Guide complet d'installation de quarantaine de Spam sur l'appliance de sécurité du courrier électronique (ESA) et l'appliance de Gestion de la sécurité (SMA)

Contenu

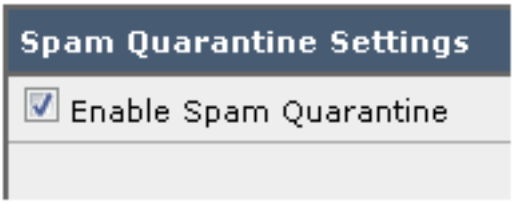
Introduction

Ce document décrit comment configurer la quarantaine de Spam sur l'ESA ou le SMA et les caractéristiques associées : authentification externe avec la notification de quarantaine de LDAP et de Spam.

Procédure

Configurez la quarantaine locale de Spam sur l'ESA

1. Sur l'ESA, choisissez la **quarantaine de moniteur > de Spam**.
2. Dans la quarantaine de Spam les configurations sectionnent, cochent la case de **quarantaine de Spam d'enable** et placent les configurations désirées de quarantaine.

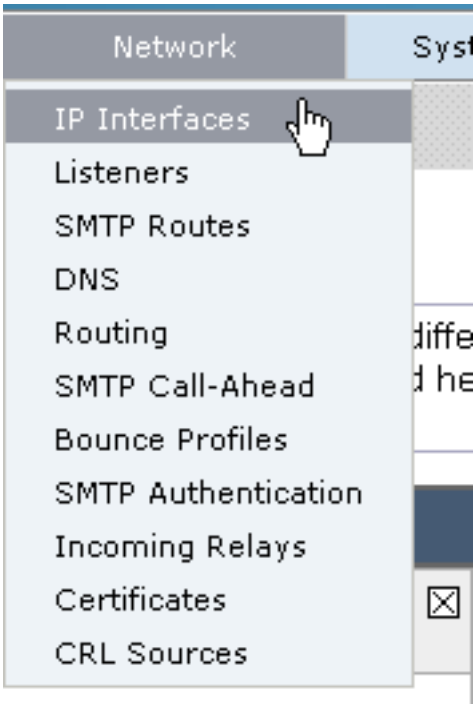


3. Choisissez les **Services de sécurité > la quarantaine de Spam**.
4. Assurez que la case **externe de quarantaine de Spam d'enable** est décochée, à moins que vous prévoyiez d'utiliser la quarantaine externe de Spam (voir la section ci-dessous).

5. Soumettez et commettez les modifications.

Activez les ports de quarantaine et spécifiez un URL de quarantaine à l'interface

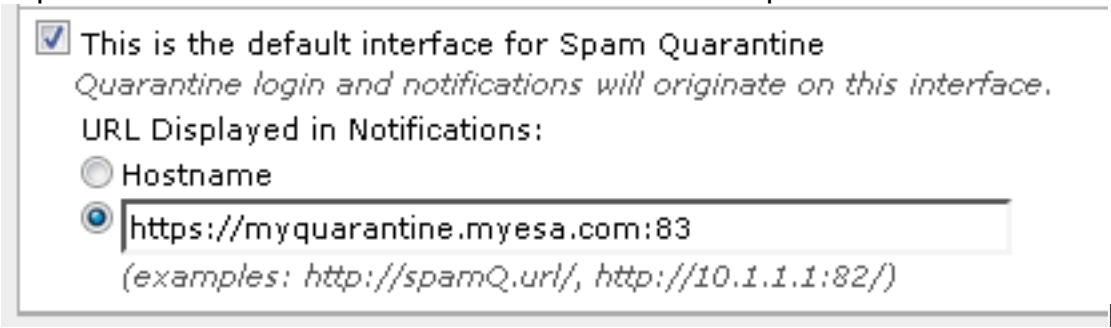
1. Choisissez le **réseau > les interfaces IP**.



2. Cliquez sur le nom d'interface de l'interface que vous utiliserez afin d'accéder à la quarantaine. Dans la section de quarantaine de Spam, vérifiez les cases et spécifiez les ports par défaut ou changez au besoin :HTTP de quarantaine de SpamQuarantaine HTTPS de
Spam

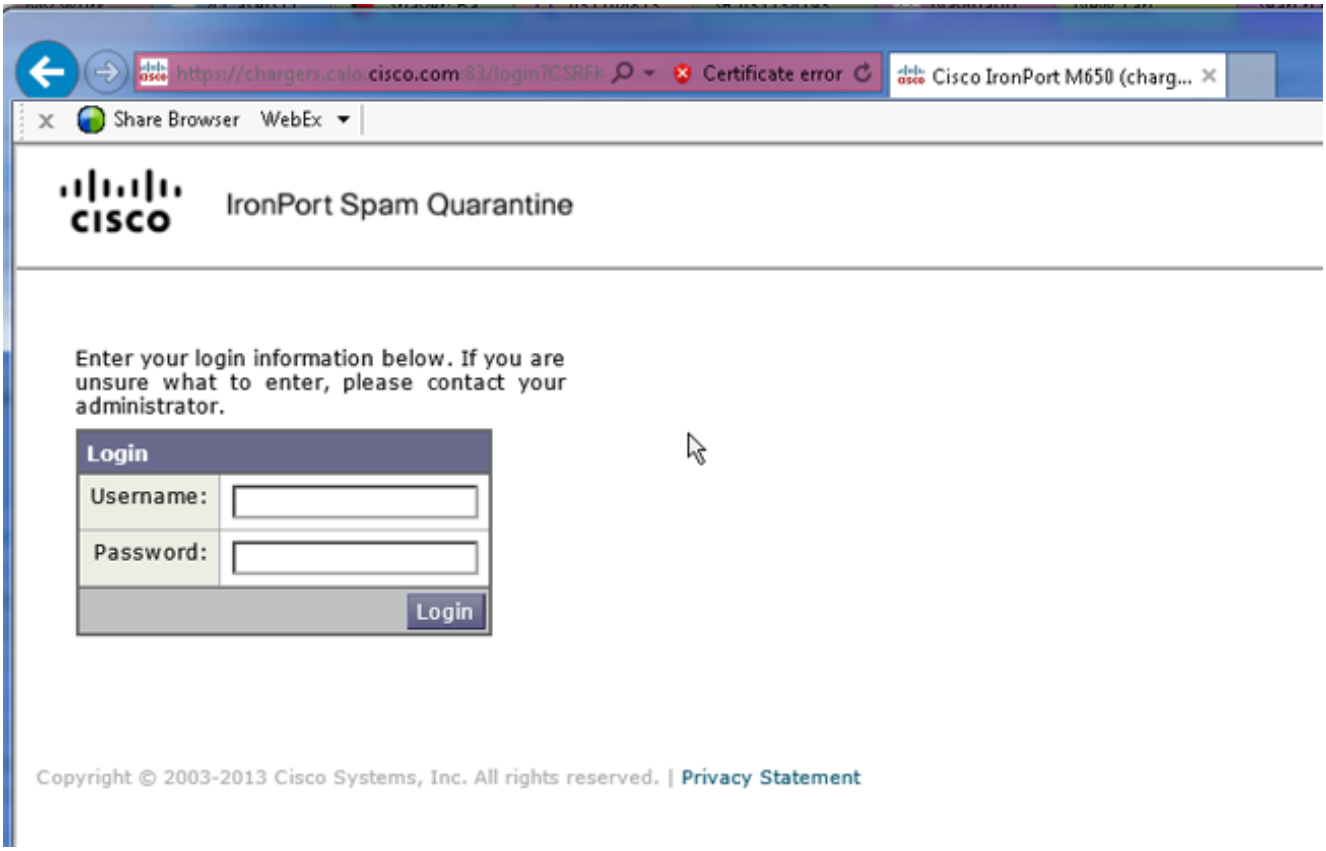
3. Cochez **ceci est l'interface par défaut pour la** case de **quarantaine de Spam**.
4. Sous le « URL affiché dans les notifications », par défaut l'appliance utilise l'adresse Internet de système (cli : **sethostname)** sauf indication contraire dans la deuxièmes option et champ texte de case d'option. Cet exemple spécifie la configuration d'adresse Internet par

défaut. Vous pouvez spécifier un URL de coutume afin d'accéder à votre quarantaine de



Spam. Remarque: Si vous configurez la quarantaine pour l'accès externe, vous aurez besoin d'une adresse IP externe configurée sur l'interface ou un IP externe qui est adresse réseau traduite à un IP interne.Si vous n'utilisez pas une adresse Internet vous pouvez maintenir la case d'option d'adresse Internet vérifiée, mais accédez à toujours la quarantaine par l'adresse IP seulement. Par exemple, https://10.10.10.10:83.

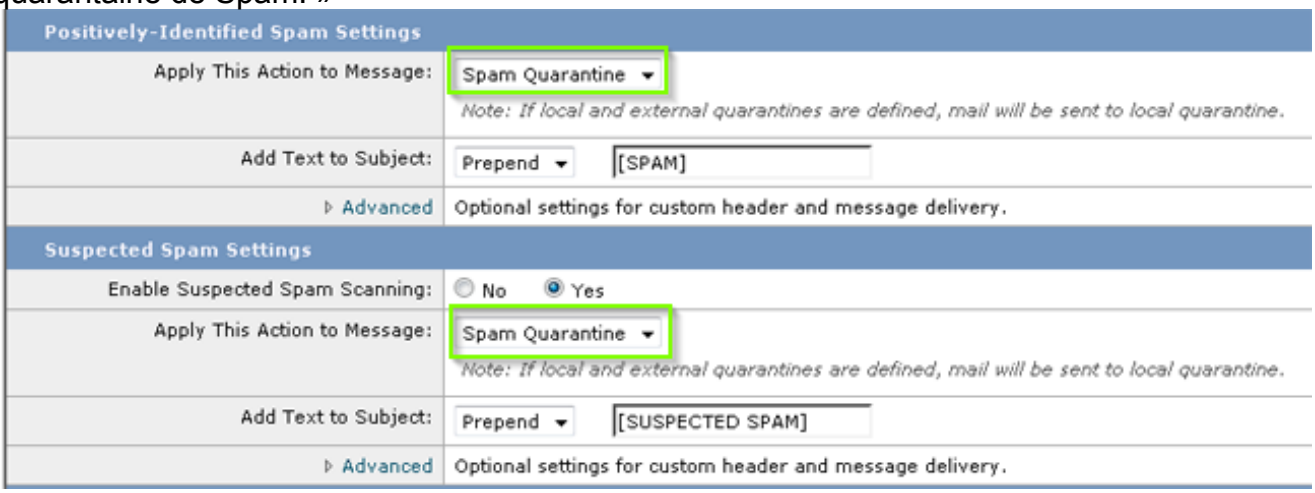
5. Soumettez et commettez les modifications.
6. Validez. Si vous spécifiez une adresse Internet pour la quarantaine de Spam, assurez que l'adresse Internet est résoluble par l'intermédiaire du Système de noms de domaine (DNS) interne ou des DN externes. Les DN résoudront l'adresse Internet à votre adresse IP.Si vous n'obtenez pas un résultat, vérifiez avec votre administrateur réseau et continuez à accéder à la quarantaine par l'adresse IP comme l'exemple précédent jusqu'à l'hôte révèle dans des DN.>nslookup quarantine.mydomain.comNaviguez vers votre URL configuré précédemment dans un navigateur Web afin de valider que vous pouvez accéder à la quarantaine : https://quarantine.mydomain.com:83https://10.10.10.10:83



Configurez l'ESA pour déplacer le Spam positif et/ou le Spam suspect pour spam la quarantaine

Afin de mettre en quarantaine votre Spam suspect et/ou messages spam franchement identifiés, terminez-vous ces étapes :

1. Sur l'ESA, les **stratégies de messagerie de** clic **> stratégies de messagerie entrante** et puis la colonne d'anti-Spam pour la stratégie par défaut.
2. Changez l'action du Spam franchement identifié ou du Spam suspect d'envoyer à la quarantaine de Spam. »



3. Répétez le processus pour n'importe quel autre ESAs que vous pourriez avoir configuré pour la quarantaine externe de Spam. Si vous apportiez cette modification à la batterie niveler vous ne devrez pas la répéter car le changement sera propagé aux autres appliances de la batterie.
4. Soumettez et commettez les modifications.
5. En ce moment, la messagerie qui aurait été autrement fournie ou abandonnée obtiendra mis en quarantaine.

Configurez la quarantaine externe de Spam sur le SMA

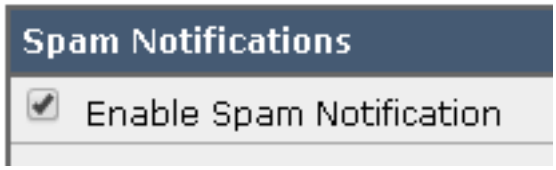
Les étapes pour configurer la quarantaine externe de Spam sur le SMA sont identiques que la section précédente à quelques exceptions :

1. Sur chacun de votre ESAs, vous devrez désactiver la quarantaine locale. Choisissez le **moniteur > les quarantaines**.
2. Sur votre ESA, choisissez les **Services de sécurité > la quarantaine de Spam** et cliquez sur la **quarantaine externe de Spam d'enable**.
3. Indiquez l'ESA l'adresse IP de votre SMA et spécifiez le port que vous voudriez utiliser. Le par défaut est le port 6025.

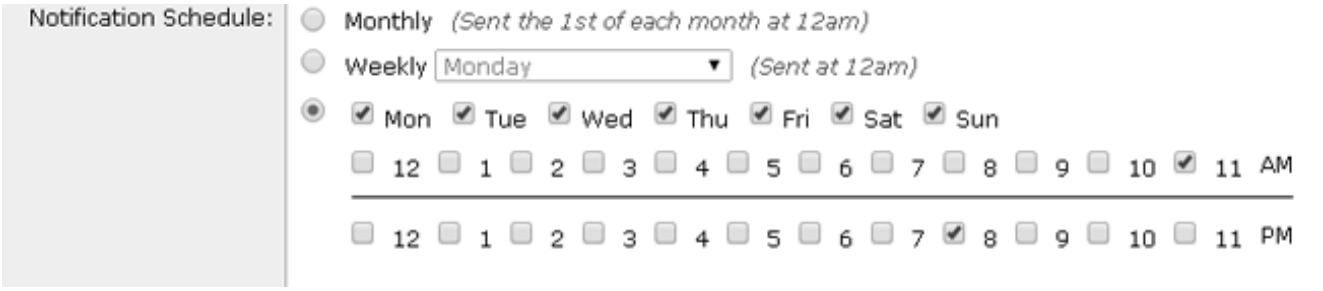
4. Assurez que le port 6025 est ouvert de l'ESA de SMA. *Ce port est pour la livraison des messages mis en quarantaine de ESA > SMA. Ceci peut être validé par avec un test de telnet du CLI sur l'ESA sur le port 6025. Si une connexion s'ouvre et des séjours ouverts vous devriez être placé.*
```
tarheel.rtp> telnet 14.2.30.116 6025
Trying 14.2.30.116...
Connected to steelers.rtp.
Escape character is '^]'.
220 steelers.rtp ESMTP
```
5. Assurez que vous avez configuré l'IP/hostname pour accéder à la quarantaine de Spam, comme dans « des ports de quarantaine d'enable et pour spécifier un URL de quarantaine à l'interface ».
6. Vérifiez que les messages arrivent à la quarantaine de Spam de votre ESAs. Si la quarantaine de Spam n'affiche aucun message, il pourrait y a une question avec la Connectivité de ESA > SMA sur le port 6025 (voir les étapes précédentes).

Configurez la notification de quarantaine de Spam

1. Sur l'ESA, choisissez la **quarantaine de moniteur > de Spam**.
2. Sur le SMA vous navigueriez vers les configurations de quarantaine de Spam afin d'exécuter les mêmes étapes.
3. **Quarantaine de Spam de** clic.
4. Cochez la case de **notification de Spam d'enable**.



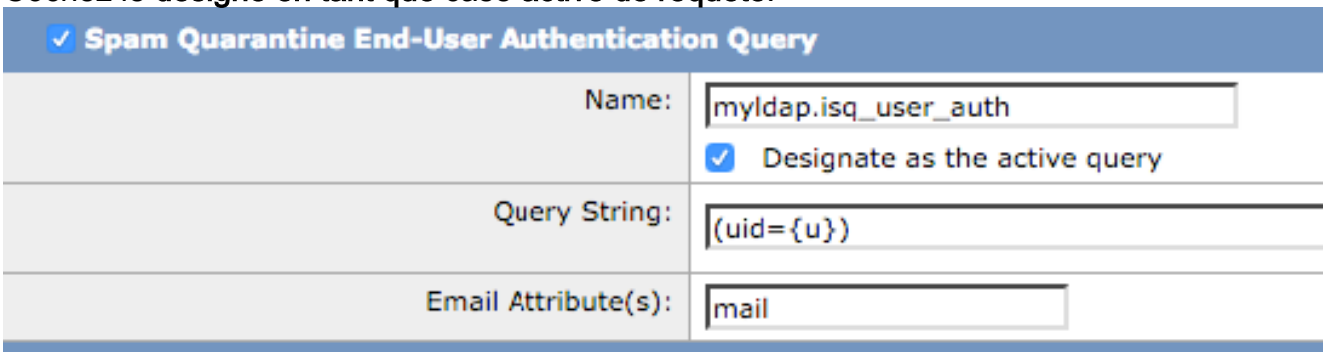
5. Choisissez votre programme de notification.



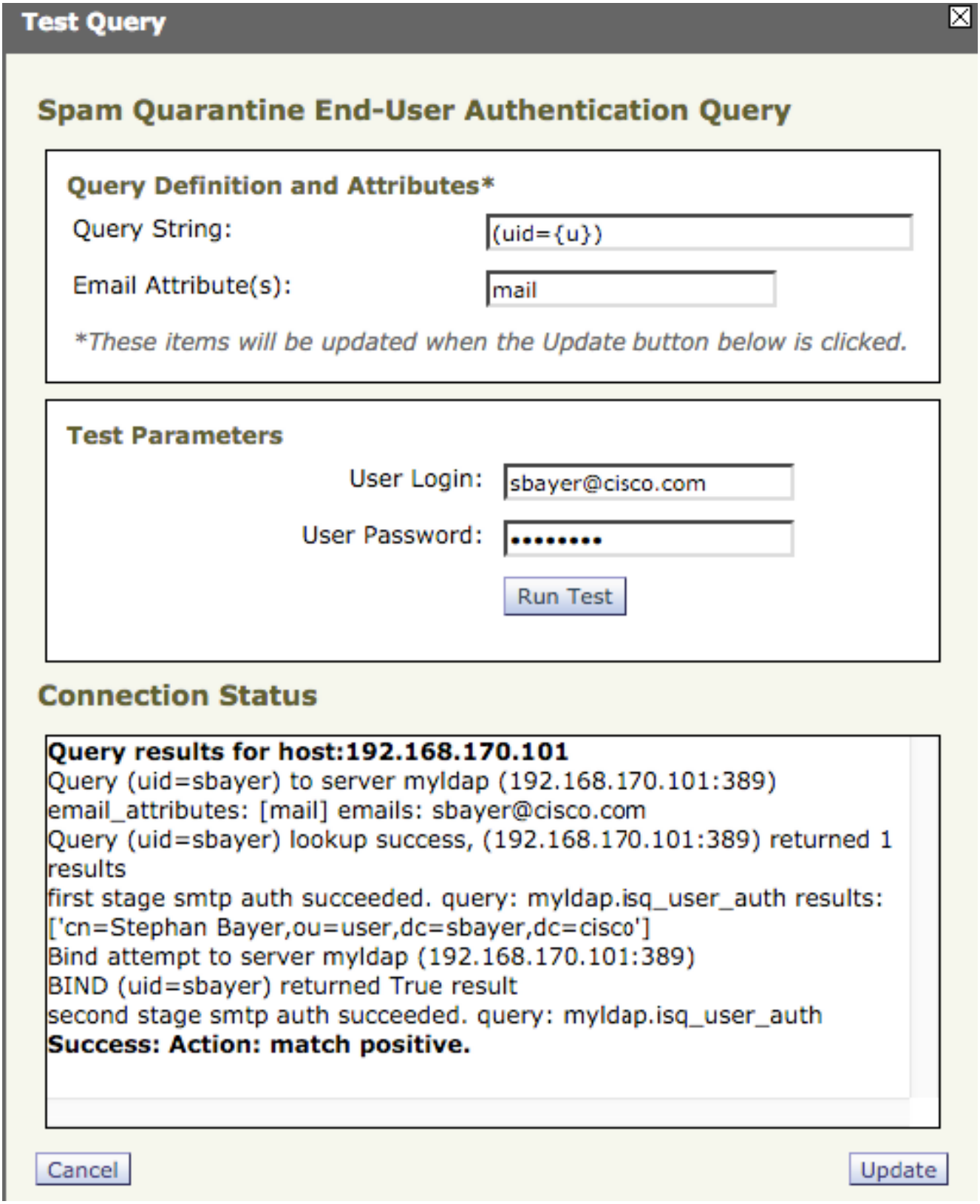
6. Soumettez et commettez les modifications.

Configurez la quarantaine Access de Spam d'utilisateur par l'intermédiaire de la requête d'authentification d'utilisateur de quarantaine de Spam

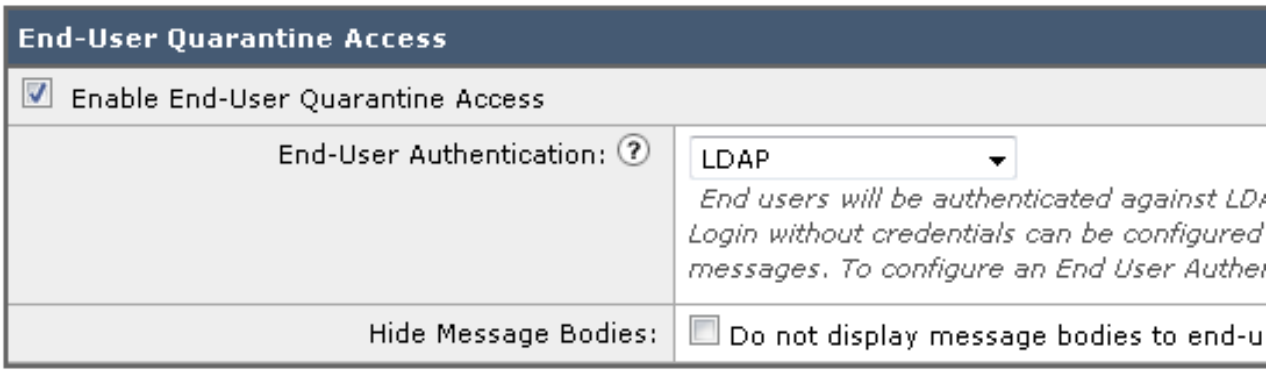
1. Sur le SMA ou l'ESA, choisissez l'**administration système > le LDAP**.
2. Ouvrez votre profil de serveur LDAP.
3. Afin de vous vérifier pouvez authentifier avec un compte de Répertoire actif, vérifient votre utilisateur de quarantaine de Spam que la requête d'authentification est activée.
4. Cochez le **désigné en tant que** case **active de requête**.



5. **Test de** clic afin de tester la requête. Appariez positif signifie que l'authentification était réussie
:



6. Soumettez et commettez les modifications.
7. Sur l'ESA, choisissez la **quarantaine de moniteur > de Spam**. Sur le SMA, naviguez vers les configurations de quarantaine de Spam afin d'exécuter les mêmes étapes.
8. **Quarantaine de Spam de** clic.
9. Cochez la case d'**Access d'End User Quarantine d'enable**.
10. Choisissez le **LDAP de la** liste déroulante d'authentification d'utilisateur.



11. Soumettez et commettez les modifications.
12. Validez que l'authentification externe est sur ESA/SMA.
13. Naviguez vers votre URL configuré précédemment dans un navigateur Web afin de valider que vous pouvez accéder à la quarantaine : https://quarantine.mydomain.com:83 https://10.10.10.10:83
14. Procédure de connexion avec votre compte de LDAP. Si ceci échoue, vérifiez le profil de LDAP d'authentification externe et activez l'End User Quarantine Access (voir les étapes précédentes).

Configurez l'accès client administratif à la quarantaine de Spam

Employez la procédure dans cette section afin de permettre aux utilisateurs administratifs avec ces rôles pour gérer des messages dans la quarantaine de Spam : Opérateur, opérateur en lecture seule, centre d'assistance, ou Guestroles, et rôles de l'utilisateur faits sur commande qui incluent l'accès à la quarantaine de Spam.

les utilisateurs niveau de l'administrateur, qui incluent l'utilisateur par défaut d'admin et envoient des utilisateurs d'administrateur, peuvent toujours accéder à la quarantaine de Spam et n'ont pas besoin d'être associés avec la configuration de quarantaine de Spam suivant cette procédure.

> Remarque: les utilisateurs niveau non peuvent accéder à des messages dans la quarantaine de Spam, mais ils ne peuvent pas éditer les configurations de quarantaine. les utilisateurs niveau de l'administrateur peuvent accéder à des messages et éditer les configurations.

Afin d'activer les utilisateurs administratifs qui n'ont pas de pleins privilèges d'administrateur de gérer des messages dans le Spam mettez en quarantaine, terminez-vous ces étapes :

1. Veillez-vous pour avoir créé des utilisateurs et pour leur avoir assigné un rôle de l'utilisateur avec l'accès à la quarantaine de Spam.
2. Sur l'appliance de Gestion de la sécurité, choisissez l'**appliance de Gestion > des services > quarantaine centralisés de Spam**.
3. Cliquez sur l'**enable ou éditez les configurations** dans la section de configurations de quarantaine de Spam.
4. Dans la région d'utilisateurs administrative de la quarantaine de Spam les configurations sectionnent, cliquent sur le lien de sélection pour des utilisateurs locaux, des utilisateurs extérieurement authentifiés, ou des rôles de l'utilisateur faits sur commande.
5. Choisissez les utilisateurs à qui vous voulez accorder l'accès pour visualiser et gérer des messages dans le Spam mettez en quarantaine.

6. Cliquez sur OK.
7. La répétition si nécessaire pour chacun des autres types d'utilisateurs administratifs l'a répertorié dans la section (utilisateurs locaux, utilisateurs extérieurement authentifiés, ou rôles de l'utilisateur faits sur commande).
8. Soumettez et commettez vos modifications.