在电子邮件安全工具(ESA)和安全管理设备(SMA)的全面的垃圾邮件检疫设置指南

目录

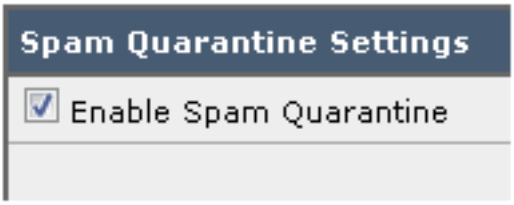
简介

本文描述如何配置在ESA的垃圾邮件检疫或SMA和相关的功能：与LDAP和垃圾邮件检疫通知的外部验证。

步骤

配置在ESA的本地垃圾邮件检疫

1. 在ESA，请选择**监视器>垃圾邮件检疫**。
2. 在垃圾邮件检疫设置部分，请检查**Enable (event)垃圾邮件检疫**复选框并且设了希望的检疫设置。

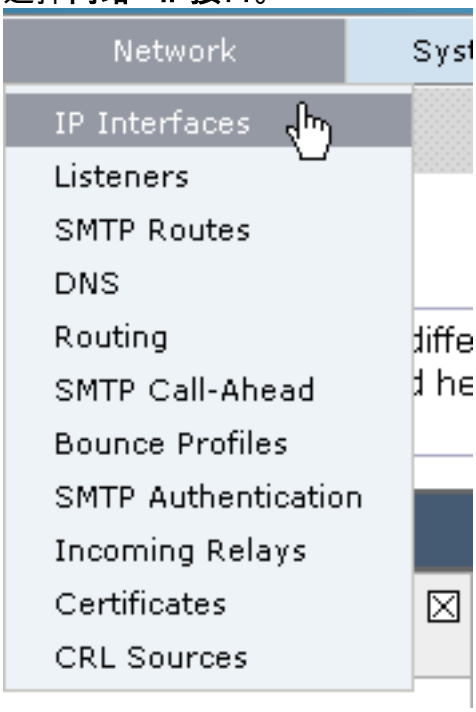


3. 选择**安全服务>垃圾邮件检疫**。
4. 保证**外部垃圾邮件检疫**复选框非选定的**Enable (event)**，除非计划使用外部垃圾邮件检疫(请参阅下面的部分)。

5. 提交并且确认更改。

启用检疫端口并且指定检疫URL在接口

1. 选择**网络> IP接口**。



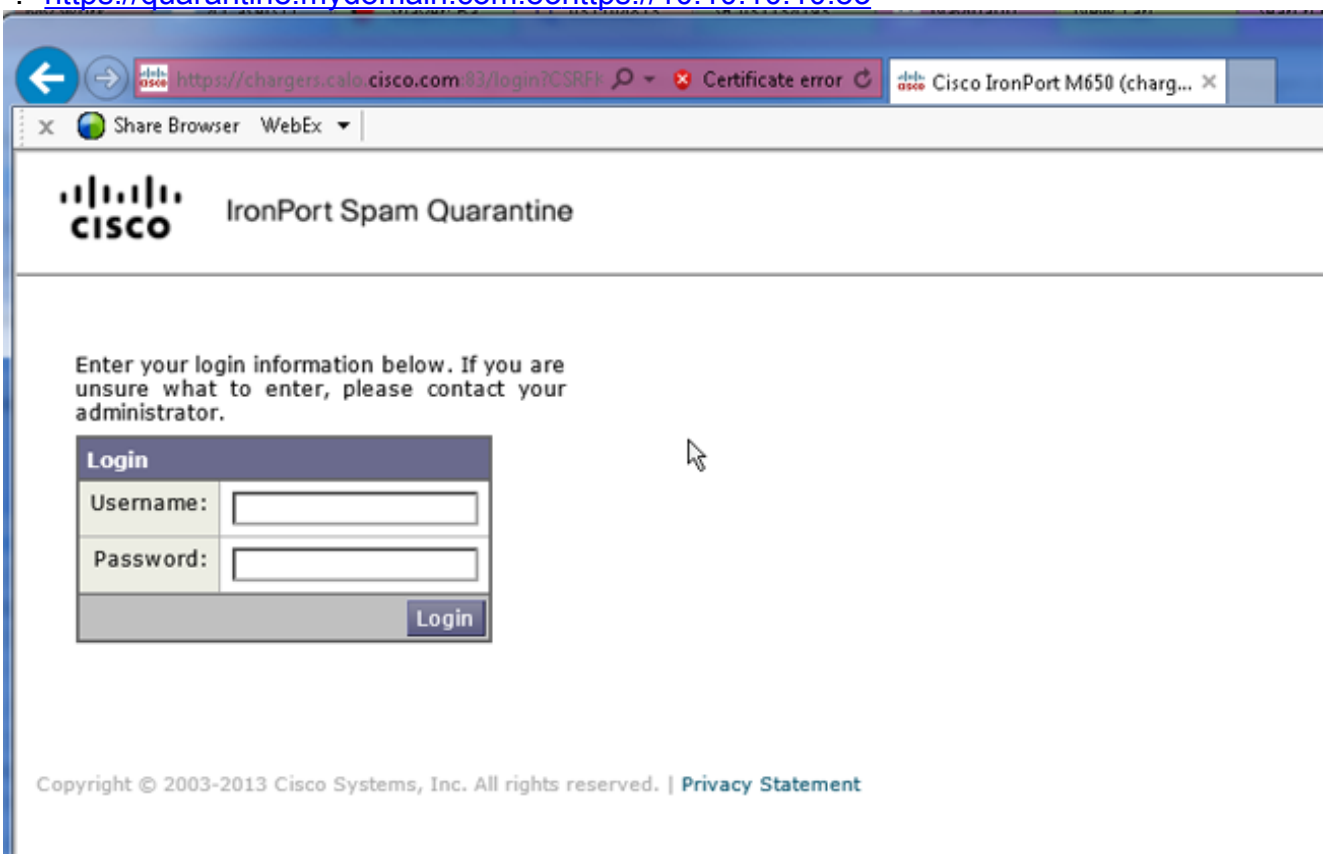
2. 点击您将使用为了访问检疫接口的接口名称。 在垃圾邮件检疫部分，请检查复选框并且指定默认端口或更改如所需求：发送消息到新闻组检疫HTTP发送消息到新闻组检疫HTTPS

3. 检查**这是垃圾邮件检疫**复选框的**默认接口**。
4. 默认情况下在“在通知显示的URL下”，设备使用系统主机名(cli ： **sethostname)**除非另外说明在第二个单选按钮选项和文本字段。 此示例指定默认主机名设置。

您能指定自定义URL为了访问您的垃圾邮件检疫。

Note:如果配置外部访问的检疫，您将需要在是翻译的网络地址对内部IP的接口或外部IP配置的外部IP地址。如果不使用一主机名您能保持主机名单选按钮被检查，但是由仅IP地址仍然访问检疫。例如，https://10.10.10.10:83。

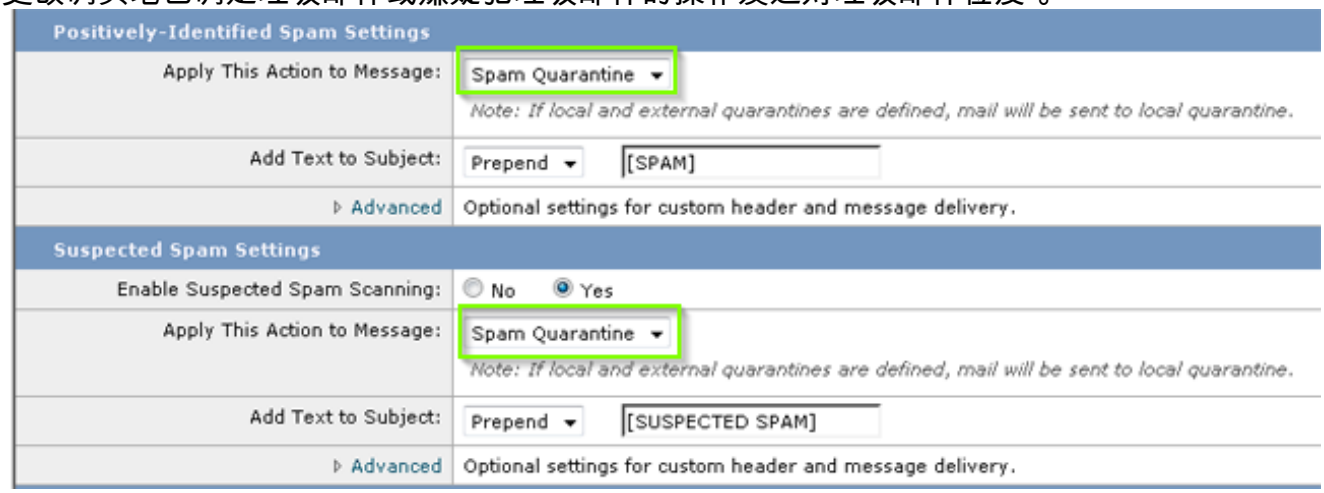
5. 提交并且确认更改。
6. 验证。 如果指定垃圾邮件检疫的一主机名，请保证主机名通过内部域名系统(DNS)或外部DNS是可解决。DNS将解决主机名对您的IP地址。如果不取得结果，请与您的网络管理员协商并且继续由IP地址访问检疫类似前一个示例，直到主机在DNS出现。>nslookup quarantine.mydomain.com导航对在Web浏览器以前配置的您的URL为了验证您能访问检疫：https://quarantine.mydomain.com:83https://10.10.10.10:83



配置ESA移动正垃圾邮件和嫌疑犯垃圾邮件发送消息到新闻组检疫

为了检疫您可疑的垃圾邮件和确实地识别的垃圾邮件消息，请完成这些步骤：

1. 在ESA，请点击**邮件"Policies" >流入的邮件"Policies"**然后反垃圾邮件列默认策略的。
2. 更改确实地已确定垃圾邮件或嫌疑犯垃圾邮件的操作发送对垃圾邮件检疫"。



3. 重复您也许为外部垃圾邮件检疫已经配置的其他ESAs的进程。如果做了此变动在集群级别您不会必须重复它，因为将传播变化对其他设备在集群上。
4. 提交并且确认更改。

5. 这时，将否则传送或丢弃了的邮件将获得检疫。

配置在SMA的外部垃圾邮件检疫

配置在SMA的外部垃圾邮件检疫的步骤是相同的象前面部分有一些例外：

1. 在你的每一ESAs，您将需要禁用本地检疫。选择**监视器>检疫**。
2. 在您的ESA，请选择**安全服务>垃圾邮件检疫**并且点击**Enable (event)外部垃圾邮件检疫**。
3. 指向ESA您的SMA的IP地址并且指定您希望使用的端口。默认是波尔特6025。

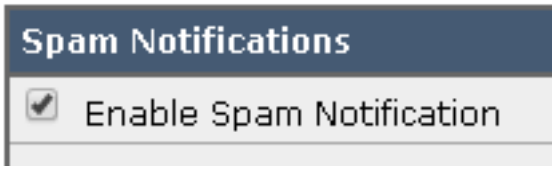
4. 保证波尔特6025从ESA是开放的到SMA。*此端口是为被检疫的消息交付从ESA > SMA。这可以由与从CLI的一telnet测验验证在端口6025的ESA。如果连接打开，并且开放的逗留您应该设置。*

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

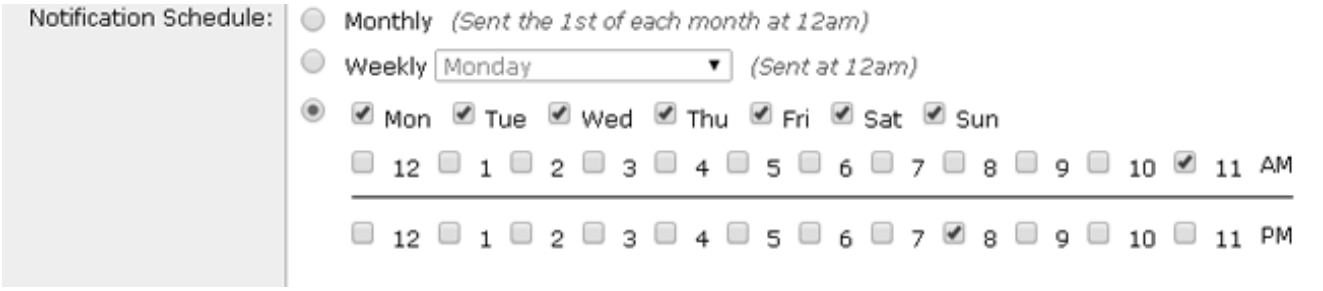
5. 在“Enable (event)检疫端口保证您配置IP/hostname -访问垃圾邮件检疫，例如和指定检疫URL在接口”。
6. 验证消息到达对从您的ESAs的垃圾邮件检疫。如果垃圾邮件检疫不表示任何消息，也许有与连接的一个问题从在端口6025的ESA > SMA (请参阅上一个步骤)。

配置垃圾邮件检疫通知

1. 在ESA，请选择**监视器>垃圾邮件检疫**。
2. 在SMA您会导航对垃圾邮件检疫设置为了执行同样步骤。
3. 点击**垃圾邮件检疫**。
4. 检查**Enable (event)垃圾邮件通知**复选框。



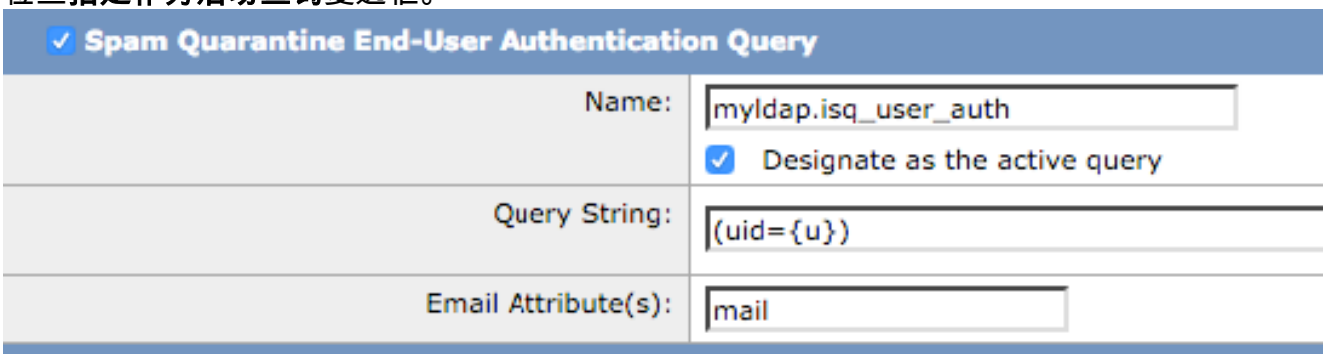
5. 选择您的通知日程。



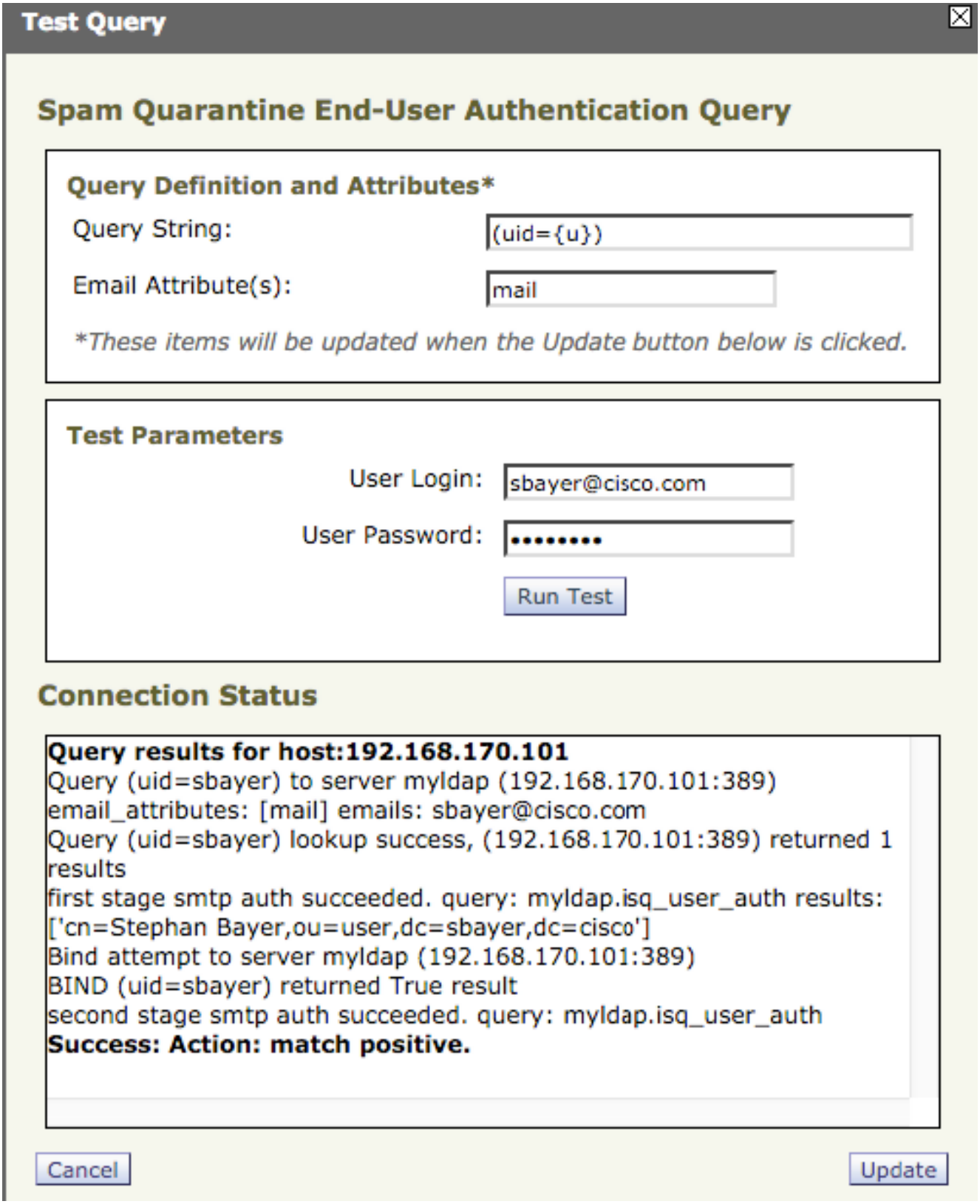
6. 提交并且确认更改。

通过垃圾邮件检疫最终用户验证查询配置最终用户垃圾邮件检疫访问

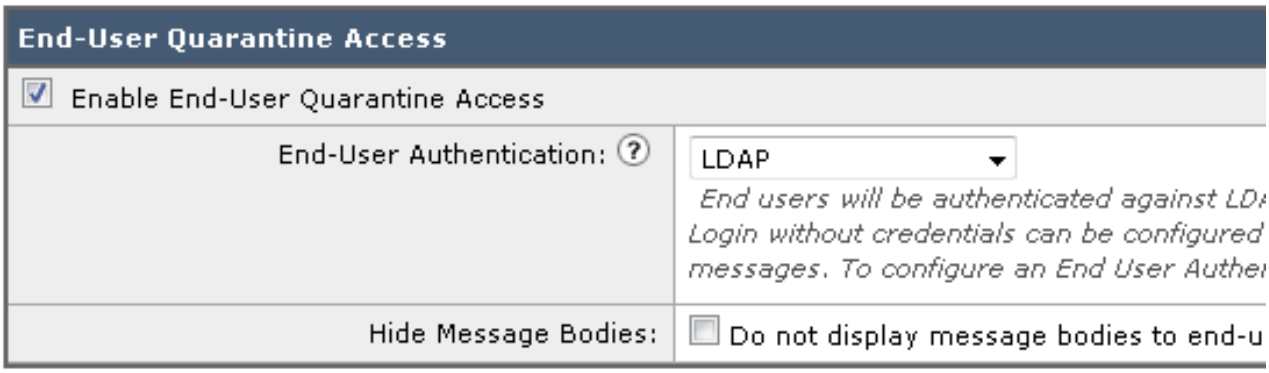
1. 在SMA或ESA，请选择**系统管理> LDAP**。
2. 打开您的LDAP服务器配置文件。
3. 为了验证您能验证与激活目录帐户，检查您的垃圾邮件检疫最终用户查询启用的验证。
4. 检查**指定作为活动查询**复选框。



5. 点击**测验**为了测试查询。 匹配正意味着验证是成功的
   ：



6. 提交并且确认更改。
7. 在ESA，请选择**监视器>垃圾邮件检疫**。 在SMA，请导航对垃圾邮件检疫设置为了执行同样步骤。
8. 点击**垃圾邮件检疫**。
9. 检查**Enable (event)最终用户检疫访问检查**复选框。
10. 从最终用户验证下拉列表选择**LDAP**。



11. 提交并且确认更改。
12. 验证外部验证在ESA/SMA。
13. 导航对在Web浏览器以前配置的您的URL为了验证您能访问检疫：
    https://quarantine.mydomain.com:83
    https://10.10.10.10:83
14. 有您的LDAP帐户的洛金。如果这发生故障，请检查外部验证LDAP配置文件并且启用最终用户检疫访问(请参阅上一个步骤)。

配置对垃圾邮件检疫的管理用户访问

使用步骤在此部分为了允许管理用户以这些角色管理在垃圾邮件检疫的消息：操作员、只读操作员、支持中心或者Guestroles和包括对垃圾邮件检疫的访问的自定义用户角色。

管理员级别用户，使用此步骤，包括默认管理员用户并且给管理员用户发电子邮件，能总是访问垃圾邮件检疫，并且不需要关联与垃圾邮件检疫功能。

> **Note**:非管理员级别用户能访问在垃圾邮件检疫的消息，但是他们不能编辑检疫设置。管理员级别用户能访问消息和编辑设置。

为了启用没有全双工管理员权限管理在垃圾邮件的消息的管理用户请检疫，完成这些步骤：

1. 确保您创建用户和分配他们与访问的一个用户角色对垃圾邮件检疫。
2. 在安全管理设备上，请选择**管理设备>集中式服务>垃圾邮件检疫**。
3. 点击**Enable (event)或编辑**在垃圾邮件检疫设置部分的**设置**。
4. 在垃圾邮件检疫设置部分的管理用户区域中，请点击本地用户、外部已认证的用户或者自定义用户角色的选择链路。
5. 选择您要准许访问查看，并且管理在垃圾邮件的消息请检疫的用户。
6. 单击 **Ok**。
7. 为在部分列出的管理用户的其他类型中的每一种若需要重复(本地用户，外部已认证的用户或者自定义用户角色)。
8. 提交并且确认您的更改。