Guida all'impostazione completa della quarantena della posta indesiderata su Email Security Appliance (ESA) e Security Management Appliance (SMA)

Sommario

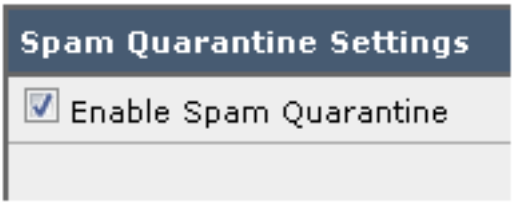
Introduzione

Questo documento descrive come configurare la quarantena della posta indesiderata sull'ESA o sull'SMA e le funzionalità associate: autenticazione esterna con notifica di quarantena LDAP e spam.

Procedura

Configurazione della quarantena della posta indesiderata locale sull'ESA

1. Sull'ESA, scegliere **Monitoraggio > Quarantena posta indesiderata**.
2. Nella sezione Impostazioni quarantena posta indesiderata selezionare la casella di controllo **Abilita quarantena posta indesiderata** e impostare le impostazioni di quarantena desiderate.

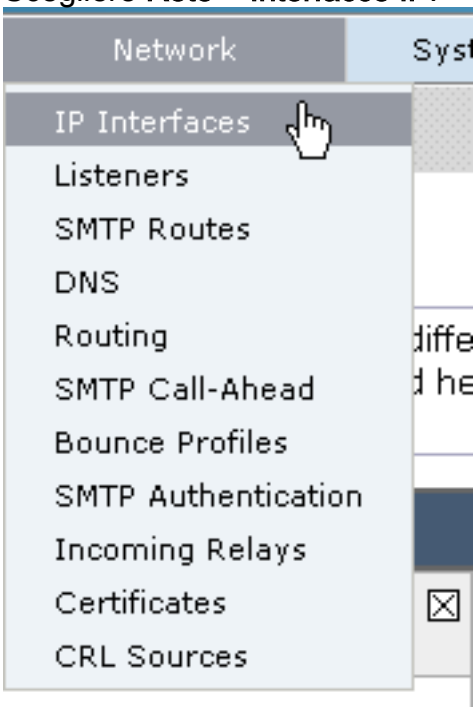


3. Scegliere **Servizi di sicurezza > Quarantena posta indesiderata**.
4. Verificare che la casella di controllo **Abilita quarantena posta indesiderata esterna** sia deselezionata, a meno che non si preveda di utilizzare la quarantena (vedere la sezione seguente).

5. Inviare e confermare le modifiche.

Abilitare le porte di quarantena e specificare un URL di quarantena nell'interfaccia

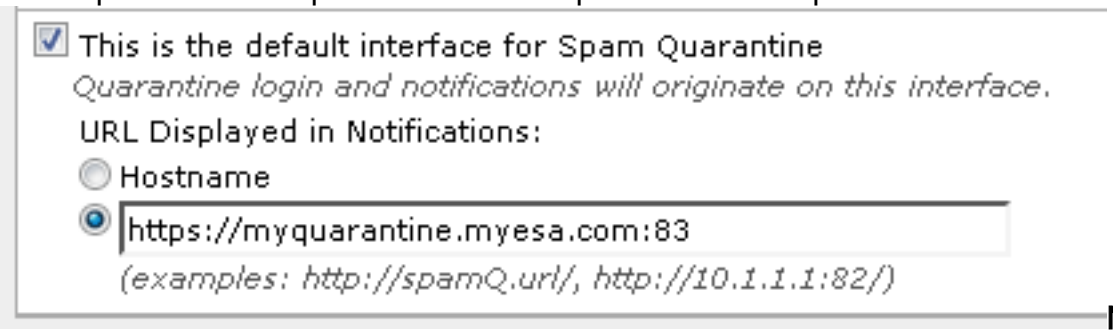
1. Scegliere **Rete > Interfacce IP**.



2. Fare clic sul nome dell'interfaccia che verrà utilizzata per accedere alla quarantena. Nella sezione quarantena posta indesiderata, selezionare le caselle di controllo e specificare le porte predefinite o modificare come richiesto:HTTP quarantena posta indesideratoHTTPS quarantena posta indesiderata

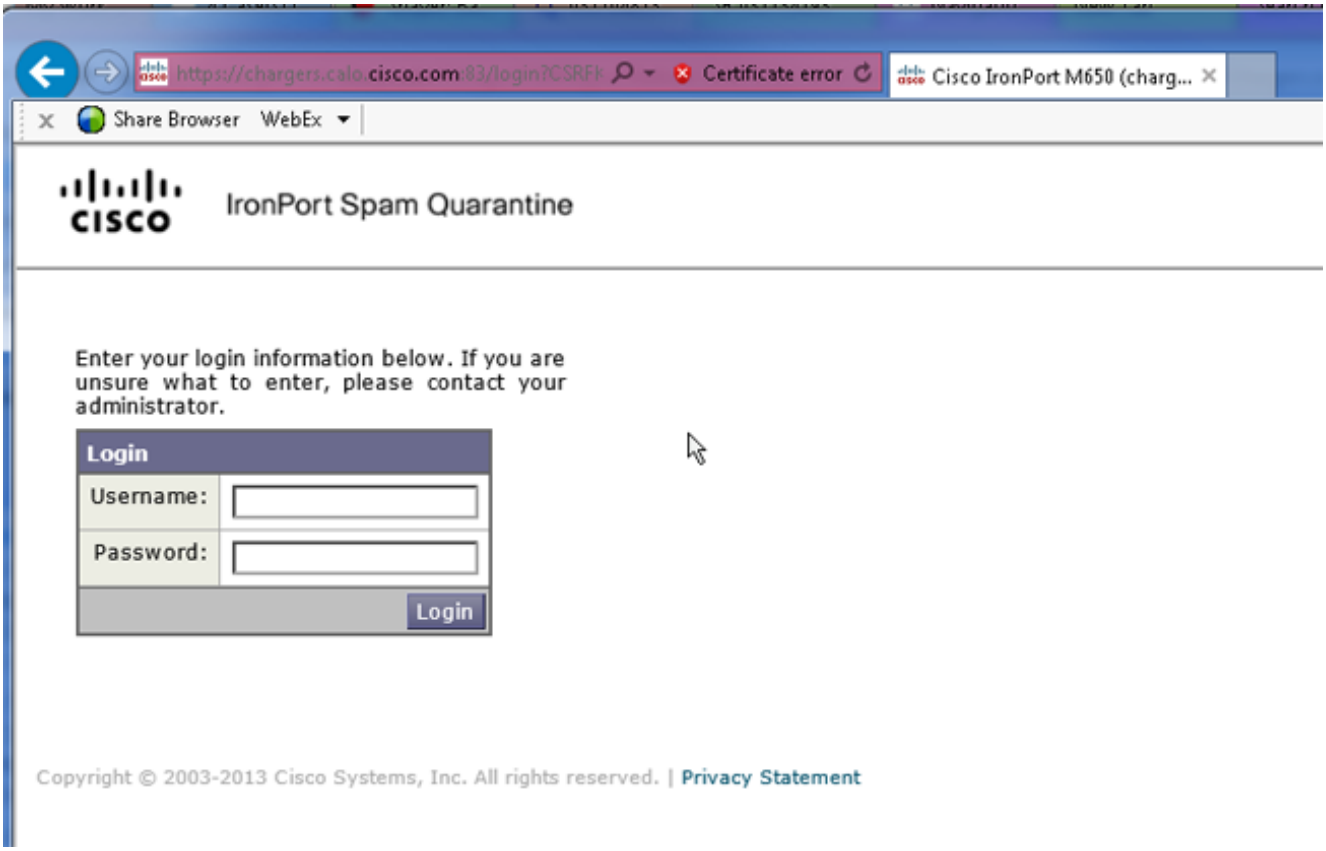
3. Selezionare la casella di controllo **Questa è l'interfaccia predefinita per la quarantena della posta indesiderata**.
4. Per impostazione predefinita, in "URL visualizzato nelle notifiche" l'accessorio utilizza il nome host del sistema (cli: **nomeostest)**, a meno che non sia specificato diversamente nel secondo pulsante di opzione e nel campo di testo. In questo esempio viene specificata l'impostazione predefinita per il nome

host. Èpossibile specificare un URL personalizzato per accedere alla quarantena della posta



indesiderata. **Nota:** Se si configura la quarantena per l'accesso esterno, sarà necessario un indirizzo IP esterno configurato sull'interfaccia o un indirizzo IP esterno convertito in indirizzo di rete interno.Se non si utilizza un nome host, è possibile mantenere selezionato il pulsante di opzione Nome host, ma accedere alla quarantena solo tramite l'indirizzo IP. Ad esempio, https://10.10.10.10:83.

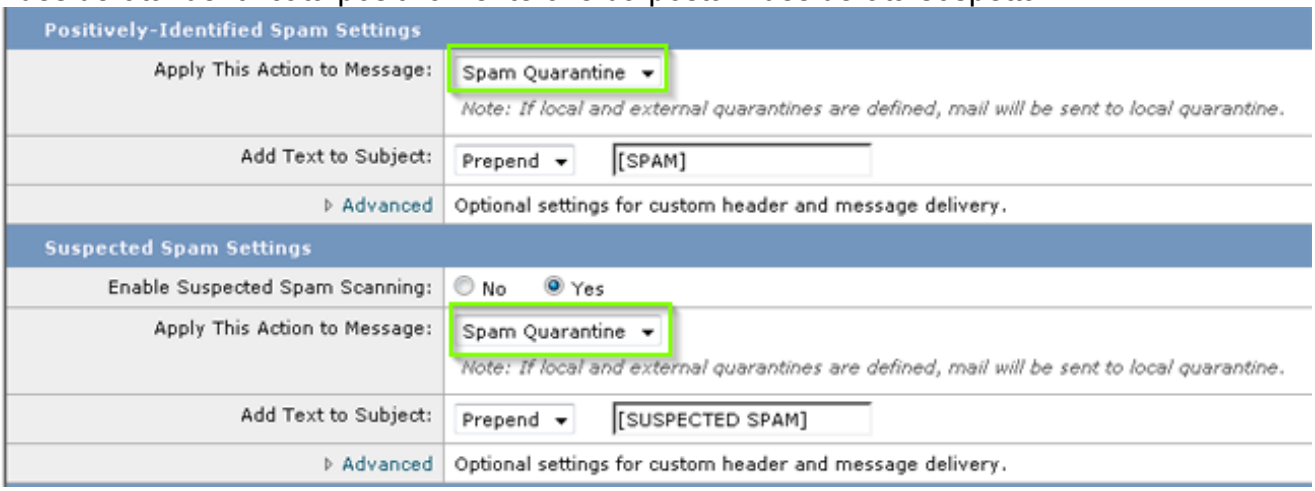
5. Inviare e confermare le modifiche.
6. Convalida. Se si specifica un nome host per la quarantena della posta indesiderata, verificare che il nome host sia risolvibile tramite DNS (Domain Name System) interno o DNS esterno. Il DNS risolverà il nome host nel tuo indirizzo IP.Se non si ottiene alcun risultato, contattare l'amministratore di rete e continuare ad accedere alla quarantena per indirizzo IP come nell'esempio precedente fino a quando l'host non viene visualizzato in DNS.>nslookup quarantine.mydomain.comPassare all'URL configurato in precedenza in un browser Web per verificare che sia possibile accedere alla quarantena: https://quarantine.mydomain.com:83https://10.10.10.10:83



Configurazione dell'ESA per lo spostamento di posta indesiderata positiva e/o sospetta in quarantena

Per mettere in quarantena i messaggi di posta indesiderata sospetti e/o identificati come posta indesiderata, attenersi alla seguente procedura:

1. Dall'ESA, fare clic su **Mail Policies > Incoming Mail Policies** (Policy di posta in arrivo), quindi sulla colonna anti-spam per il criterio predefinito.
2. Modificare l'azione da inviare alla quarantena della posta indesiderata sia da posta indesiderata identificata positivamente che da posta indesiderata sospetta."



3. Ripetere la procedura su tutte le altre ESA configurate per la quarantena della posta indesiderata esterna. Se si apporta questa modifica a livello di cluster, non sarà necessario ripeterla in quanto la modifica verrà propagata agli altri accessori del cluster.
4. Inviare e confermare le modifiche.
5. A questo punto, la posta che altrimenti sarebbe stata recapitata o eliminata verrà messa in quarantena.

Configurazione della quarantena della posta indesiderata esterna sull'SMA

La procedura per configurare la quarantena della posta indesiderata esterna sull'SMA è la stessa della sezione precedente, con alcune eccezioni:

1. Su ciascuna ESA, è necessario disattivare la quarantena locale. Scegliete **Monitor > Quarantene**.
2. Sull'ESA, scegliere **Security Services > Spam Quarantine** (Servizi di sicurezza > Quarantena posta indesiderata) e fare clic su **Enable External Spam Quarantine** (Abilita quarantena posta indesiderata esterna).
3. Puntare l'ESA sull'indirizzo IP dell'SMA e specificare la porta che si desidera utilizzare. Il valore predefinito è Port 6025.

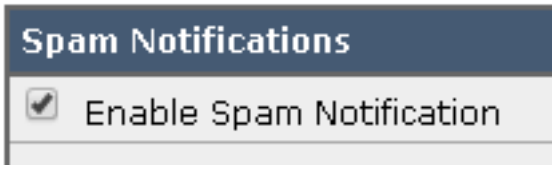
4. Verificare che la porta 6025 sia aperta dall'ESA all'SMA. *Porta per il recapito di messaggi in quarantena da ESA > SMA. Questa condizione può essere convalidata da con un test telnet dalla CLI sull'ESA sulla porta 6025. Se una connessione si apre e rimane aperta, è necessario impostarla.*

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

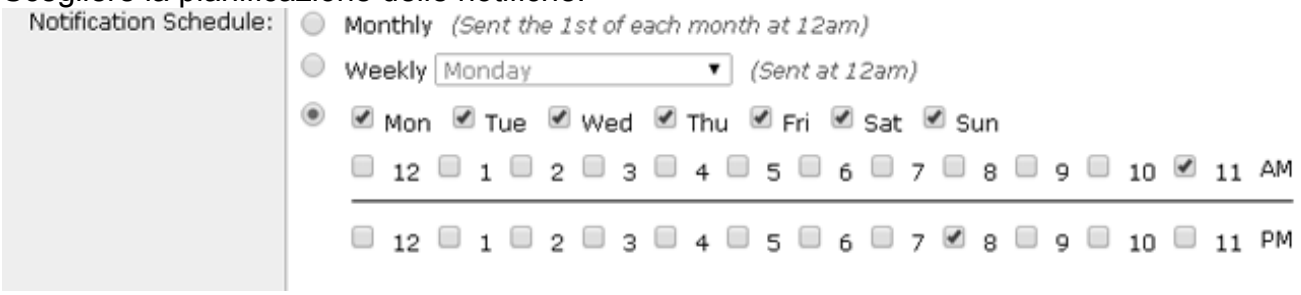
5. Accertarsi di aver configurato l'indirizzo IP/il nome host per accedere alla quarantena della posta indesiderata, ad esempio in "Abilita porte di quarantena e specifica un URL di quarantena sull'interfaccia".
6. Verificare che i messaggi arrivino alla quarantena della posta indesiderata dalle ESA. Se nella quarantena della posta indesiderata non vengono visualizzati messaggi, potrebbe essersi verificato un problema di connettività da ESA > SMA sulla porta 6025 (vedere i passaggi precedenti).

Configura notifica quarantena posta indesiderata

1. Sull'ESA, scegliere **Monitoraggio > Quarantena posta indesiderata**.
2. SMA consente di passare alle impostazioni di quarantena della posta indesiderata per eseguire gli stessi passaggi.
3. Fare clic su **Quarantena posta indesiderata**.
4. Selezionare la casella di controllo **Abilita notifica posta indesiderata**.



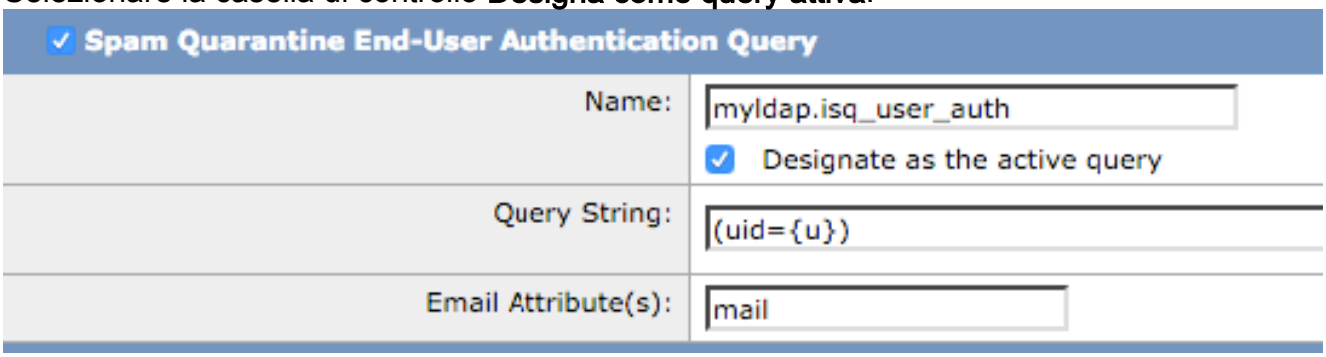
5. Scegliere la pianificazione delle notifiche.



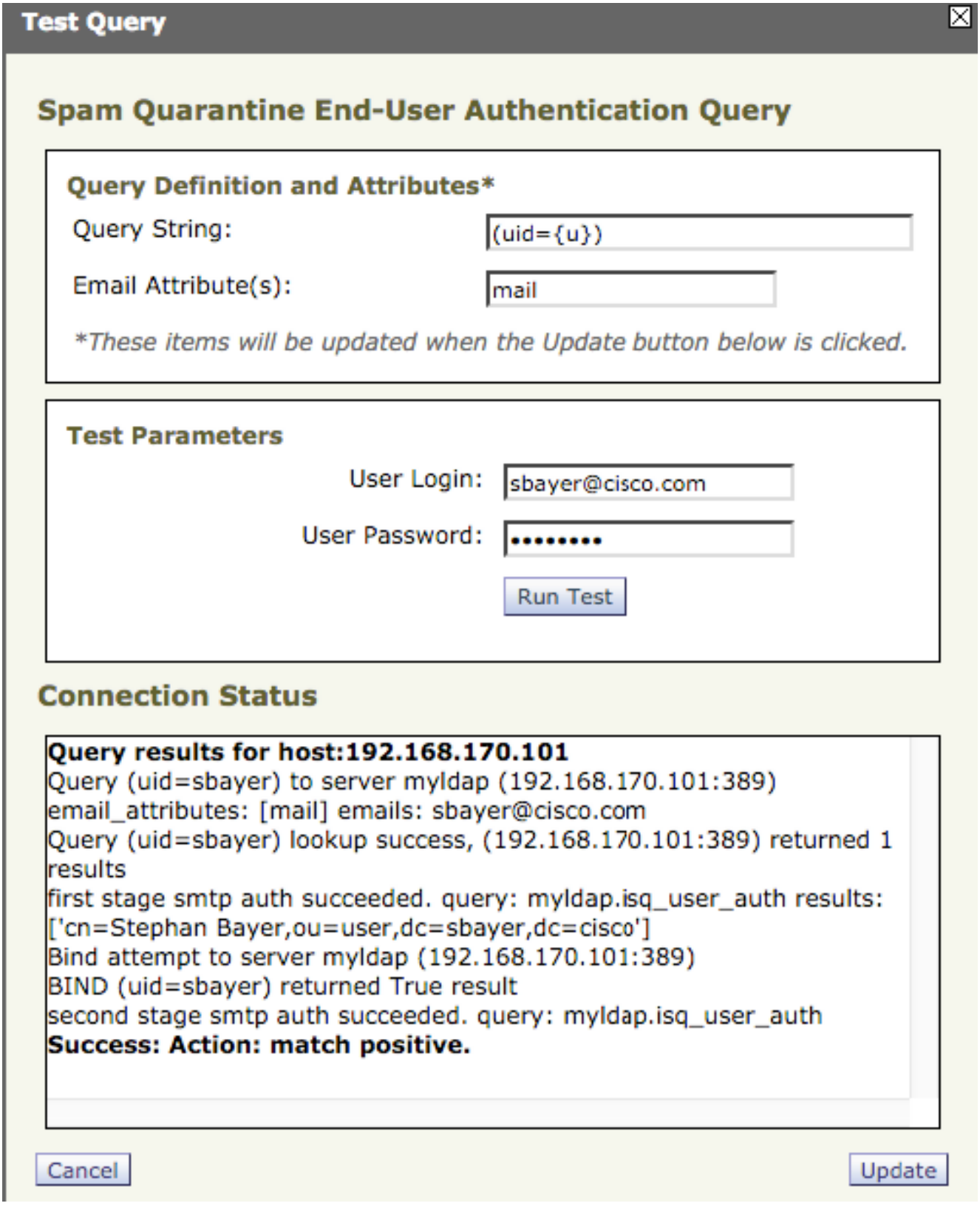
6. Inviare e confermare le modifiche.

Configurazione dell'accesso dell'utente finale alla quarantena della posta indesiderata tramite la query di autenticazione dell'utente finale per la quarantena della posta indesiderata

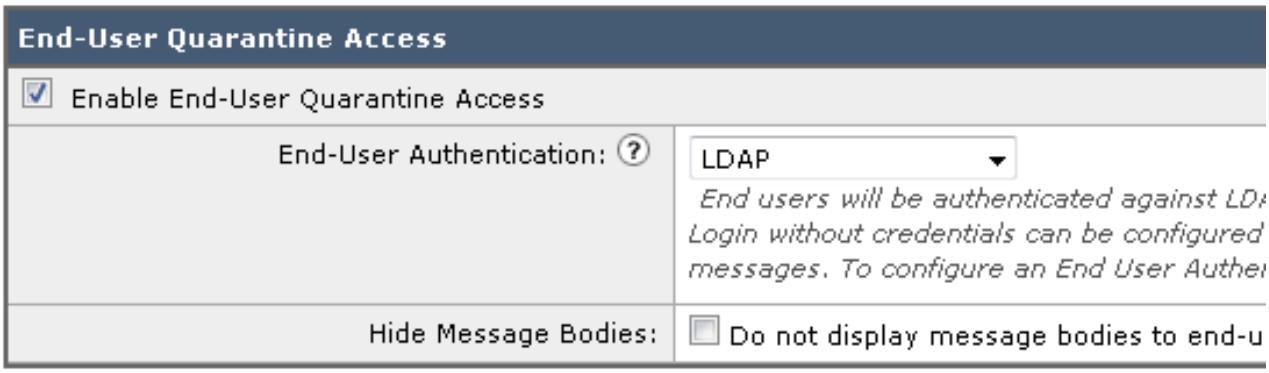
1. Su SMA o ESA, scegliere **Amministrazione sistema > LDAP**.
2. Aprire il profilo del server LDAP.
3. Per verificare che sia possibile eseguire l'autenticazione con un account Active Directory, verificare che la query di autenticazione utente finale per la quarantena della posta indesiderata sia abilitata.
4. Selezionare la casella di controllo **Designa come query attiva**.



5. Fare clic su **Test** per verificare la query. Corrispondenza positiva indica che l'autenticazione è
riuscita:



6. Inviare e confermare le modifiche.
7. Sull'ESA, scegliere **Monitoraggio > Quarantena posta indesiderata**. Nell'SMA, passare alle impostazioni di quarantena della posta indesiderata per eseguire gli stessi passaggi.
8. Fare clic su **Quarantena posta indesiderata**.
9. Selezionare la casella di controllo **Abilita accesso quarantena utente finale**.
10. Selezionare **LDAP** dall'elenco a discesa Autenticazione utente finale.



11. Inviare e confermare le modifiche.
12. Verificare che l'autenticazione esterna sia su ESA/SMA.
13. Passare all'URL configurato in precedenza in un browser Web per verificare che sia possibile accedere alla quarantena: https://quarantine.mydomain.com:83 https://10.10.10.10:83
14. Accedere con l'account LDAP. Se l'operazione non riesce, controllare il profilo LDAP di autenticazione esterna e abilitare Accesso quarantena utente finale (vedere i passaggi precedenti).

Configurazione dell'accesso degli utenti con privilegi amministrativi alla quarantena della posta indesiderata

Utilizzare la procedura descritta in questa sezione per consentire agli utenti amministrativi con questi ruoli di gestire i messaggi nella quarantena della posta indesiderata: ruoli di operatore, operatore di sola lettura, help desk o guest e ruoli utente personalizzati che includono l'accesso alla quarantena della posta indesiderata.

Questa procedura consente agli utenti a livello di amministratore, tra cui l'utente amministratore predefinito e gli utenti amministratori della posta elettronica, di accedere sempre alla quarantena della posta indesiderata e di non essere associati alla funzione di quarantena della posta indesiderata.

> **Nota:** Gli utenti non amministratori possono accedere ai messaggi nella quarantena della posta indesiderata, ma non possono modificare le impostazioni di quarantena. Gli utenti con privilegi di amministratore possono accedere ai messaggi e modificare le impostazioni.

Per consentire agli utenti con privilegi amministrativi che non dispongono di tutti i privilegi di amministratore di gestire i messaggi nella quarantena della posta indesiderata, eseguire la procedura seguente:

1. Accertarsi di aver creato utenti e di avergli assegnato un ruolo utente con accesso alla quarantena della posta indesiderata.
2. Sull'appliance di gestione della sicurezza, scegliere **Appliance di gestione > Servizi centralizzati > Quarantena posta indesiderata**.
3. Fare clic su **Abilita o Modifica impostazioni** nella sezione Impostazioni quarantena posta indesiderata.
4. Nell'area Utenti amministrativi della sezione Impostazioni quarantena posta indesiderata fare clic sul collegamento di selezione Utenti locali, Utenti autenticati esternamente o Ruoli utente

personalizzati.
5. Scegliere gli utenti a cui si desidera concedere l'accesso per visualizzare e gestire i messaggi nella quarantena della posta indesiderata.
6. Fare clic su **OK**.
7. Ripetere l'operazione se necessario per ognuno degli altri tipi di utenti amministrativi elencati nella sezione (Utenti locali, Utenti autenticati esternamente o Ruoli utente personalizzati).
8. Inviare e confermare le modifiche.