Всестороннее карантинное руководство по установке спама на Email Security Appliance (ESA) и устройстве управления безопасностью (SMA)

Содержание

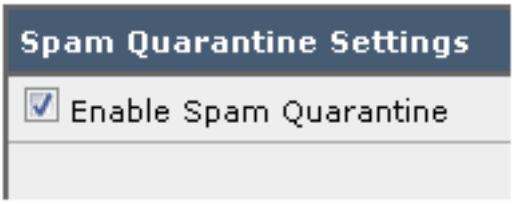
Введение

Этот документ описывает, как настроить карантин спама на ESA или SMA и привязанных функциях: внешняя проверка подлинности с LDAP и спамом изолирует уведомление.

Процедура

Настройте локальный карантин спама на ESA

1. На ESA выберите **Monitor> Spam Quarantine**.
2. В Карантинном разделе Параметров настройки Спама проверьте флажок **Enable Spam Quarantine** и установите желаемые карантинные параметры настройки.

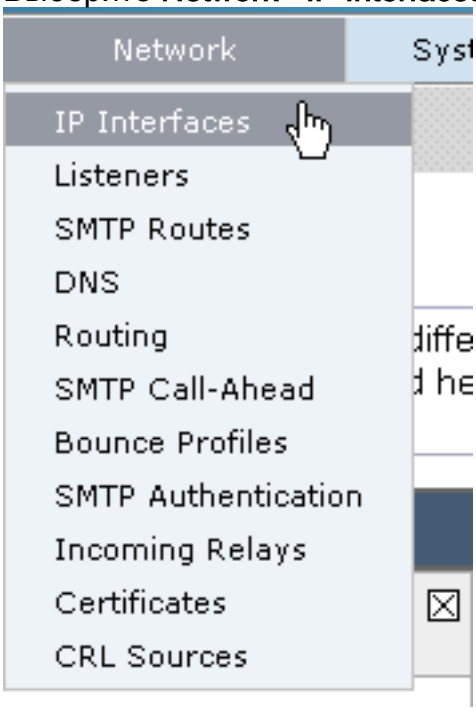


3. Выберите **Security Services> Spam Quarantine**.
4. Гарантируйте , что флажок **Enable External Spam Quarantine** неконтролируем, пока вы не планируете использовать Внешний Карантин Спама (см. раздел ниже).

5. Отправьте и передайте изменения.

Включите карантинные порты и задайте карантинный URL в интерфейсе

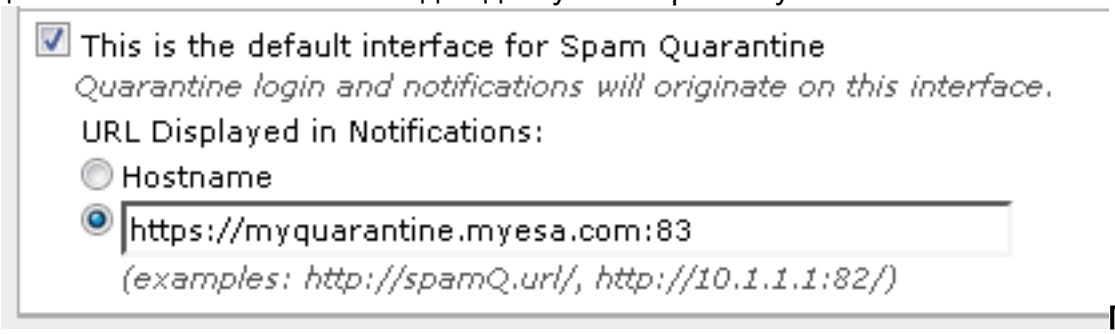
1. Выберите **Network> IP Interfaces**.



2. Нажмите имя интерфейса интерфейса, который вы будете использовать для доступа к карантину. В карантинном разделе спама проверьте флажки и задайте порты по умолчанию или изменение как требуется:Карантинный HTTP спамаКарантинный HTTPS
спама

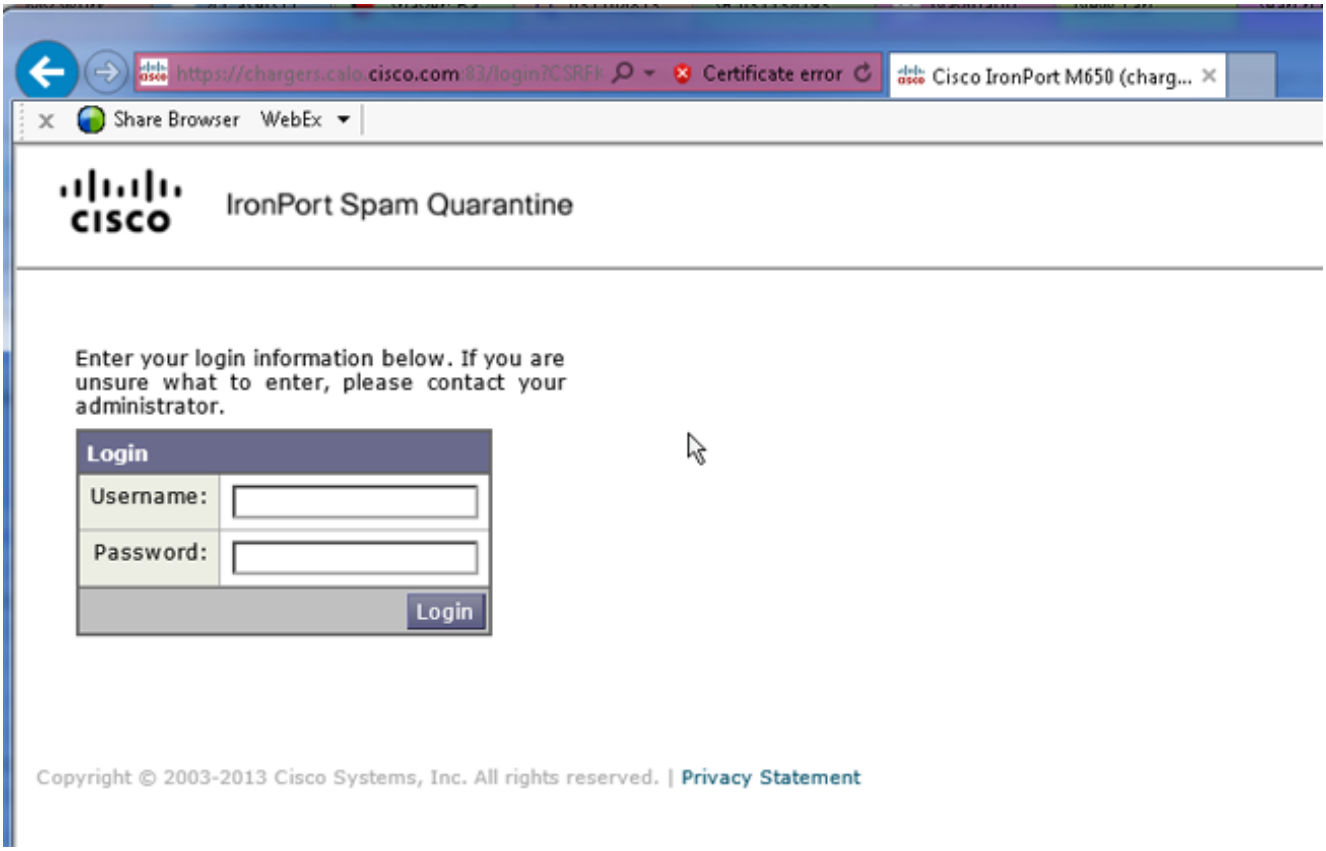
3. Проверьте**, что Это является интерфейсом по умолчанию для** флажка **Spam Quarantine**.
4. Под "URL, Отображенным в Уведомлениях", по умолчанию устройство использует системное имя хоста (cli: **sethostname)**, пока иначе не задано во втором параметре переключателей и текстовом поле. Данный пример задает значение имени хоста по

умолчанию. 

Можно задать пользовательский URL для доступа к Карантину Спама. 

Примечание: При настройке карантина на внешний доступ вам будет нужен внешний IP - адрес, настроенный на интерфейсе или внешнем IP, который является Сетевым адресом, Преобразованным во внутреннего IP.Если вы не используете имя хоста, можно поддержать кнопку с зависимой фиксацией Hostname проверенной, но все еще обратиться к карантину IP-адресом только. Например, https://10.10.10.10:83.

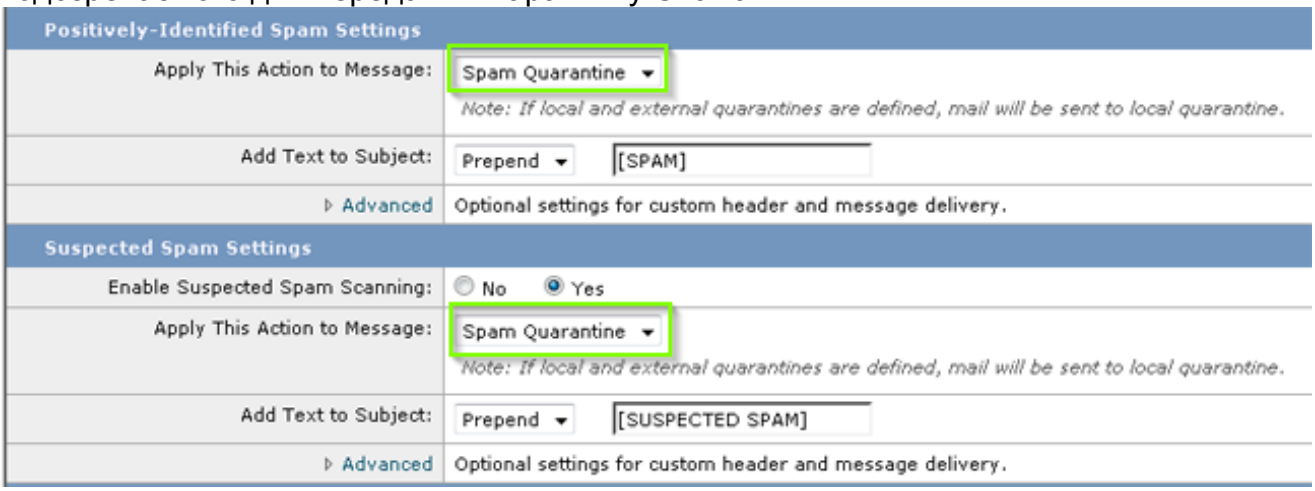
5. Отправьте и передайте изменения.
6. Проверить. Если вы задаете имя хоста для карантина спама, гарантируете, что имя хоста разрешимо через внутреннюю Систему доменных имен (DNS) или внешний DNS. DNS решит имя хоста к вашему IP-адресу.Если вы не получаете результат, сверяетесь с вашим Администратором сети и продолжаете обращаться к Карантину IP-адресом как предыдущий пример , пока хост не обнаруживается в DNS.>nslookup quarantine.mydomain.comПерейдите к своему URL, настроенному ранее в web-браузере, чтобы проверить, что можно обратиться к карантину: https://карантин mydomain.com:83https://10.10.10.10:83



Настройте ESA для Перемещения Положительного Спама Спама и/или Подозреваемого для Спама Карантина

Для изоляции Подозрительного Спама и/или Положительно Определенных сообщений Спама, выполните эти шаги:

1. На ESA нажмите **Mail Policies> Incoming Mail Policies** и затем столбец для защиты от спама для Политики по умолчанию.
2. Измените действие или Положительно Определенного Спама Спама или Подозреваемого для передачи к Карантину Спама."



3. Повторите процесс для любых других ESA, которые вы, возможно, настроили для Внешнего Карантина Спама. При внесении этого изменения на кластерном уровне, вы не должны будете повторять его, поскольку изменение будет propogated к другим устройствам в кластере.
4. Отправьте и передайте изменения.
5. На этом этапе почта, которая была бы иначе отправлена или отброшена, будет

изолирована.

Настройте внешний карантин спама на SMA

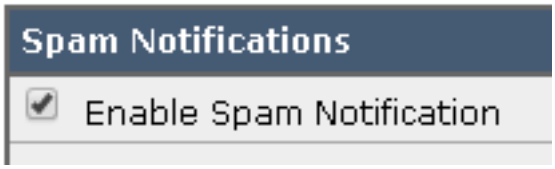
Шаги для настройки Внешнего Карантина Спама на SMA совпадают с предыдущим разделом за немногим исключением:

1. На каждом из ваших ESA необходимо будет отключить локальный карантин. Выберите **Monitor> Quarantines**.
2. На вашем ESA выберите **Security Services> Spam Quarantine** и нажмите **Enable External Spam Quarantine**.
3. Укажите ESA к IP-адресу вашего SMA и задайте порт, который требуется использовать. По умолчанию является портом 6025.

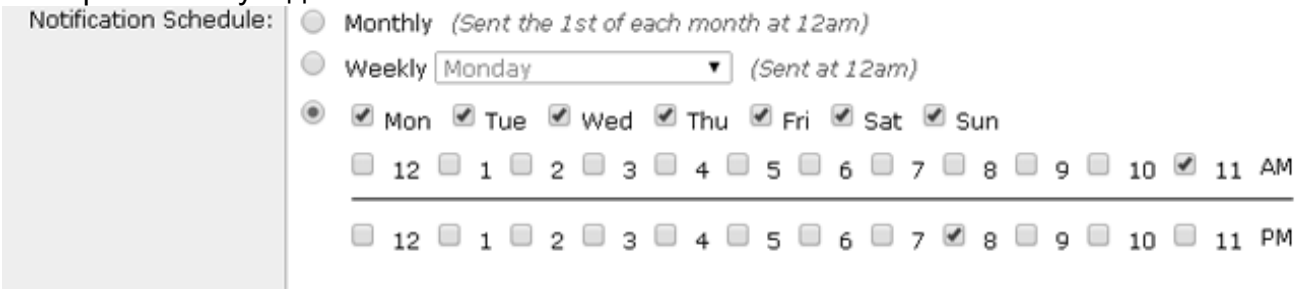
4. Гарантируйте, что порт 6025 открыт от ESA до SMA. *Этот порт для предоставления изолированных сообщений от ESA> SMA. Это может быть проверено с тестом telnet от CLI на ESA на порту 6025. Если соединение открывается и остается открытым, вы должны быть установлены.*
```
tarheel.rtp> telnet 14.2.30.116 6025
Trying 14.2.30.116...
Connected to steelers.rtp.
Escape character is '^]'.
220 steelers.rtp ESMTP
```
5. Гарантируйте настройку IP/имени хоста для доступа к карантину спама, такой, поскольку во "Включают Карантинные порты и Задают Карантинный URL в Интерфейсе".
6. Проверьте, что сообщения поступают в карантин спама от ваших ESA. Если карантин спама не показывает сообщений, могла бы быть проблема с подключением от ESA> SMA на порту 6025 (см. предыдущие шаги).

Настройте карантинное уведомление спама

1. На ESA выберите **Monitor> Spam Quarantine**.
2. На SMA вы перешли бы к Карантинным параметрам настройки Спама для выполнения тех же шагов.
3. Нажмите **Spam Quarantine**.
4. Проверьте флажок **Enable Spam Notification**.



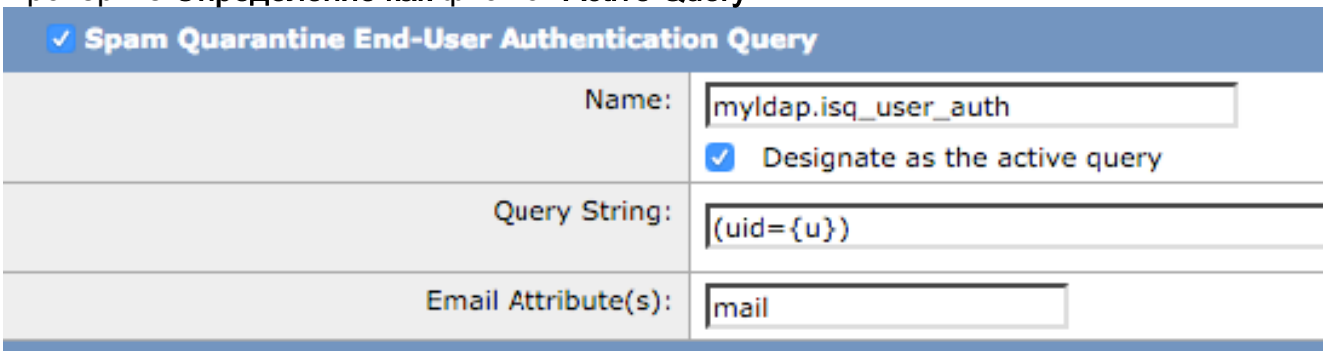
5. Выберите свое уведомление Список.



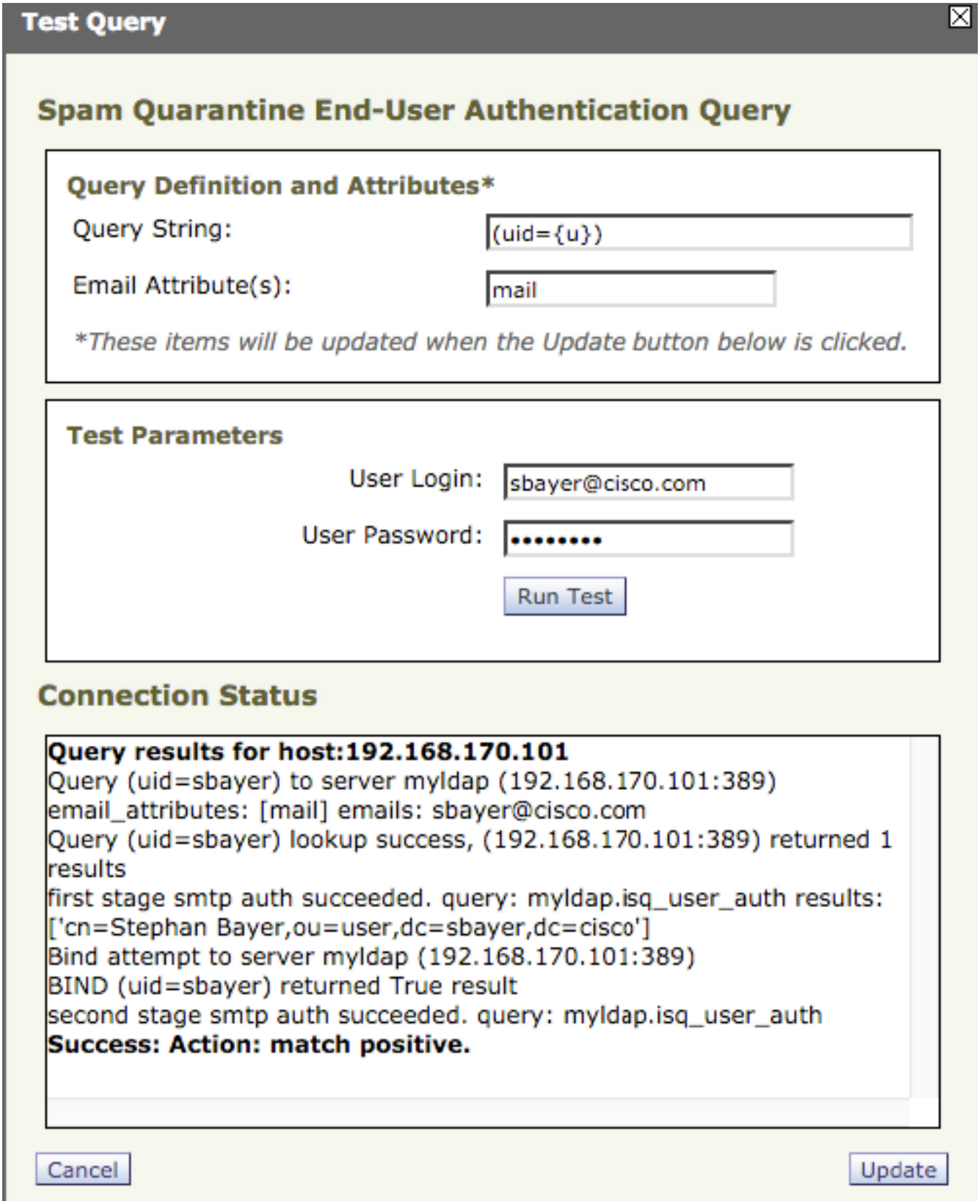
6. Отправьте и передайте изменения.

Настройте Карантинный Доступ Спама Конечного пользователя через Карантинный Запрос Аутентификации Конечного пользователя Спама

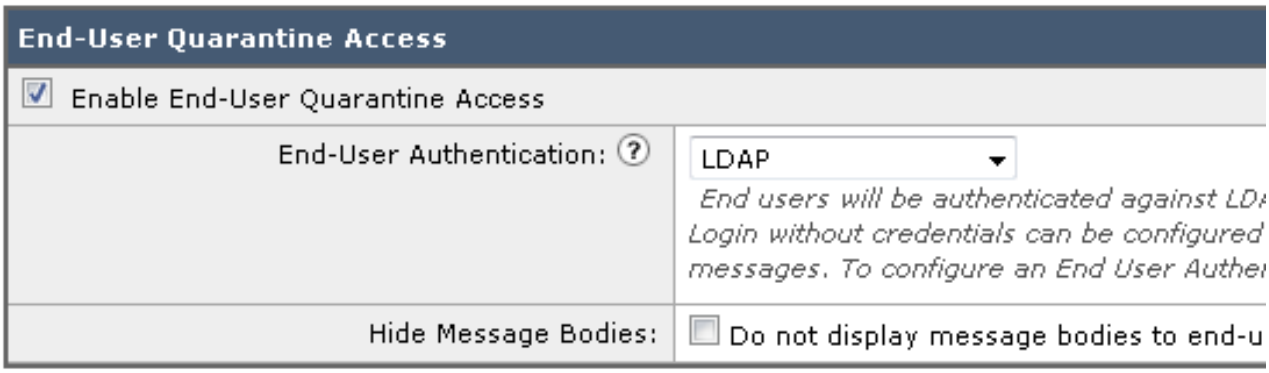
1. На SMA или ESA, выберите **System Administration> LDAP**.
2. Откройте свой Профиль Сервера LDAP.
3. Чтобы проверить, что вы в состоянии аутентифицироваться с Учетной записью Active Directory, проверить, что включен ваш Карантинный Запрос Аутентификации Конечного пользователя Спама.
4. Проверьте **Определение как** флажок **Active Query**.



5. Нажмите **Test** для тестирования запроса. Совпадите Положительный, означает, что аутентификация была
успешна:



6. Отправьте и передайте изменения.
7. На ESA выберите **Monitor> Spam Quarantine**. На SMA перейдите к Карантинным параметрам настройки Спама для выполнения тех же шагов.
8. Нажмите **Spam Quarantine**.
9. Установите **Разрешать Карантинный** флажок **Проверки доступа Конечного пользователя**.
10. Выберите **LDAP** из выпадающего списка Аутентификации Конечного пользователя.



11. Отправьте и передайте изменения.
12. Проверьте ту Внешнюю проверку подлинности, находится на ESA/SMA.
13. Перейдите к своему URL, настроенному ранее в web-браузере, чтобы проверить, что можно обратиться к карантину: https://карантин mydomain.com:83 https://10.10.10.10:83
14. Войдите со своей учетной записью LDAP. Если это отказывает, проверьте, что LDAP Внешней проверки подлинности представляет и включает Карантинный Доступ Конечного пользователя (см. предыдущие шаги).

Настройте доступ административного пользователя к карантину спама

Используйте процедуру в этом разделе, чтобы позволить административным пользователям с этими ролями управлять сообщениями в Карантине Спама: Оператор, Оператор Только для чтения, Справочный стол, или Guestroles и пользовательские роли пользователя, которые включают доступ к Карантину Спама.

Пользователи уровня администратора, среди которых пользователь с правами администратора по умолчанию и Почтовые Администраторы, могут всегда обращаться к Карантину Спама и не должными быть привязываться к Карантинной функции Спама с помощью этой процедуры.

> **Примечание:** Пользователи неуровня администратора могут обратиться к сообщениям в Карантине Спама, но они не могут отредактировать карантинные параметры настройки. Пользователи уровня администратора могут обратиться к сообщениям и отредактировать параметры настройки.

Чтобы включить административным пользователям, которые не имеют прав полного администратора для управления сообщениями в Карантине Спама, выполняют эти шаги:

1. Удостоверьтесь, что вы создали пользователей и назначили их роль пользователя с доступом к Карантину Спама.
2. На устройстве Управления системой безопасности выберите **Management Appliance> Centralized Services> Spam Quarantine**.
3. Нажмите **Enable или Edit Settings** в Карантинном разделе Параметров настройки Спама.
4. В области Administrative Users Карантинного раздела Параметров настройки Спама щелкните по ссылке выбора для Локальных пользователей, Внешне Проверенных пользователей или Пользовательских Ролей пользователя.

5. Выберите пользователей, которым вы хотите предоставить доступ, чтобы просмотреть и управлять сообщениями в Карантине Спама.
6. Нажмите кнопку ОК.
7. Повторитесь в случае необходимости для каждого из других типов Административных пользователей, перечисленных в разделе (Локальные пользователи, Внешне Проверенные пользователи или Пользовательские Роли пользователя).
8. Отправьте и передайте свои изменения.