Guia detalhado da instalação da quarentena do Spam na ferramenta de segurança do email (ESA) e no dispositivo do Gerenciamento de segurança (S A)

Índice

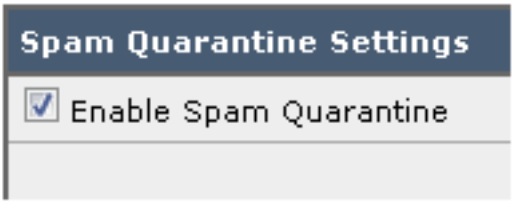
Introdução

Este documento descreve como configurar a quarentena do Spam no ESA ou o S A e as características associadas: autenticação externa com LDAP e notificação da quarentena do Spam.

Procedimento

Configurar a quarentena local do Spam no ESA

1. No ESA, escolha a **quarentena do monitor > do Spam**.
2. Na quarentena do Spam os ajustes secionam, verificam a caixa de verificação da **quarentena do Spam da possibilidade** e ajustam os ajustes desejados da quarentena.

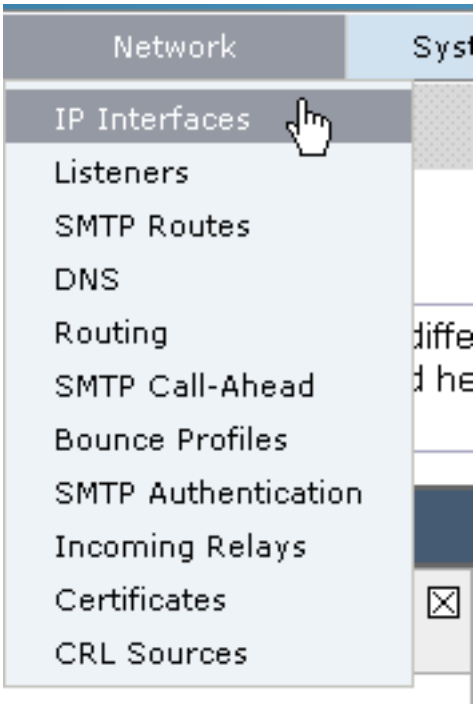


3. Escolha **Serviços de segurança > quarentena do Spam**.
4. Assegure-se de que a caixa de verificação **externo da quarentena do Spam da possibilidade** esteja desmarcada, a menos que você planejar usar a quarentena externo do Spam (veja a seção abaixo).

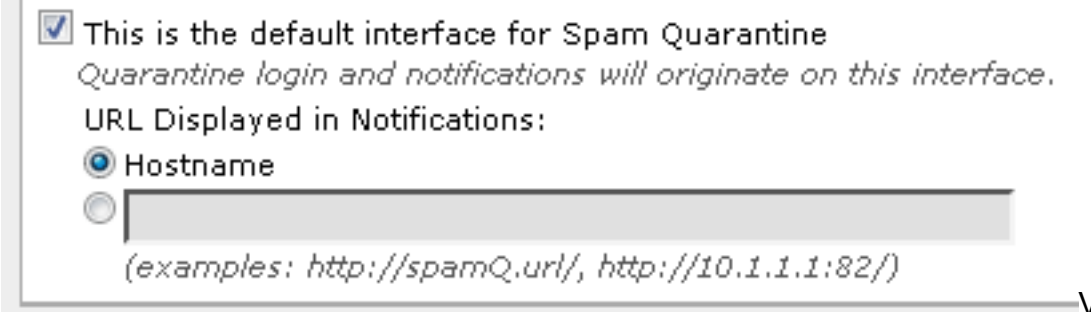
5. Submeta e comprometa mudanças.

Permita portas da quarentena e especifique uma quarentena URL na relação

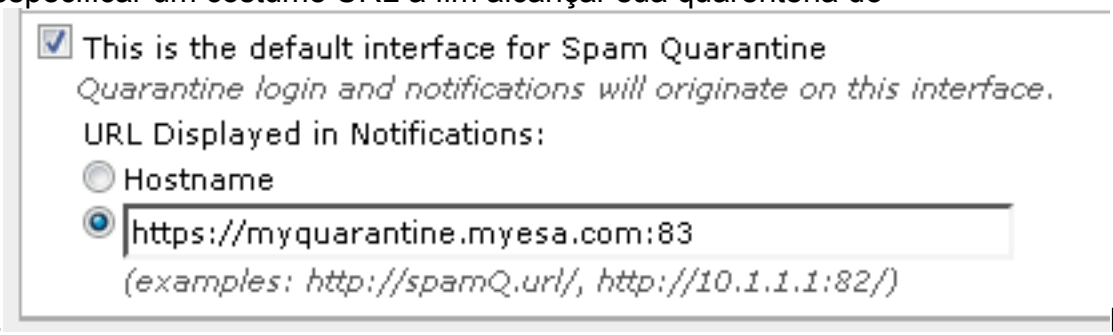
1. Escolha a **rede > as interfaces IP**.



2. Clique o nome da relação da relação que você se usará a fim alcançar a quarentena. Na seção da quarentena do Spam, verifique as caixas de seleção e especifique portas padrão ou mude-as como necessário:Spam a quarentena HTTPSpam a quarentena HTTPS

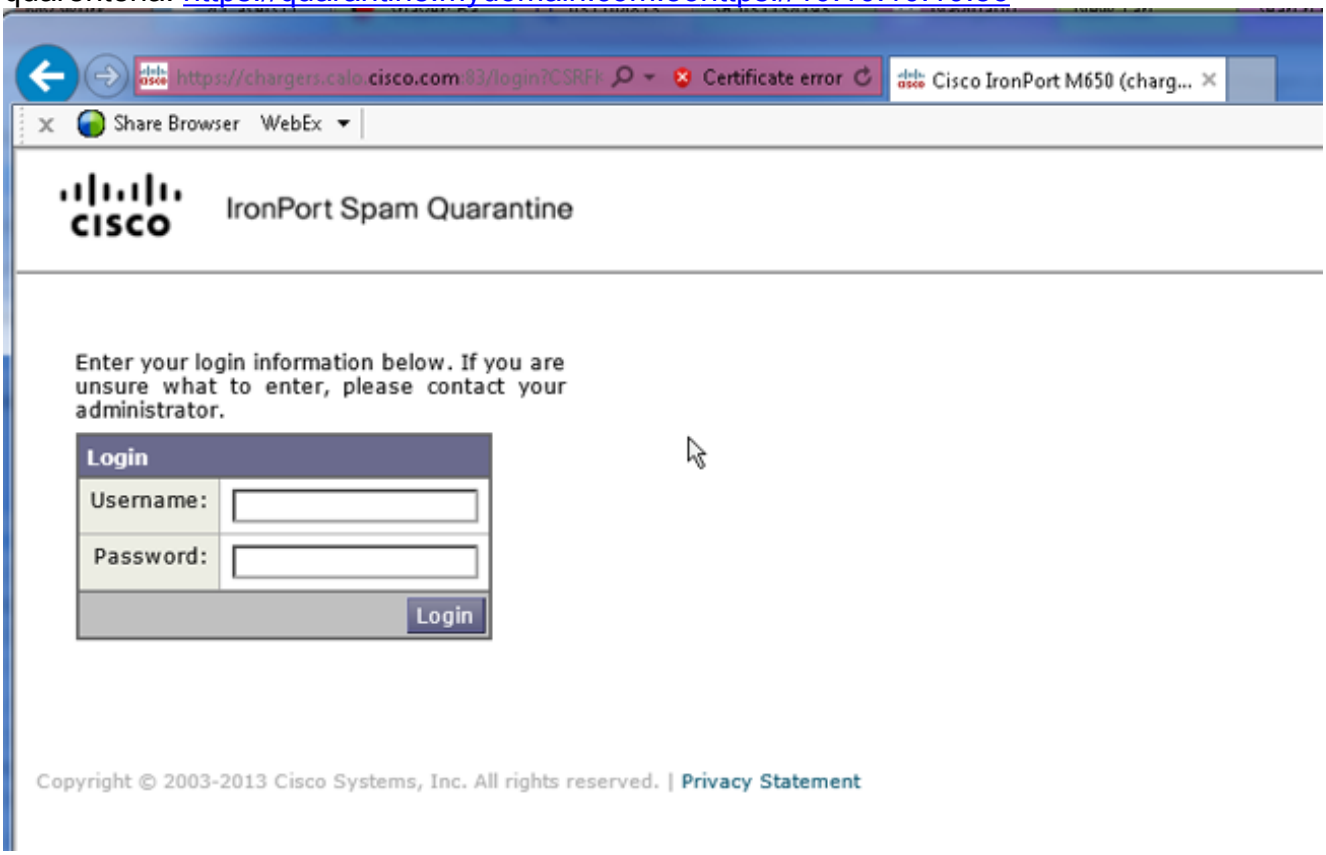
3. Verifique **isto é a interface padrão para a** caixa de verificação da **quarentena do Spam**.
4. Sob a “URL indicada nas notificações”, à revelia o dispositivo usa o hostname do sistema (CLI: **sethostname)** salvo disposição em contrário na segundos opção e campo de texto do botão de rádio. Este exemplo especifica o ajuste do hostname de padrão. 

Você

pode especificar um costume URL a fim alcançar sua quarentena do Spam. 

Note: Se você configura a quarentena para o acesso externo, você precisará um endereço IP externo configurado na relação ou em um IP externo que é endereço de rede traduzido a um IP interno.Se você não usa um hostname você pode manter o botão de rádio do hostname verificado, mas ainda alcança a quarentena pelo endereço IP de Um ou Mais Servidores Cisco ICM NT somente. Por exemplo, https://10.10.10.10:83.

5. Submeta e comprometa mudanças.
6. Valide. Se você especifica um hostname para a quarentena do Spam, assegure-se de que o hostname esteja solucionável através do Domain Name System (DNS) interno ou do DNS externo. O DNS resolverá o hostname a seu endereço IP de Um ou Mais Servidores Cisco ICM NT.Se você não obtém um resultado, verifique com seu administrador de rede e continue a alcançar a quarentena pelo endereço IP de Um ou Mais Servidores Cisco ICM NT como o exemplo anterior até o host aparece no DNS.>nslookup quarantine.mydomain.comNavegue a sua URL configurada previamente em um navegador da Web a fim validar que você pode alcançar a quarentena: https://quarantine.mydomain.com:83https://10.10.10.10:83

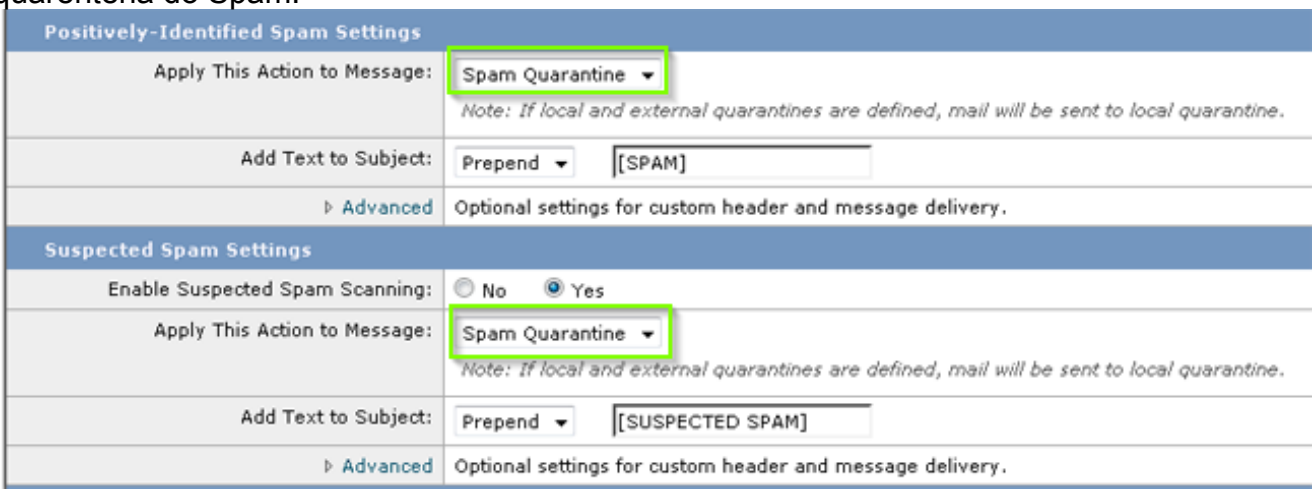


Configurar o ESA para mover o Spam positivo e/ou o Spam suspeito para spam a quarentena

A fim quarantine seus Spam suspeito e/ou mensagens positivamente identificadas do Spam,

termine estas etapas:

1. No ESA, clique **políticas do correio > políticas do correio recebido** e então a coluna do anti-Spam para a política padrão.
2. Mude a ação do Spam positivamente identificado ou do Spam suspeito para enviar à quarentena do Spam.”

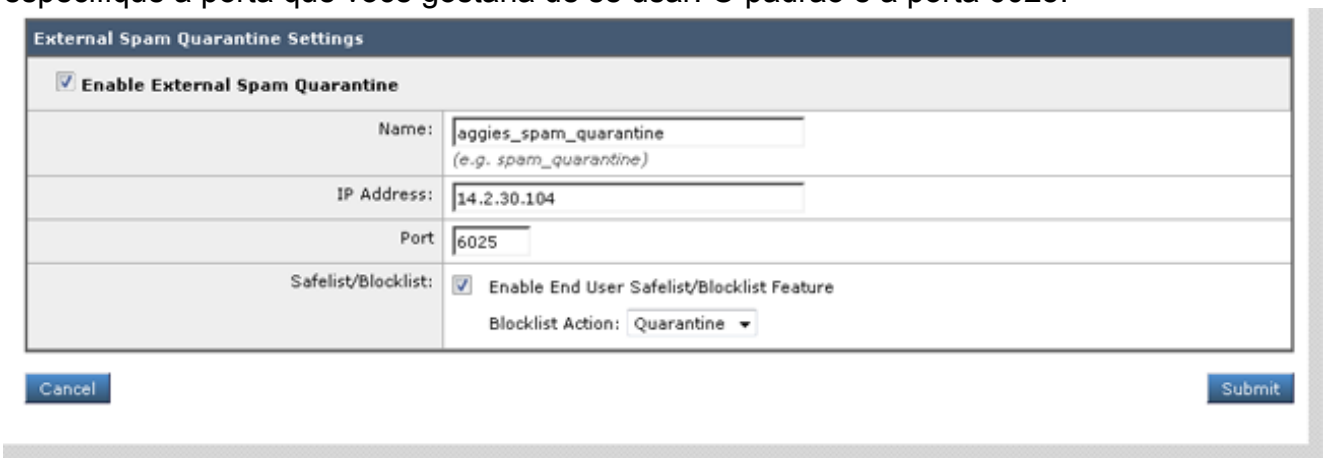


3. Repita o processo para todos os outros ESA que você possa ter configurado para a quarentena externo do Spam. Se você fez esta mudança a nível do conjunto você não terá que repeti-lo porque a mudança será propagada aos outros dispositivos no conjunto.
4. Submeta e comprometa mudanças.
5. Neste momento, o correio que de outra maneira seria entregado ou deixado cair obterá quarantined.

Configurar a quarentena externo do Spam no S A

As etapas para configurar a quarentena externo do Spam no S A são as mesmas que a seção anterior com algumas exceções:

1. Em cada um de seus ESA, você precisará de desabilitar a quarentena local. Escolha o **monitor > as quarentena**.
2. Em seu ESA, escolha **Serviços de segurança > quarentena do Spam** e o clique **permite a quarentena externo do Spam**.
3. Aponte o ESA ao endereço IP de Um ou Mais Servidores Cisco ICM NT de seu S A e especifique a porta que você gostaria de se usar. O padrão é a porta 6025.



4. Assegure-se de que a porta 6025 esteja aberta do ESA ao S A. *Esta porta é para a entrega de mensagens quarantined de ESA > S A. Isto pode ser validado com por um teste do telnet*

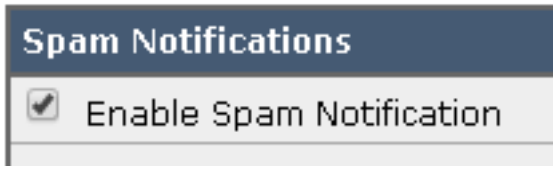
do CLI no ESA na porta 6025. Se uma conexão abre e as estadas abertas você deve ser ajustado.

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

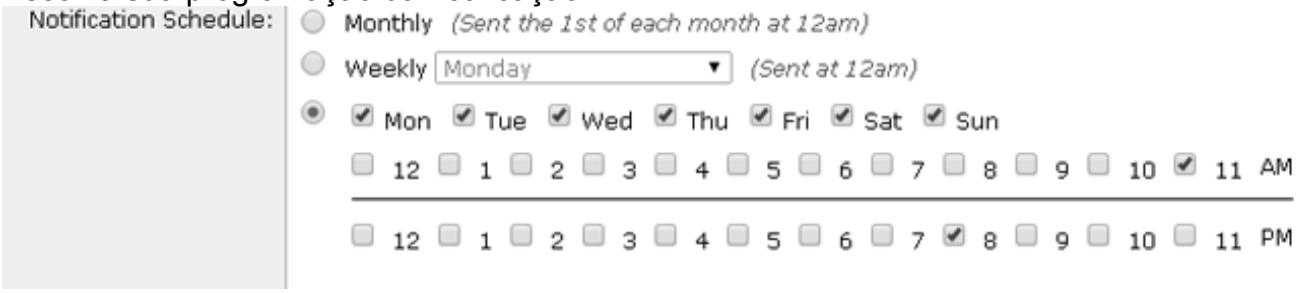
5. Assegure que você configurou o IP/hostname para alcançar a quarentena do Spam, como em “permita portas da quarentena e especifique uma quarentena URL na relação”.
6. Verifique que as mensagens chegam à quarentena do Spam de seus ESA. Se a quarentena do Spam não mostra nenhuma mensagens, pôde haver uma edição com Conectividade de ESA > S A na porta 6025 (veja etapas precedentes).

Configurar a notificação da quarentena do Spam

1. No ESA, escolha a **quarentena do monitor > do Spam**.
2. No S A você navegaria aos ajustes da quarentena do Spam a fim executar as mesmas etapas.
3. **Quarentena do Spam do** clique.
4. Verifique a caixa de verificação da **notificação do Spam da possibilidade**.



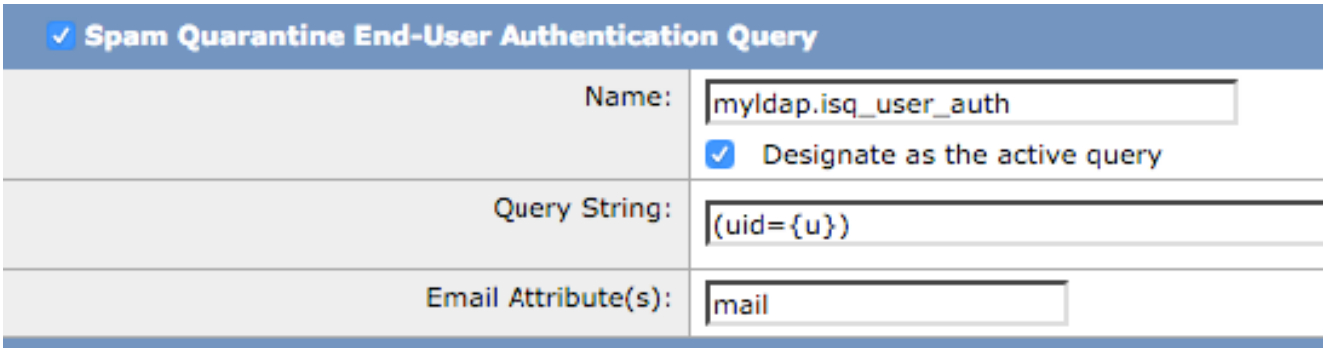
5. Escolha sua programação da notificação.



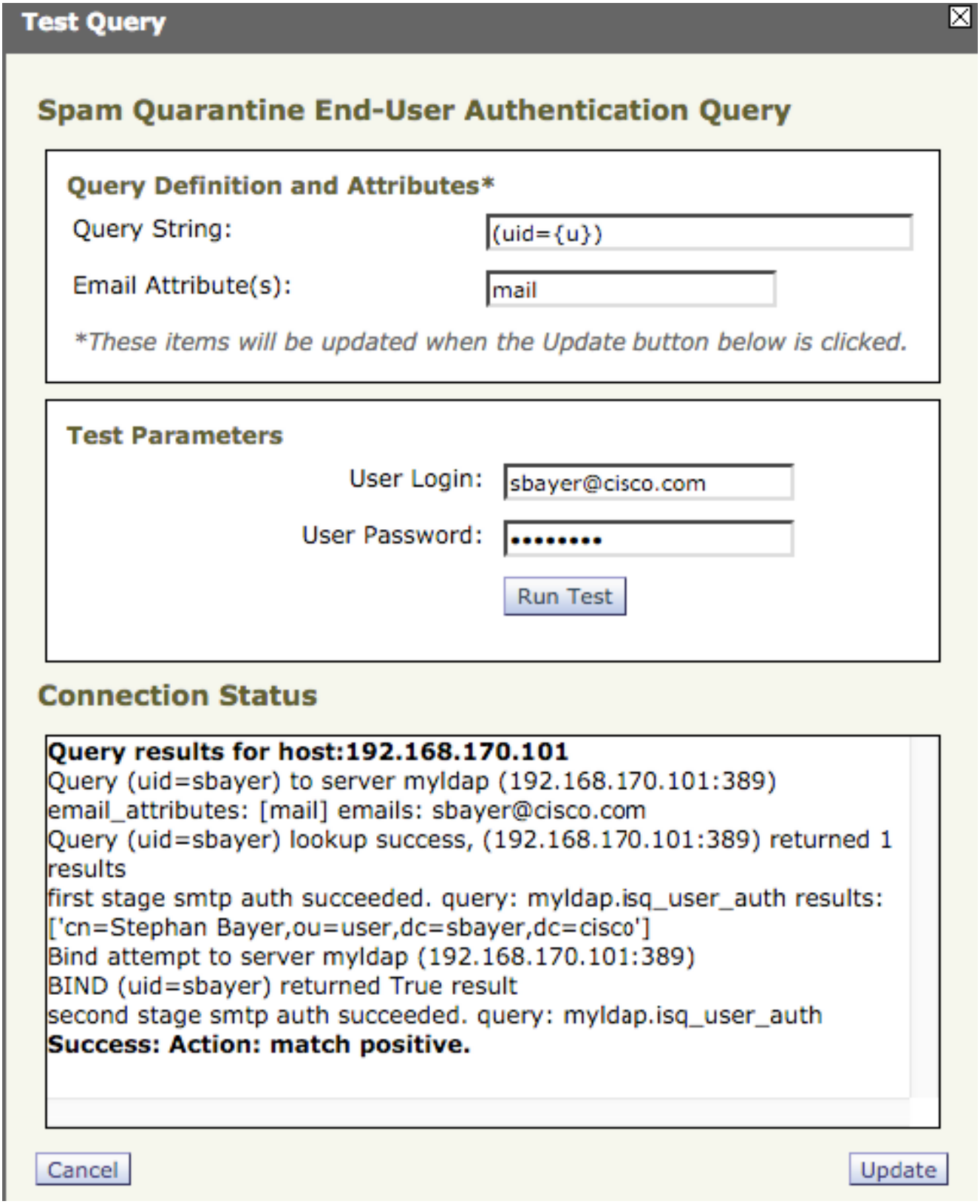
6. Submeta e comprometa mudanças.

Configurar o acesso da quarentena do Spam do utilizador final através da pergunta da autenticação do utilizador final da quarentena do Spam

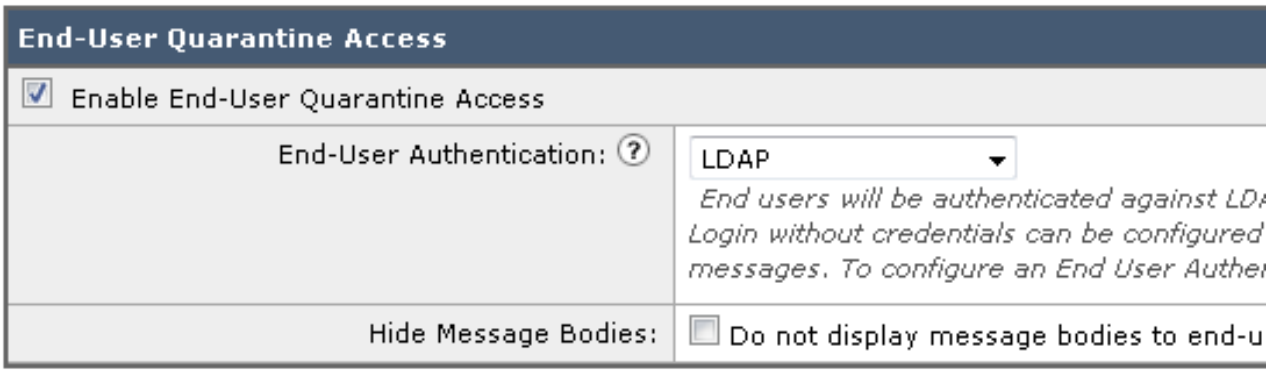
1. No S A ou no ESA, escolha a **administração do sistema > o LDAP**.
2. Abra seu perfil do servidor ldap.
3. A fim verificá-lo possa autenticar com uma conta de diretório ativo, verificam seu utilizador final da quarentena do Spam a pergunta da autenticação que é permitida.
4. Verifique o **designado como a** caixa de verificação **ativa da pergunta**.



5. Clique o **teste** a fim testar a pergunta. Combine positivo significa que a autenticação era bem sucedida:



6. Submeta e comprometa mudanças.
7. No ESA, escolha a **quarentena do monitor > do Spam**. No S A, navegue aos ajustes da quarentena do Spam a fim executar as mesmas etapas.
8. Clique a **quarentena do Spam**.
9. Verifique a caixa de **verificação de acesso da quarentena do utilizador final da possibilidade**.
10. Escolha o **LDAP da** lista de drop-down da autenticação do utilizador final.



11. Submeta e comprometa mudanças.
12. Valide que a autenticação externa está em ESA/SMA.
13. Navegue a sua URL configurada previamente em um navegador da Web a fim validar que você pode alcançar a quarentena: https://quarantine.mydomain.com:83 https://10.10.10.10:83
14. Início de uma sessão com sua conta LDAP. Se isto falha, verifique o perfil da autenticação externa LDAP e permita o acesso da quarentena do utilizador final (veja etapas precedentes).

Configurar o acesso de usuário administrativo à quarentena do Spam

Use o procedimento nesta seção a fim permitir que os usuários administrativos com estes papéis controlem mensagens na quarentena do Spam: Operador, operador de leitura apenas, help desk, ou Guestroles, e papéis de usuário feitos sob encomenda que incluem o acesso à quarentena do Spam.

os usuários do Administrador-nível, que incluem os usuários do administrador do usuário admin e do email do padrão, podem sempre alcançar a quarentena do Spam e não precisam de ser associados com a característica da quarentena do Spam usando este procedimento.

> **Note**: os usuários do NON-Administrador-nível podem alcançar mensagens na quarentena do Spam, mas não podem editar os ajustes da quarentena. os usuários do Administrador-nível podem alcançar mensagens e editar os ajustes.

A fim permitir os usuários administrativos que não têm privilégios do administrado completos controlar mensagens no Spam Quarantine, termine estas etapas:

1. Certifique-se de você ter criado usuários e ter-lhes atribuído um papel de usuário com acesso à quarentena do Spam.
2. No dispositivo do Gerenciamento de segurança, escolha o **dispositivo do Gerenciamento > serviços > quarentena centralizados do Spam**.
3. O clique **permite ou edita ajustes na** seção dos ajustes da quarentena do Spam.
4. Na área de usuários administrativa dos ajustes da quarentena do Spam secione, clique o link da seleção para usuários locais, externamente usuários autenticados, ou papéis de usuário feitos sob encomenda.
5. Escolha os usuários a quem você quer conceder o acesso para ver e para controlar mensagens no Spam Quarantine.
6. Click **OK**.

7. Repita se necessário para cada um dos outros tipos de usuários administrativos alistados na seção (usuários locais, externamente usuários autenticados, ou papéis de usuário feitos sob encomenda).
8. Submeta e comprometa suas mudanças.