양성으로 식별된 스팸 메시지를 격리하려면 다음 단계를 완료하십시오.

1. ESA에서 **Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)**를 클릭한 다음 Default Policy(기본 정책)에 대한 안티스팸 열을 클릭합니다.
2. 스팸 격리로 전송할 Positively Identified Spam 또는 Suspect Spam의 작업을 변경합니다."

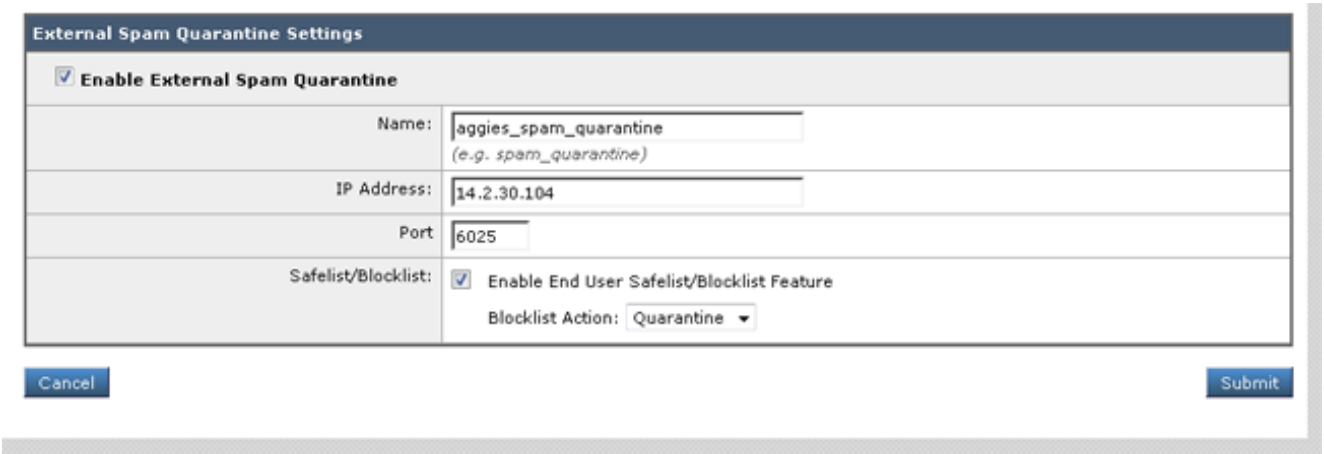


3. 외부 스팸 격리에 대해 구성한 다른 ESA에 대해 이 프로세스를 반복합니다.클러스터 레벨에서 이 변경 사항을 적용한 경우 변경 사항이 클러스터의 다른 어플라이언스에 전달되므로 이 변경을 반복할 필요가 없습니다.
4. 변경 사항을 제출하고 커밋합니다.
5. 이 시점에서 전달되거나 삭제되었을 메일은 격리됩니다.

SMA에서 외부 스팸 격리 구성

SMA에서 외부 스팸 쿼런틴을 구성하는 단계는 몇 가지 예외를 제외하고 이전 섹션과 동일합니다.

1. 각 ESA에서 로컬 격리를 비활성화해야 합니다.Monitor(**모니터) > Quarantines(격리)를 선택합니다**.
2. ESA에서 **Security Services(보안 서비스) > Spam Quarantine(스팸 격리)을** 선택하고 **Enable External Spam Quarantine(외부 스팸 격리 활성화)**을 클릭합니다.
3. ESA를 SMA의 IP 주소로 가리키고 사용할 포트를 지정합니다.기본값은 Port 6025입니다.



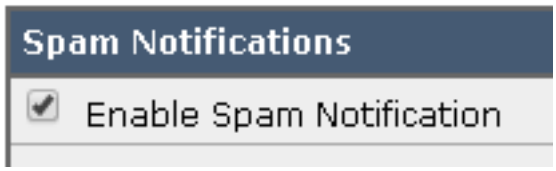
4. 포트 6025가 ESA에서 SMA로 열려 있는지 확인합니다. *이 포트는 ESA > SMA에서 격리된 메시지를 전달하기 위한 것입니다. 이는 포트 6025의 ESA에서 CLI에서 텔넷 테스트를 통해 확인할 수 있습니다.연결이 열리고 열린 상태로 유지되면 설정해야 합니다.*

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

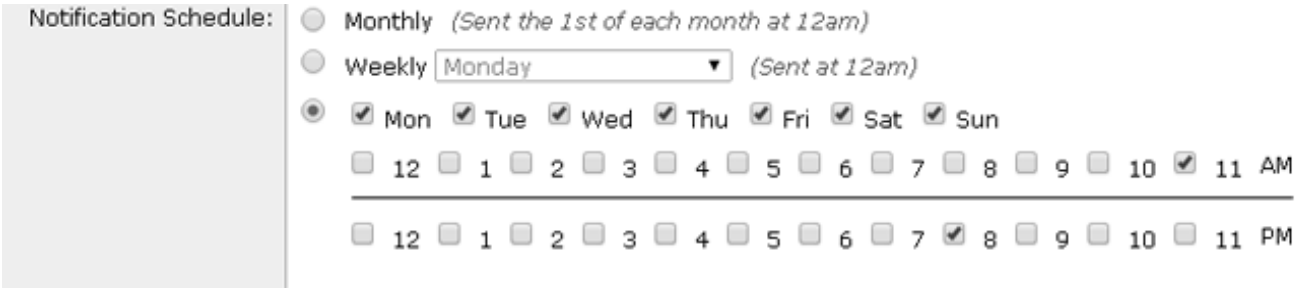
5. "Enable Quarantine Ports and Specify a Quarantine URL at the Interface"와 같이 스팸 격리에 액세스하도록 IP/호스트 이름을 구성했는지 확인합니다.
6. 메시지가 ESA에서 스팸 격리에 도착하는지 확인합니다.스팸 격리에 메시지가 표시되지 않으면 포트 6025에서 ESA > SMA의 연결에 문제가 발생할 수 있습니다(이전 단계 참조).

스팸 격리 알림 구성

1. ESA에서 Monitor(모니터링) **> Spam Quarantine(스팸 격리)을** 선택합니다.
2. SMA에서 Spam Quarantine(스팸 격리) 설정으로 이동하여 동일한 단계를 수행합니다.
3. Spam **Quarantine(스팸 격리)을 클릭합니다**.
4. Enable **Spam Notification** 확인란을 선택합니다.



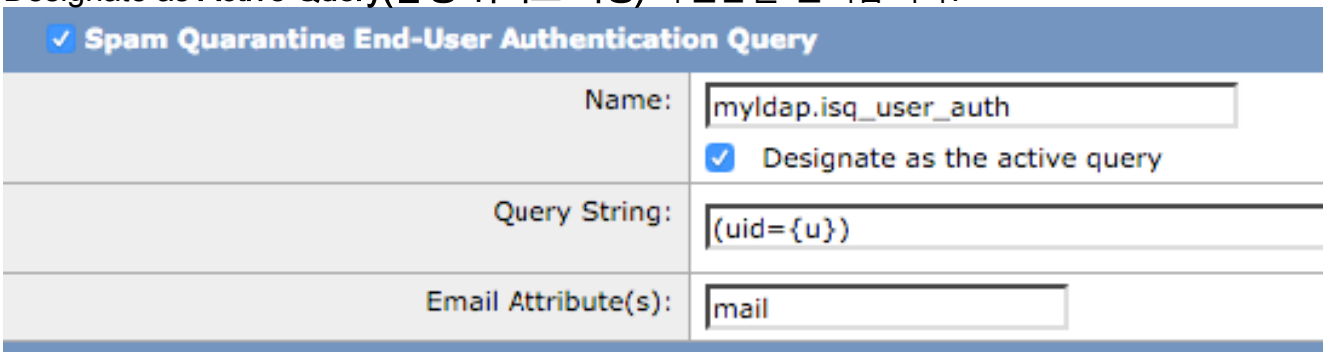
5. 알림 일정을 선택합니다.



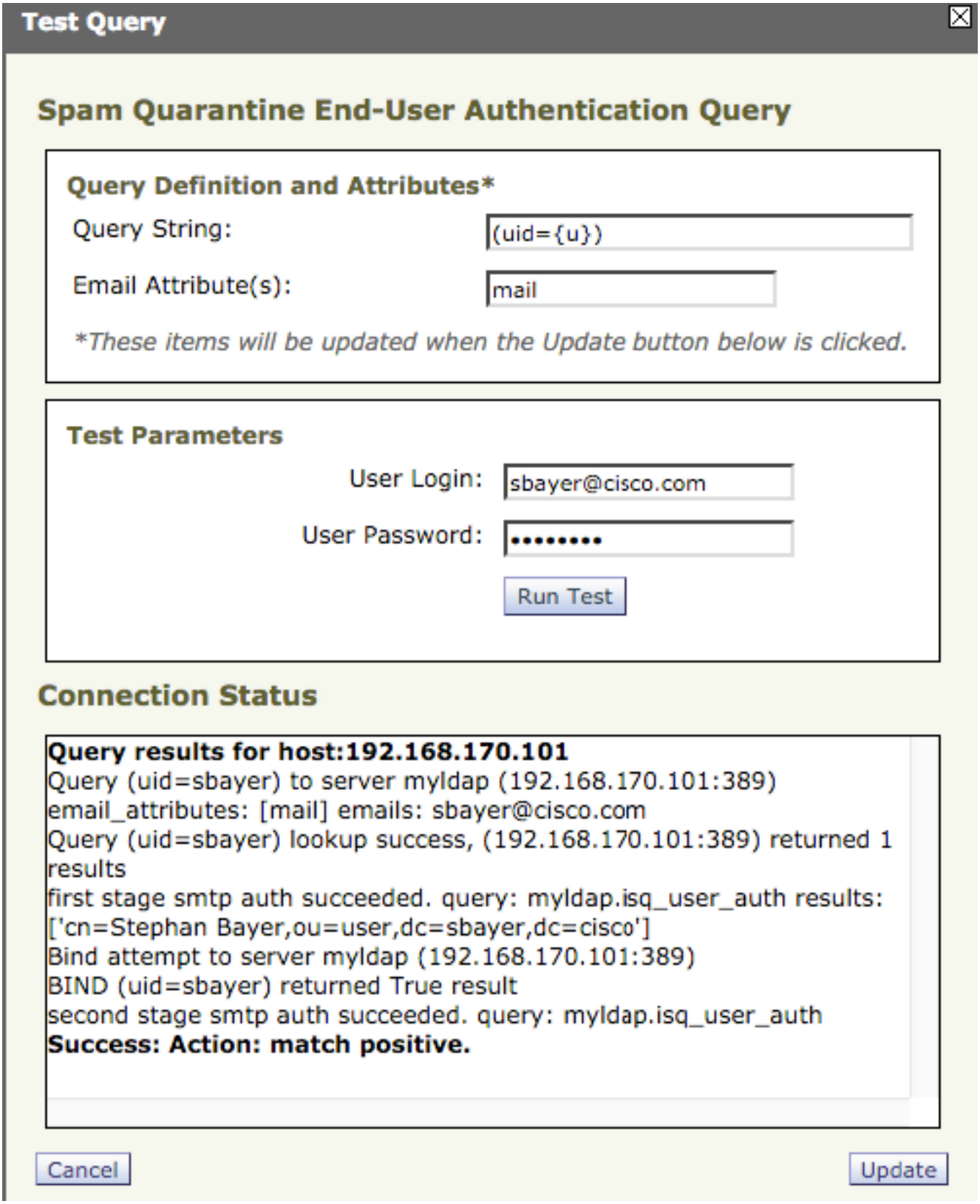
6. 변경 사항을 제출하고 커밋합니다.

스팸 쿼런틴을 통한 최종 사용자 스팸 쿼런틴 액세스 구성 최종 사용자 인증 쿼리

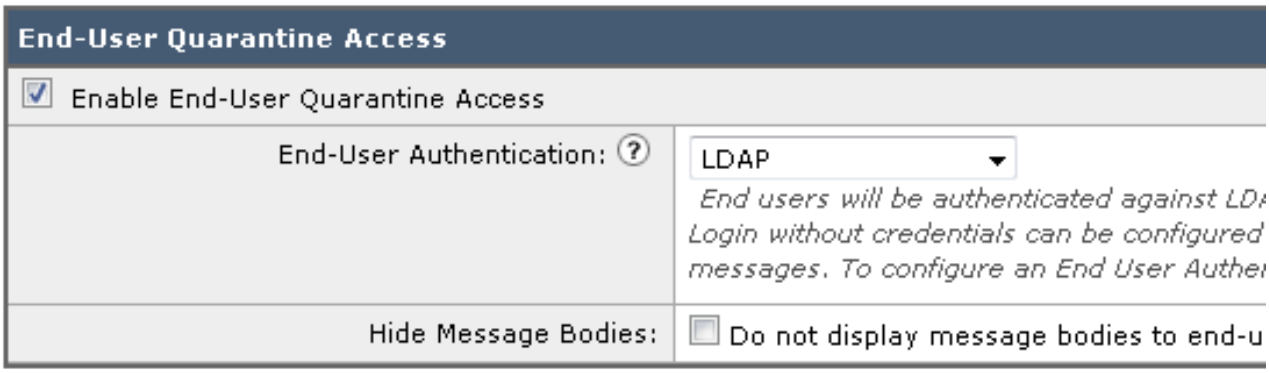
1. SMA 또는 ESA에서 System **Administration(시스템 관리) > LDAP를** 선택합니다.
2. LDAP 서버 프로필을 엽니다.
3. Active Directory 계정으로 인증할 수 있는지 확인하려면 스팸 쿼런틴 최종 사용자 인증 쿼리가 활성화되어 있는지 확인하십시오.
4. Designate as **Active Query(활성 쿼리로 지정)** 확인란을 선택합니다.



5. 쿼리를 테스트하려면 **테스트**를 클릭합니다. Match Positive는 인증이 성공했음을 의미합니다
.



6. 변경 사항을 제출하고 커밋합니다.
7. ESA에서 Monitor(모니터링) **> Spam Quarantine(스팸 격리)을** 선택합니다. SMA에서 Spam Quarantine(스팸 격리) 설정으로 이동하여 동일한 단계를 수행합니다.
8. Spam **Quarantine(스팸 격리)을 클릭합니다**.
9. Enable **End-User Quarantine Access(최종 사용자 격리 액세스 활성화)** 확인란을 선택합니다.
10. End-User Authentication 드롭다운 목록에서 LDAP를 선택합니다.



11. 변경 사항을 제출하고 커밋합니다.
12. 외부 인증이 ESA/SMA에 있는지 확인합니다.
13. 이전에 웹 브라우저에서 구성한 URL로 이동하여 격리에 액세스할 수 있는지 확인합니다.
    https://quarantine.mydomain.com:83
    https://10.10.10.10:83
14. LDAP 계정으로 로그인합니다.이 오류가 발생하면 External authentication LDAP profile(외부 인증 LDAP 프로파일)을 선택하고 End-User Quarantine Access(최종 사용자 격리 액세스)를 활성화합니다(이전 단계 참조).

스팸 격리에 대한 관리 사용자 액세스 구성

다음 역할의 관리 사용자가 스팸 격리에서 메시지를 관리할 수 있도록 하려면 이 섹션의 절차를 사용하십시오.운영자, 읽기 전용 운영자, 헬프 데스크 또는 게스트 역할, 스팸 격리에 대한 액세스를 포함하는 사용자 지정 사용자 역할.

기본 관리자 사용자 및 이메일 관리자 사용자를 포함하는 관리자 레벨 사용자는 항상 스팸 격리에 액세스할 수 있으며 이 절차를 사용하여 스팸 격리 기능과 연결할 필요가 없습니다.

> **참고:**관리자가 아닌 사용자는 스팸 격리의 메시지에 액세스할 수 있지만 쿼런틴 설정을 편집할 수는 없습니다.관리자 레벨 사용자는 메시지에 액세스하고 설정을 편집할 수 있습니다.

전체 관리자 권한이 없는 관리자가 스팸 격리에서 메시지를 관리할 수 있도록 하려면 다음 단계를 완료하십시오.

1. 사용자를 생성하고 스팸 격리에 액세스할 수 있는 사용자 역할을 할당했는지 확인합니다.
2. Security Management Appliance에서 Management **Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Spam Quarantine(스팸 격리)을** 선택합니다.
3. Spam **Quarantine** Settings(스팸 격리 설정) 섹션에서 Enable(활성화) 또는 Edit Settings(설정 편집)를 클릭합니다.
4. Spam Quarantine Settings(스팸 격리 설정) 섹션의 Administrative Users(관리 사용자) 영역에서 Local Users(로컬 사용자), Externally Authenticated Users(외부 인증 사용자) 또는 Custom User Roles(사용자 지정 사용자 역할)에 대한 선택 링크를 클릭합니다.
5. 스팸 격리에서 메시지를 보고 관리하기 위한 액세스 권한을 부여할 사용자를 선택합니다.
6. **확인을 클릭합니다**.
7. 섹션에 나열된 다른 유형의 관리 사용자(로컬 사용자, 외부 인증 사용자 또는 사용자 지정 사용자 역할)에 대해 필요한 경우 이 단계를 반복합니다.
8. 변경 사항을 제출하고 커밋합니다.