Guía completa de la configuración de la cuarentena del Spam en el dispositivo de seguridad del correo electrónico (ESA) y el dispositivo de la Administración de seguridad (S A)

Contenido

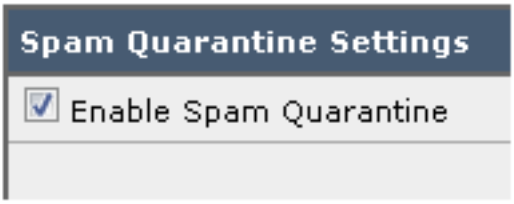
Introducción

Este documento describe cómo configurar la cuarentena del Spam en el ESA o el S A y las características asociadas: autenticación externa con el LDAP y la notificación de la cuarentena del Spam.

Procedimiento

Cuarentena local del Spam de la configuración en el ESA

1. En el ESA, elija la **cuarentena del monitor > del Spam**.
2. En la cuarentena del Spam las configuraciones seccionan, marcan la casilla de verificación de la **cuarentena del Spam del permiso** y fijan las configuraciones deseadas de la cuarentena.



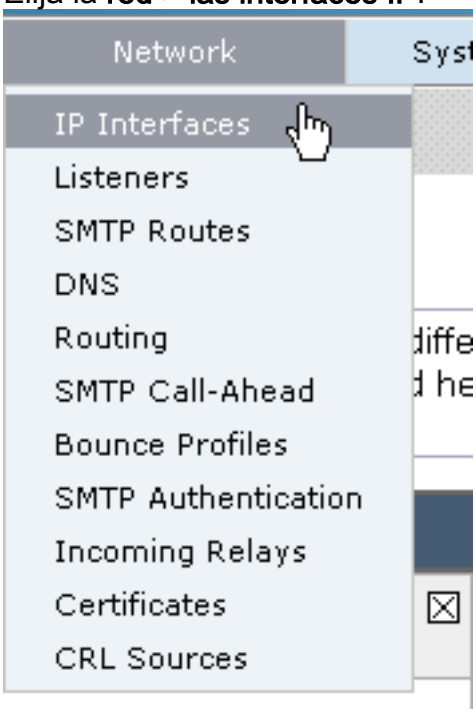
3. Elija los **Servicios de seguridad > la cuarentena del Spam**.
4. Asegúrese que la casilla de verificación **externa de la cuarentena del Spam del permiso** esté desmarcada, a menos que usted planee utilizar la cuarentena externa del Spam (véase la

sección abajo).

5. Someta y confíe los cambios.

Habilite los puertos de la cuarentena y especifique una cuarentena URL en la interfaz

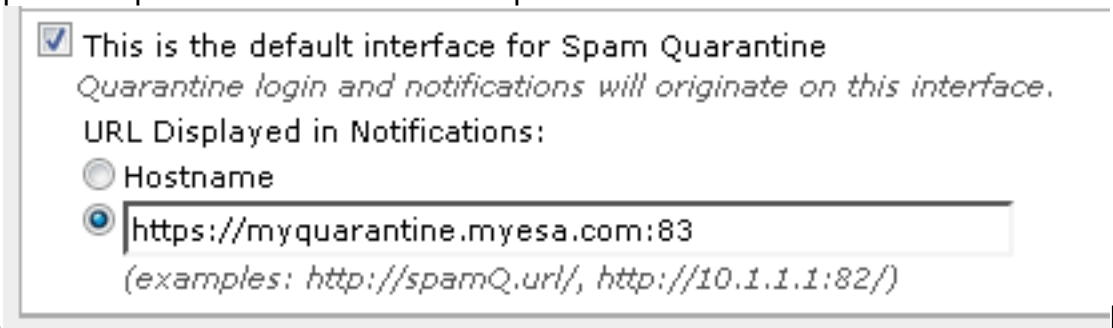
1. Elija la **red > las interfaces IP**.



2. Haga clic el nombre de la interfaz de la interfaz que usted utilizará para acceder la cuarentena. En la sección de la cuarentena del Spam, marque las casillas de verificación y especifique los puertos predeterminados o cambie como sea necesario:Mande spam la cuarentena HTTPMande spam la cuarentena
HTTPS

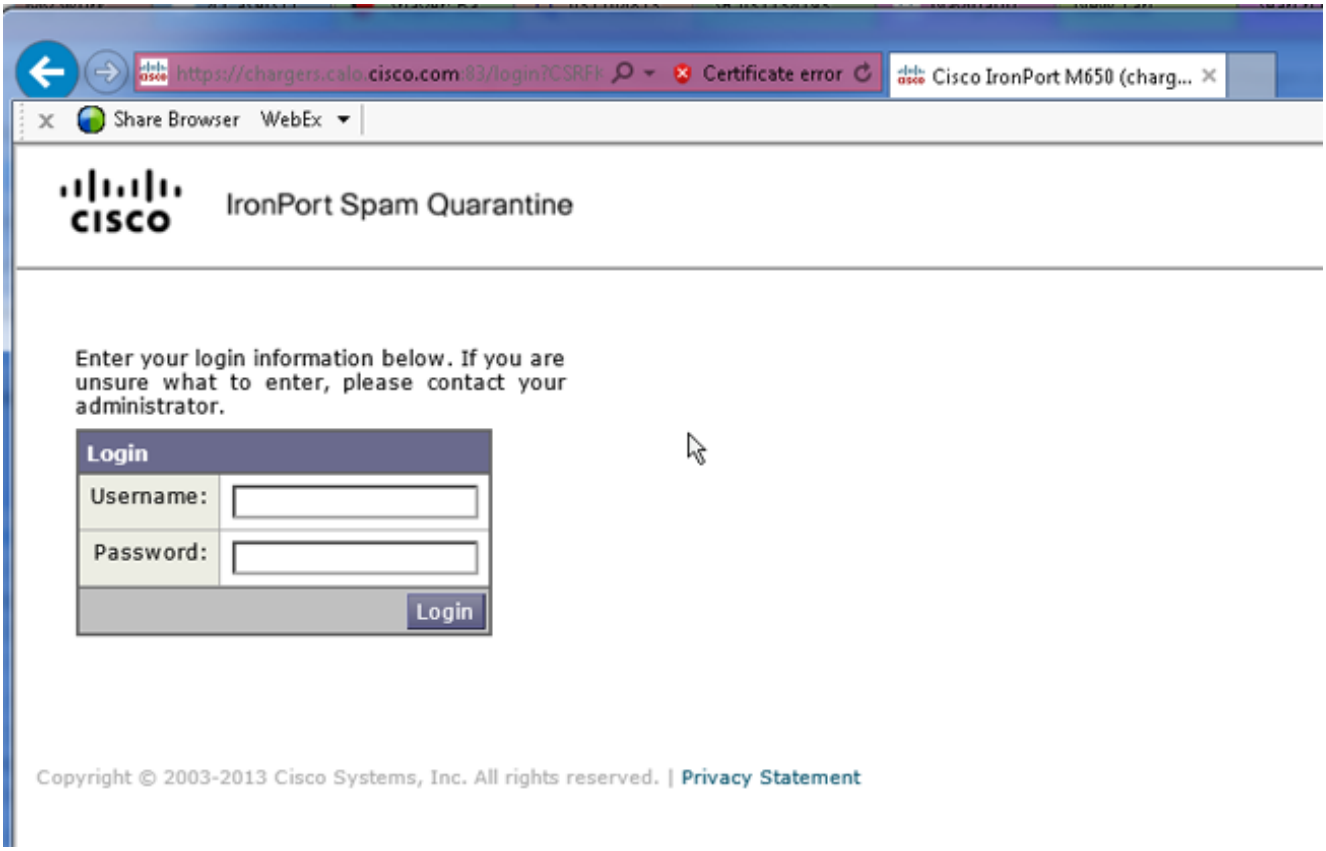
3. Marque **esto es la interfaz predeterminada para la** casilla de verificación de la **cuarentena del Spam**.
4. Bajo el “URL visualizado en las notificaciones”, por abandono el dispositivo utiliza el nombre de host del sistema (cli: **sethostname)** salvo especificación de lo contrario en la segunda opción y campo de texto del botón de radio. Este ejemplo especifica la configuración del nombre de host

predeterminado. 

Usted puede especificar una aduana URL para acceder su cuarentena del Spam. 

Note: Si usted configura la cuarentena para el acceso externo, usted necesitará un IP Address externo configurado en la interfaz o IP externa que es dirección de red traducida a un IP interno.Si usted no utiliza un nombre de host usted puede mantener el botón de radio del nombre de host marcado, pero todavía accede la cuarentena por la dirección IP solamente. Por ejemplo, https://10.10.10.10:83.

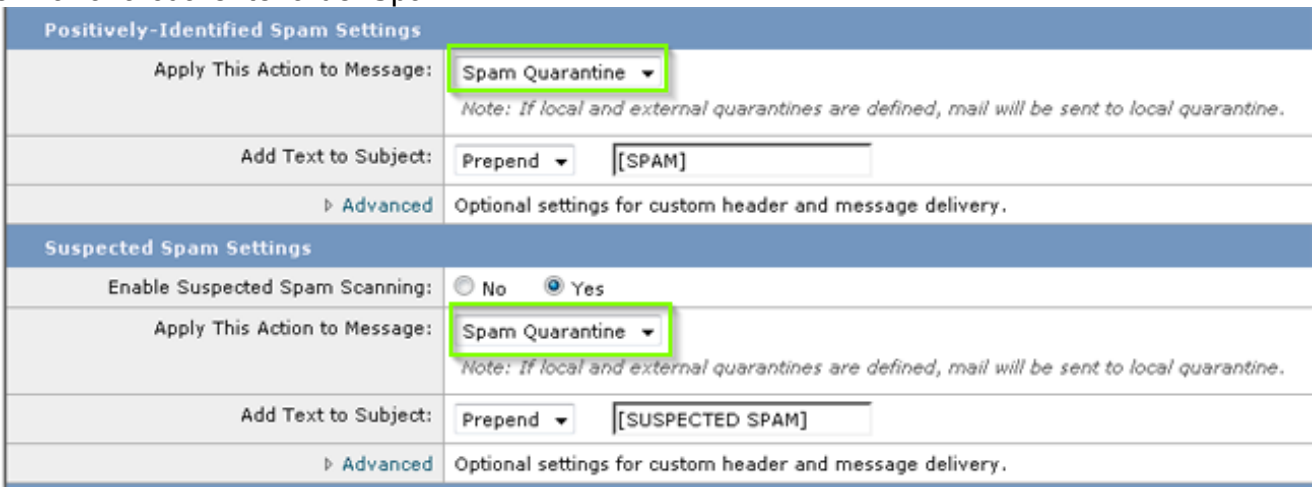
5. Someta y confíe los cambios.
6. Valide. Si usted especifica un nombre de host para la cuarentena del Spam, asegúrese que el nombre de host sea resolvable vía el Domain Name System (DNS) o el externo interno DNS. El DNS resolverá el nombre de host a su dirección IP.Si usted no consigue un resultado, marque con su administrador de la red y continúe accediendo la cuarentena por la dirección IP como el ejemplo anterior hasta el host aparece en el DNS.>nslookup quarantine.mydomain.comNavegue a su URL configurado previamente en un buscador Web para validar que usted puede acceder la cuarentena: https://quarantine.mydomain.com:83https://10.10.10.10:83



Configure el ESA para mover el Spam positivo y/o el Spam del sospechoso para mandar spam la cuarentena

Para quarantine su Spam sospechado y/o mensajes spam positivamente identificados, complete estos pasos:

1. En el ESA, haga clic las **directivas del correo > las directivas del correo entrante** y entonces la columna del anti-Spam para la política predeterminada.
2. Cambie la acción del Spam positivamente identificado o del Spam del sospechoso para enviar a la cuarentena del Spam."



3. Relance el proceso para cualquier otro ESA que usted puede ser que haya configurado para la cuarentena externa del Spam. Si usted realizó este cambio en el nivel del cluster usted no tendrá que relanzarlo pues el cambio será propagado a los otros dispositivos en el cluster.
4. Someta y confíe los cambios.
5. En este momento, el correo que habría sido entregado o caído de otra manera conseguirá quarantined.

Cuarentena externa del Spam de la configuración en el S A

Los pasos para configurar la cuarentena externa del Spam en el S A son lo mismo que la sección anterior con algunas excepciones:

1. En cada uno de sus ESA, usted necesitará inhabilitar la cuarentena local. Elija el **monitor > las cuarentenas**.
2. En su ESA, elija los **Servicios de seguridad > la cuarentena del Spam** y haga clic la **cuarentena externa del Spam del permiso**.
3. Señale el ESA a la dirección IP de su S A y especifique el puerto que usted quisiera utilizar. El valor por defecto es el puerto 6025.

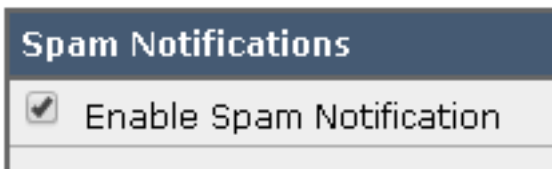
4. Asegúrese que el puerto 6025 esté abierto del ESA al S A. *Este puerto está para la salida de los mensajes quarantined de ESA > S A. Esto se puede validar por con una prueba telnet del CLI en el ESA en el puerto 6025. Si una conexión se abre y las estancias abiertas usted debe ser fijado.*

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

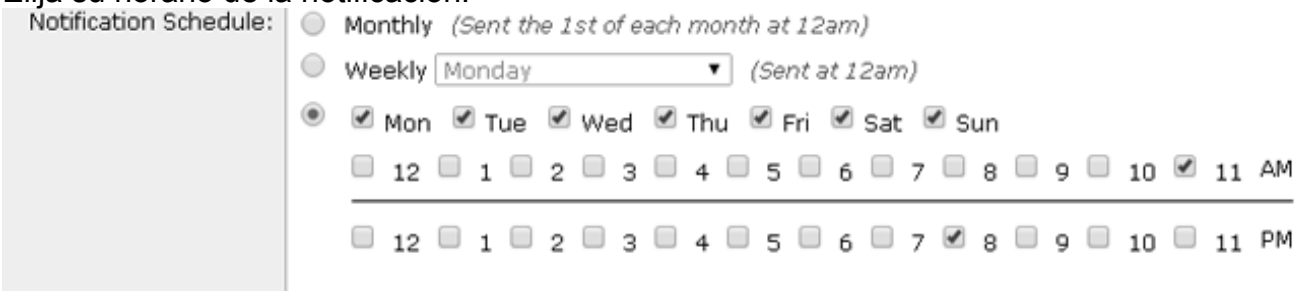
5. Asegúrese que usted haya configurado el IP/hostname para acceder la cuarentena del Spam, por ejemplo en “los puertos de la cuarentena del permiso y para especificar una cuarentena URL en la interfaz”.
6. Verifique que los mensajes lleguen a la cuarentena del Spam de sus ESA. Si la cuarentena del Spam no muestra ninguna mensajes, pudo haber un problema con la Conectividad de ESA > S A en el puerto 6025 (véase los pasos anteriores).

Configure la notificación de la cuarentena del Spam

1. En el ESA, elija la **cuarentena del monitor > del Spam**.
2. En el S A usted navegaría a las configuraciones de la cuarentena del Spam para realizar los mismos pasos.
3. **Cuarentena del Spam del** tecleo.
4. Marque la casilla de verificación de la **notificación del Spam del permiso**.



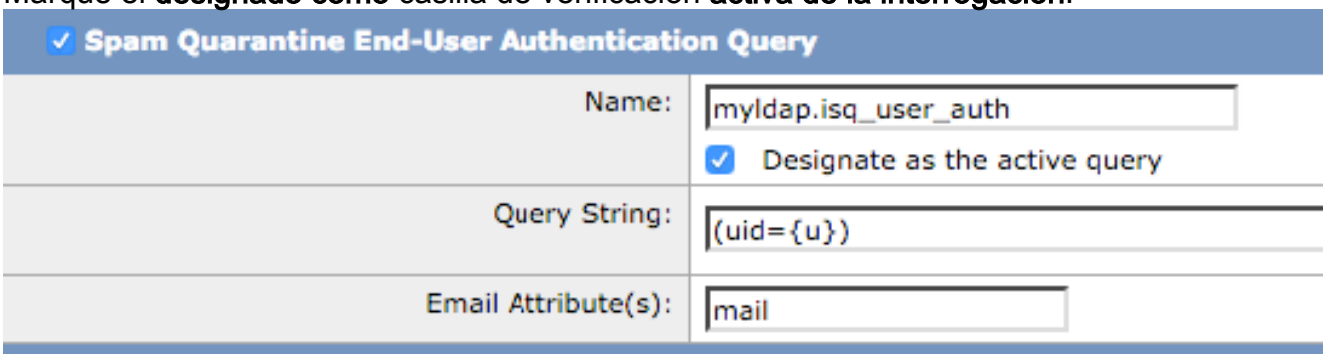
5. Elija su horario de la notificación.



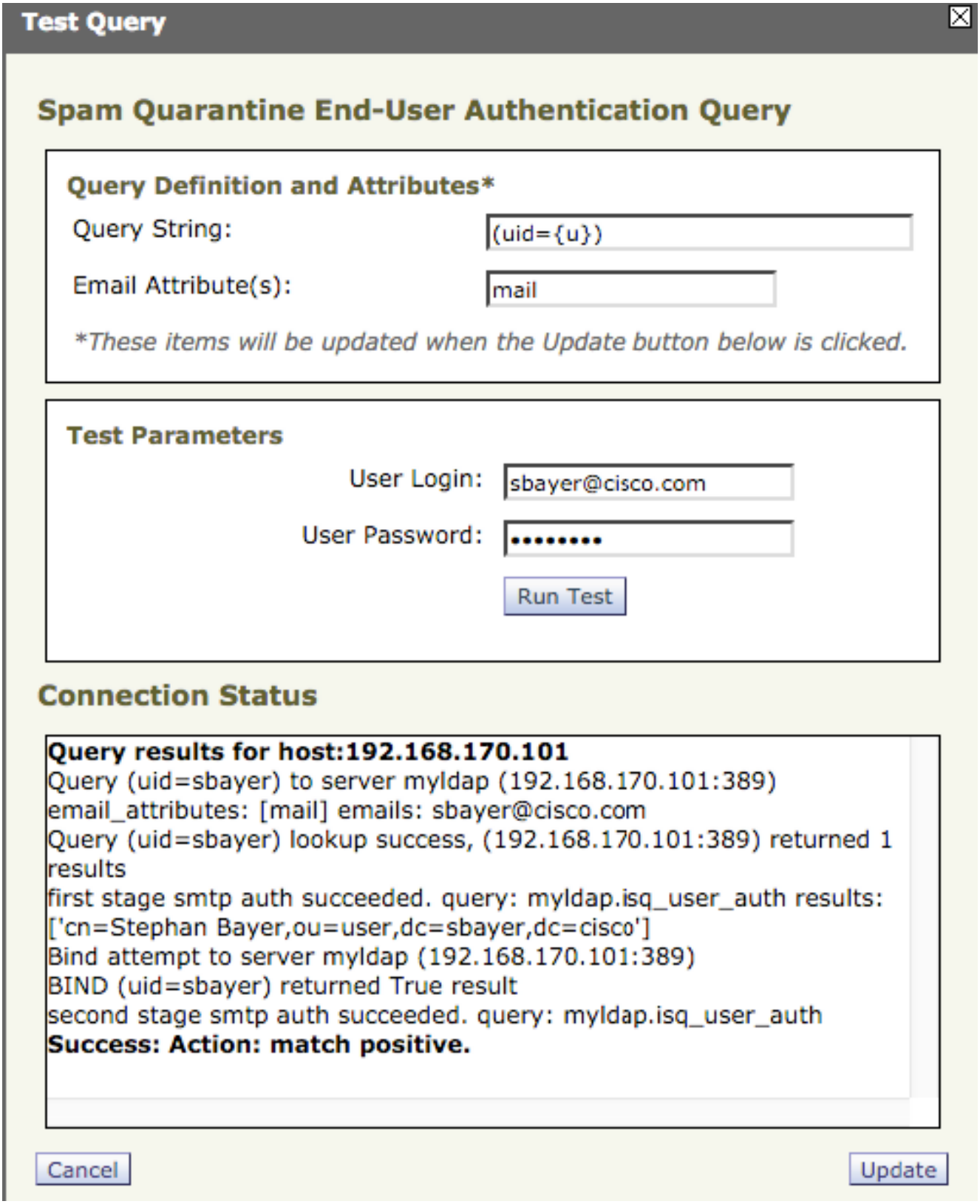
6. Someta y confíe los cambios.

Configure el acceso de la cuarentena del Spam del usuario final vía la interrogación de la autenticación del usuario final de la cuarentena del Spam

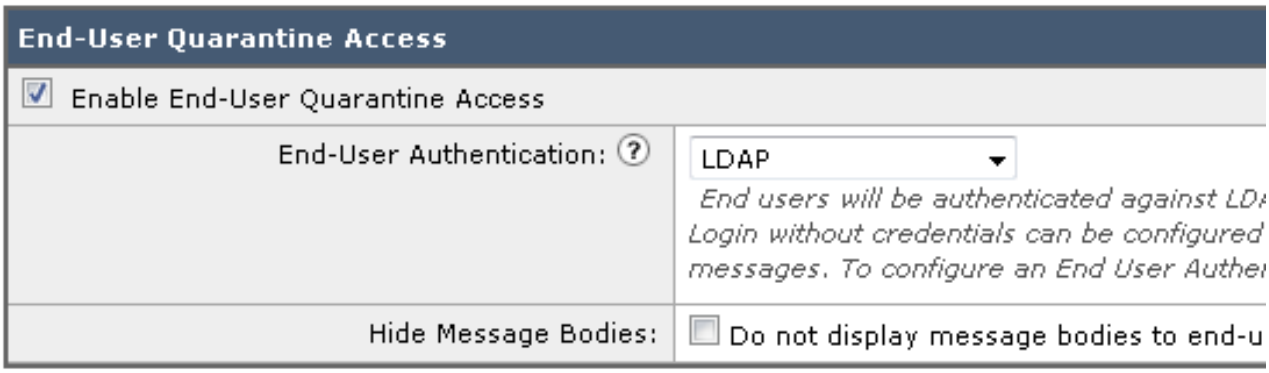
1. En el S A o el ESA, elija la **administración del sistema > el LDAP**.
2. Abra su perfil del servidor LDAP.
3. Para verificarle pueda autenticar con una cuenta de directorio activa, marcan a su usuario final de la cuarentena del Spam que se habilita la interrogación de la autenticación.
4. Marque el **designado como** casilla de verificación **activa de la interrogación**.



5. Haga clic la **prueba** para probar la interrogación. Haga juego positivo significa que la autenticación era
acertada:



6. Someta y confíe los cambios.
7. En el ESA, elija la **cuarentena del monitor > del Spam**. En el S A, navegue a las configuraciones de la cuarentena del Spam para realizar los mismos pasos.
8. Haga clic la **cuarentena del Spam**.
9. Marque el cuadro de **verificación de acceso de la cuarentena del usuario final del permiso**.
10. Elija el **LDAP de la** lista desplegable de la autenticación del usuario final.



11. Someta y confíe los cambios.
12. Valide que la autenticación externa está en ESA/SMA.
13. Navegue a su URL configurado previamente en un buscador Web para validar que usted puede acceder la cuarentena: https://quarantine.mydomain.com:83 https://10.10.10.10:83
14. Login con su cuenta LDAP. Si esto falla, marque el perfil de la autenticación externa LDAP y habilite el acceso de la cuarentena del usuario final (véase los pasos anteriores).

Configure el acceso de usuario administrador a la cuarentena del Spam

Utilice el procedimiento en esta sección para permitir que los usuarios administradores con estos papeles manejen los mensajes en la cuarentena del Spam: Operador, operador solo lectura, escritorio de ayuda, o Guestroles, y rol del usuario de encargo que incluyen el acceso a la cuarentena del Spam.

Los usuarios con nivel de administrador, que incluyen al Usuario administrador predeterminado y envían por correo electrónico a los usuarios administradores, pueden acceder siempre la cuarentena del Spam y no necesitan ser asociados a la característica de la cuarentena del Spam usando este procedimiento.

> **Note**: los usuarios del NON-Administrador-nivel pueden acceder los mensajes en la cuarentena del Spam, pero no pueden editar las configuraciones de la cuarentena. Los usuarios con nivel de administrador pueden acceder los mensajes y editar las configuraciones.

Para habilitar a los usuarios administradores que no tienen privilegios de administrador completos de manejar los mensajes en el Spam Quarantine, complete estos pasos:

1. Aseegurese le haber creado a los usuarios y haber asignadoles un rol del usuario con el acceso a la cuarentena del Spam.
2. En el dispositivo de la Administración de seguridad, elija el **dispositivo de la Administración > los servicios > cuarentena centralizados del Spam**.
3. Haga clic el **permiso o edite las configuraciones** en la sección de las configuraciones de la cuarentena del Spam.
4. En el área de usuarios administradores de las configuraciones de la cuarentena del Spam seccione, haga clic el link de la selección para los usuarios locales, externamente los usuarios autenticados, o los rol del usuario de encargo.
5. Elija a los usuarios a quienes usted quiere conceder el acceso para ver y manejar los

mensajes en el Spam Quarantine.
6. Click OK.
7. La repetición si es necesario para cada uno de los otros tipos de usuarios administradores enumeró en la sección (usuarios locales, externamente los usuarios autenticados, o los rol del usuario de encargo).
8. Someta y confíe sus cambios.