E メール セキュリティ アプライアンス（ESA）およびセキュリティ管理アプライアンス（SMA）における包括的なスパム検疫設定ガイド

目次

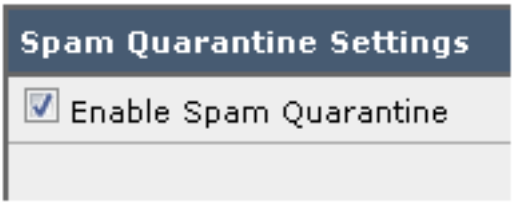
概要

この資料に ESA のスパム検疫をか SMA および関連する機能設定する方法を記述されています: LDAP およびスパム検疫通知の外部認証。

手順

ESA のローカル スパム検疫を設定して下さい

1. ESA で、**> スパム検疫**『Monitor』 を選択 して下さい。
2. スパム検疫では設定は区分し、**イネーブル スパム検疫**チェックボックスをチェックし、望ましい検疫設定を行います。

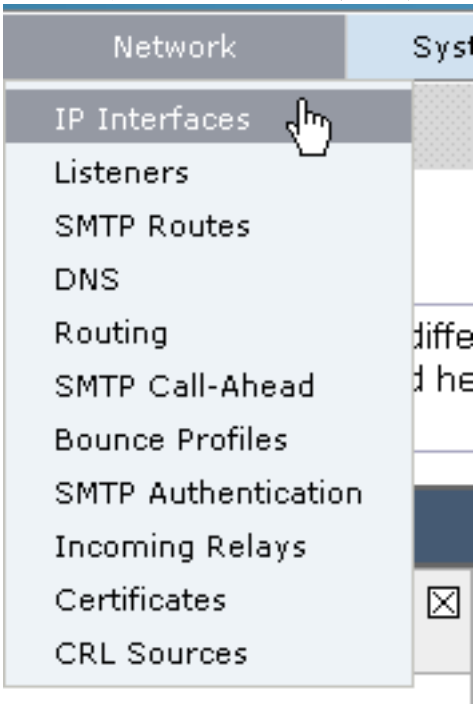


3. **サービス > スパム検疫を**『Security』 を選択 して下さい。
4. 外部スパム検疫を使用するために計画しなかったら、**外部スパム検疫**チェックボックスがチェックを外される**イネーブルを**確認して下さい（下記の例を参照して下さい）。

5. 変更を送信し、保存します。

検疫ポートを有効に し、インターフェイスで検疫 URL を規定 して下さい

1. **ネットワーク > IP インターフェイスを**選択して下さい。



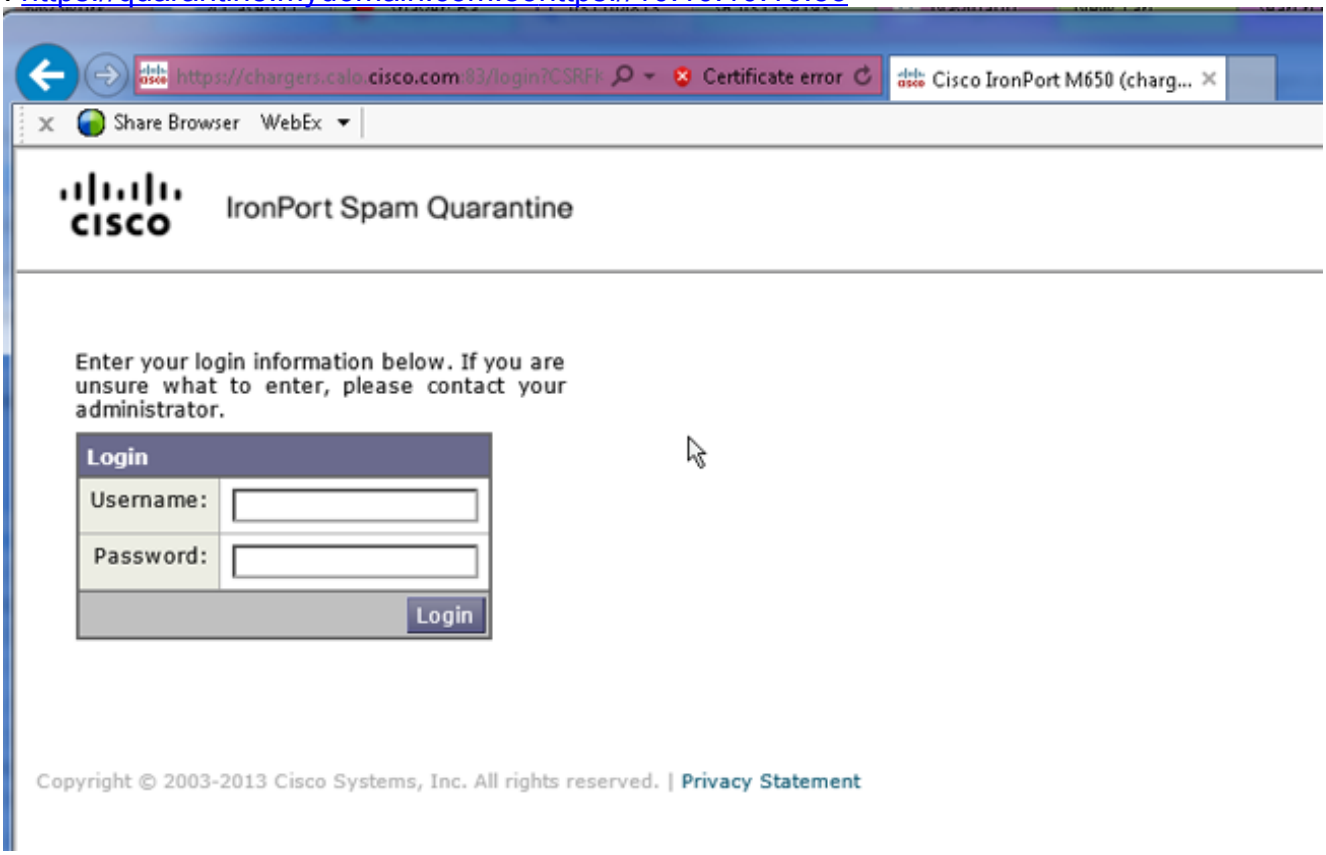
2. 検疫にアクセスするために使用するインターフェイスのインターフェイス名をクリックして下さい。 スパム検疫セクションでは、チェックボックスをチェックし、デフォルトポートを規定 するか、または要求に応じて変更して下さい:検疫 HTTP を無差別に送信して下さい 検疫 HTTPS を無差別に送信して下さい

3. **これですスパム検疫**チェックボックス**のためのデフォルト インターフェイス** チェックして下さい。
4. 「通知で」表示される URL の下でデフォルトでアプライアンスはシステム ホスト名 (cli を使用します: 第 2 Radio ボタン オプションおよびテキスト フィールドの **sethostname**) 他に特に規定がなければ。 この例はデフォルトホスト名設定を規定 したものです。

スパム検疫にアクセスするためにカスタム URL を規定できます。

注: 外部アクセスのための検疫を設定する場合、変換される内部 IP へのネットワーク アドレスである外部 IP かインターフェイスで設定された外部 IPアドレスを必要とします。ホスト名を使用しなければ-ホスト名 Radio ボタンをチェックしておくことができますがまだ IP アドレスだけによって検疫にアクセスします。 たとえば、https://10.10.10.10:83。

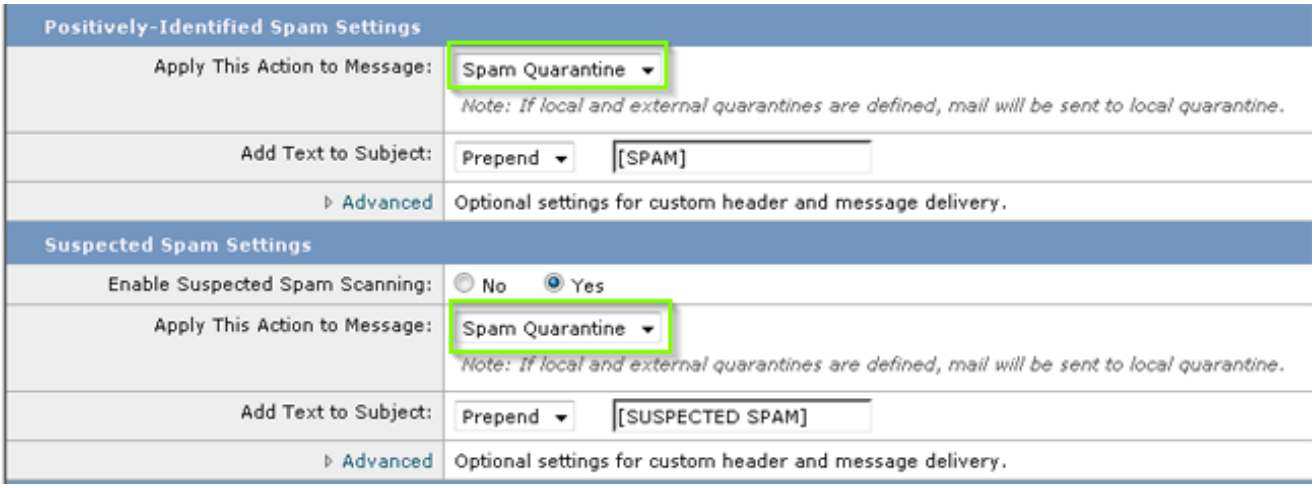
5. 変更を送信し、保存します。
6. **検証**します。 スパム検疫のためのホスト名を規定 する場合、ホスト名をです内部ドメイン ネーム システム (DNS) か外部 DNS によって解決可能確認して下さい。 DNS は IP アドレスにホスト名を解決します。結果を得ない場合、ネットワーク管理者とチェックし、ホストが DNS に出て来るまで前例のような IP アドレスによって検疫にアクセスし続けて下さい。 >nslookup quarantine.mydomain.com検疫にアクセスできること検証するために Webブラウザで前もって設定される URL にナビゲート して下さい : https://quarantine.mydomain.com:83https://10.10.10.10:83



肯定的なスパムや疑わしいスパムを検疫を無差別に送信するために移動するように ESA を設定して下さい

疑わしいスパムや肯定的に識別されたスパム メッセージを検疫するために、これらのステップを完了して下さい:

1. 次に ESA で、**メール「Policies」>** デフォルトポリシーのための**着信メール「Policies」**および反スパム カラムをクリックして下さい。
2. 変更して下さいスパム検疫に送信 する肯定的に識別されたスパムまたは疑わしいスパムの操作を」。

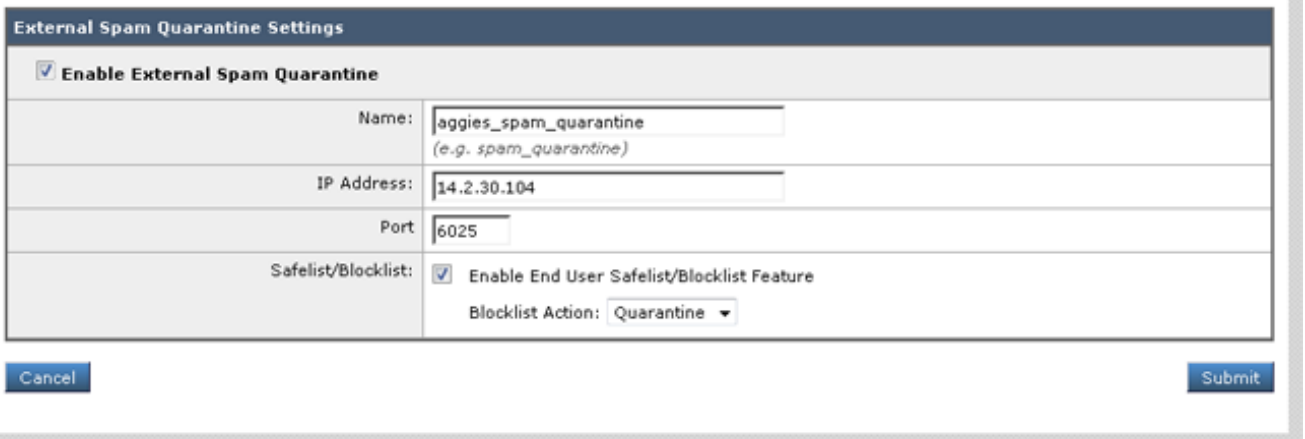


3. 外部スパム検疫のために設定するかもしれない他のどの ESA のためのプロセスも繰り返して下さい。 クラスタでこの変更を水平にならせるクラスタの他のアプライアンスへの変更が propogated のでそれを繰り返す必要がありません。
4. 変更を送信し、保存します。
5. この時点で、別の方法で提供されるか、または廃棄されたメールは検疫されて得ます。

SMA の外部スパム検疫を設定して下さい

SMA の外部スパム検疫を設定するステップは少数の例外を除く前のセクションと同じです:

1. ESA のそれぞれで、ローカル検疫を無効に する必要があります。 **> 検疫**『Monitor』 を選択 して下さい。
2. ESA で、**サービス > スパム検疫を**『Security』 を選択 し、**外部スパム検疫を**『Enable』 をクリック して下さい。
3. ESA を SMA の IP アドレスを指し、使用するために望むポートを規定 して下さい。 デフォルトはポート 6025 です。



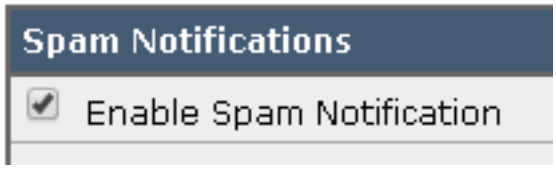
4. ポート 6025 を ESA から SMA に開いています確認して下さい。 *このポートは検疫されたメッセージの配信のためからの ESA > SMA です。 これはポート 6025 の ESA の CLI からの telnet テストでによって検証することができます。 接続がおよび開けば開いた滞在設定する必要があります。*

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

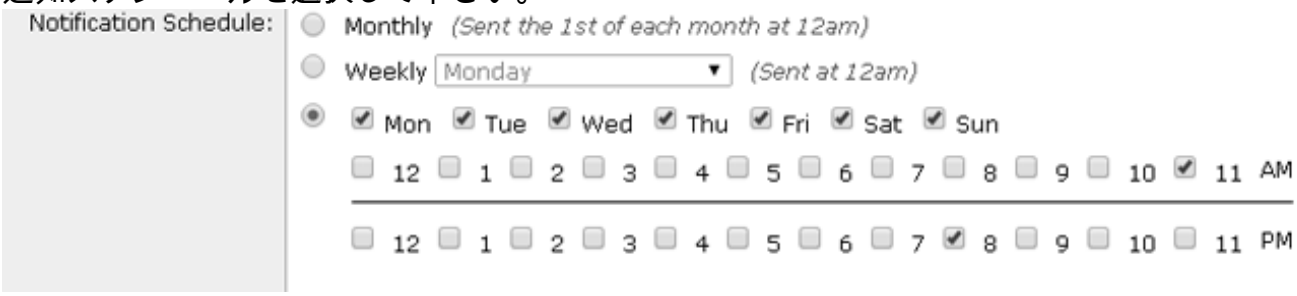
5. 「イネーブル検疫ポートののようなスパム検疫に、アクセスし、インターフェイスで検疫 URL を」規定 するために設定しました IP/hostname を-確認して下さい。
6. メッセージが ESA からのスパム検疫に着くことを確認して下さい。 スパム検疫がメッセージを表示しない場合、ESA > ポート 6025 の SMA 接続においての問題がからのあるかもしれません（前の手順を参照して下さい）。

スパム検疫通知を設定して下さい

1. ESA で、**> スパム検疫**『Monitor』 を選択 して下さい。
2. 同じステップを実行するために SMA でスパム検疫設定にナビゲート します。
3. **スパム検疫を**クリックして下さい。
4. **イネーブル スパム通知** チェックボックスをチェックして下さい。



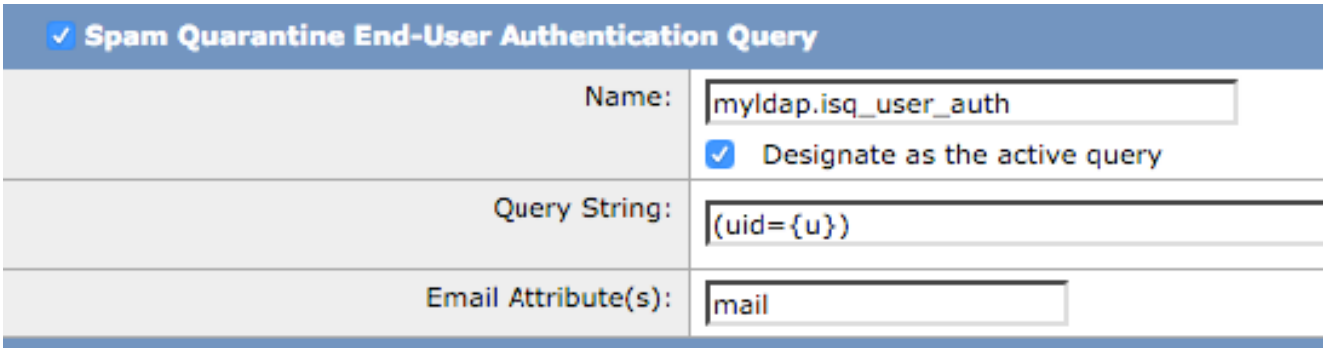
5. 通知スケジュールを選択して下さい。



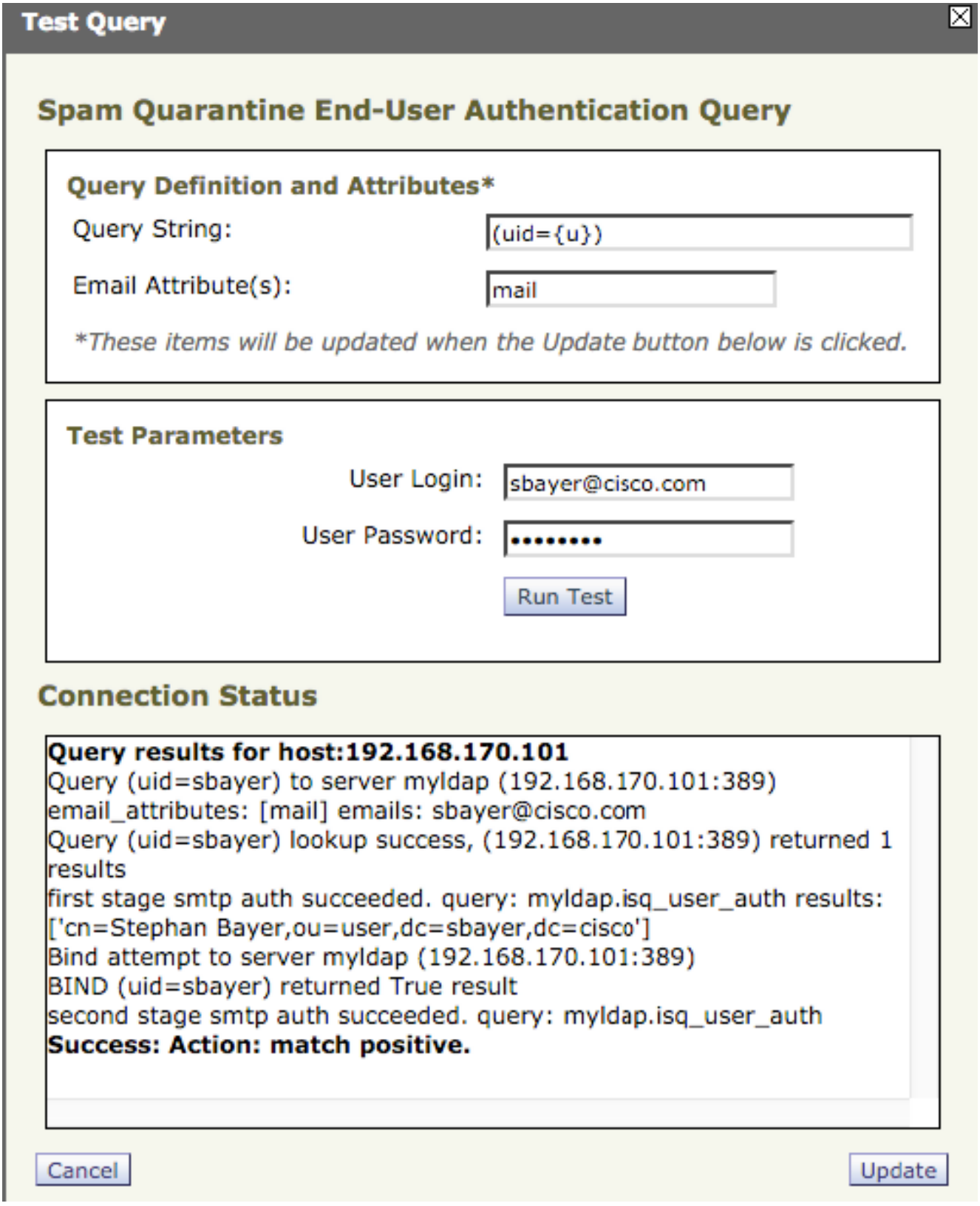
6. 変更を送信し、保存します。

スパム検疫エンドユーザ認証クエリによってエンドユーザ スパム検疫アクセスを設定して下さい

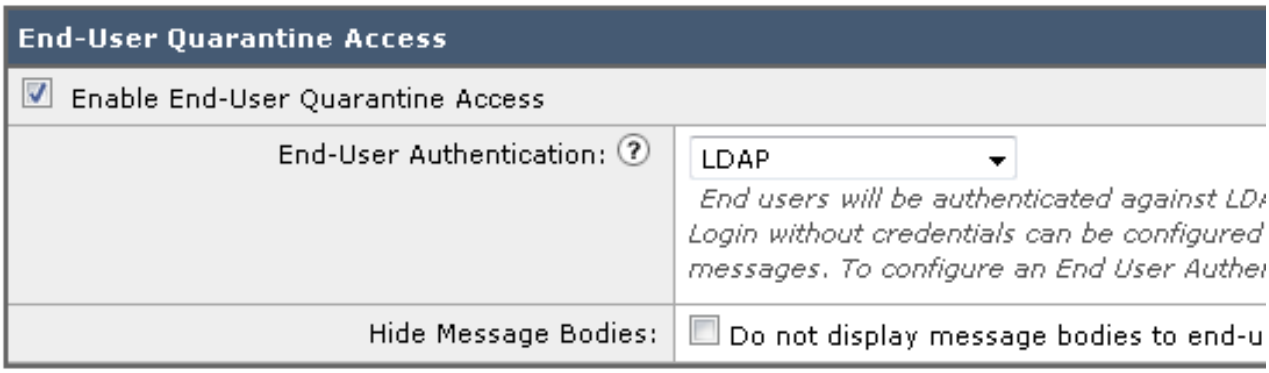
1. SMA か ESA で、**システム 管理 > LDAP を**選択して下さい。
2. LDAPサーバ プロファイルを開いて下さい。
3. 確認するためにアクティブ ディレクトリ アカウントと認証ことチェックしますスパム検疫エンドユーザをできて下さい認証クエリがイネーブルになっている。
4. **アクティブな Query チェックボックスとして指定を**チェックして下さい。



5. クエリをテストするために『Test』 をクリック して下さい。 認証が正常だったことを肯定的意味します一致する
:



6. 変更を送信し、保存します。
7. ESA で、**> スパム検疫**『Monitor』 を選択 して下さい。 SMA で、同じステップを実行するためにスパム検疫設定にナビゲート して下さい。
8. **スパム検疫を**クリックして下さい。
9. **イネーブル エンドユーザ検疫アクセスチェック** チェック ボックスをチェックして下さい。
10. エンドユーザ認証 ドロップダウン リストから **LDAP を**選択して下さい。



11. 変更を送信し、保存します。
12. 外部認証が ESA/SMA にあること検証して下さい。
13. 検疫にアクセスできること検証するために Webブラウザで前もって設定される URL にナビゲート して下さい: https://quarantine.mydomain.com:83 https://10.10.10.10:83
14. LDAP アカウントのログイン。 これが失敗した場合、外部認証 LDAP プロファイルをチェックし、エンドユーザ検疫アクセスをイネーブルにして下さい（前の手順を参照して下さい）。

スパム検疫に管理上のユーザアクセスを設定して下さい

これらのロールの管理上のユーザをスパム検疫のメッセージを管理することを許可するためにこのセクションで手順を使用して下さい: オペレータ、読み取り専用オペレータ、ヘルプ デスク、または Guestroles およびスパム検疫へのアクセスを含むカスタム ユーザの役割。

デフォルト管理者ユーザが含まれ、管理者ユーザを E-メールを送る管理者レベル ユーザはスパム検疫に常にアクセスでき、この手順を使用してスパム検疫機能と関連付けられる必要はありません。

> **注:** 非管理者レベルのユーザはスパム検疫のメッセージにアクセスできますが検疫設定を編集できません。 管理者レベル ユーザはメッセージにアクセスし、設定を編集できます。

スパムのメッセージを管理する完全なアドミニストレーター特権がない管理上のユーザを有効にするためにこれらのステップを検疫して下さい、完了して下さい:

1. ユーザを作成し、スパム検疫へのアクセスとそれらにユーザの役割を割り当てるために確かめて下さい。
2. セキュリティ管理 アプライアンスで、**管理アプライアンス > 中央 集中型 サービス > スパム検疫を**選択して下さい。
3. スパム検疫設定セクションの**設定を**『Enable』 をクリック するか、**または編集して下さい**。
4. スパム検疫設定の管理上の利用者域ではローカルユーザ、外部に認証済みユーザ、またはカスタム ユーザの役割への選択リンクを区分して下さい、クリックして下さい。
5. 対するアクセス権の付与に表示したいと思い、スパムのメッセージを管理するために検疫しなさいユーザを選択して下さい。
6. [OK] をクリックします。
7. セクション（ローカルユーザ、外部に認証済みユーザ、かカスタム ユーザの役割）にもし

必要なら繰り返して下さい。リストされている管理上のユーザの他の型のそれぞれのために
8. 変更を送信し、確定します。