دليل إعداد عزل البريد العشوائي الشامل على أجهزة أمان البريد الإلكتروني (ESA) وأجهزة إدارة الأمان (SMA)

المحتويات

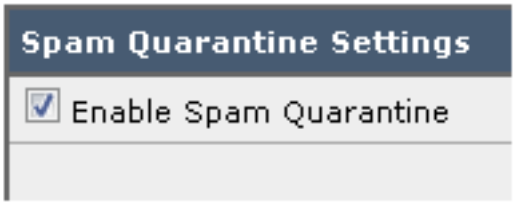
المقدمة

يوضح هذا المستند كيفية تكوين العزل العشوائي على ESA أو SMA والميزات المقترنة به: المصادقة الخارجية مع LDAP وإعلام عزل البريد العشوائي.

الإجراء

تكوين عزل البريد العشوائي المحلي على ESA

1. في ESA، أختر **مراقبة > عزل البريد العشوائي**.
2. في قسم "إعدادات عزل البريد العشوائي"، تحقق من خانة الاختيار **تمكين عزل البريد العشوائي** وقم بتعيين إعدادات العزل المطلوبة.

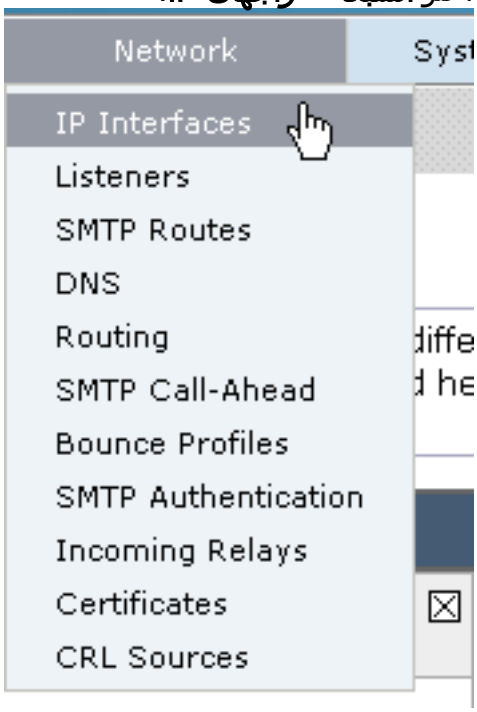


3. أختر **خدمات الأمان > عزل البريد العشوائي**.
4. تأكد من إلغاء تحديد خانة الاختيار **تمكين عزل البريد العشوائي الخارجي**، إلا إذا كنت تخطط لاستخدام عزل البريد العشوائي الخارجي (انظر القسم أدناه).

5. إرسال التغييرات وتنفيذها.

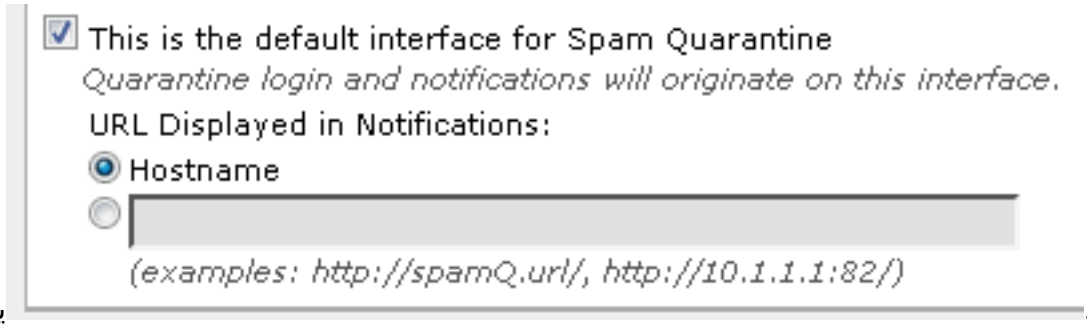
تمكين منافذ العزل وتحديد URL عزل في الواجهة

1. أختر **الشبكة > واجهات IP**.

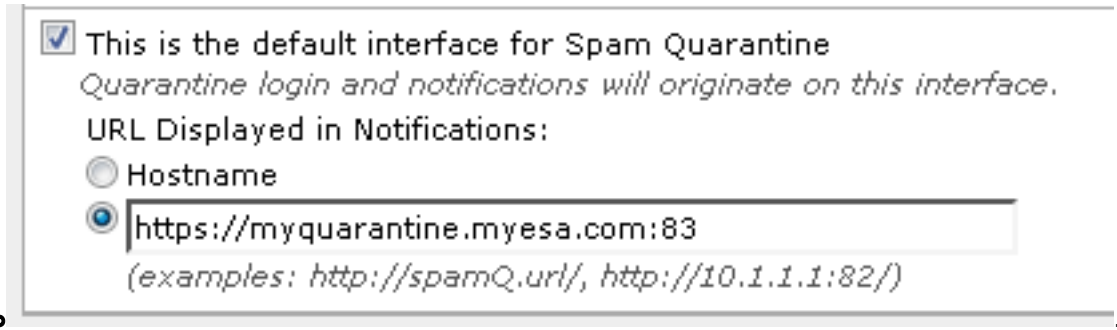


2. انقر على اسم الواجهة التي ستستخدمها للوصول إلى العزل. في قسم عزل البريد العشوائي، حدد خانات الاختيار وحدد المنافذ الافتراضية أو قم بالتغيير كما هو مطلوب:HTTP الخاص بالعزل العشوائيHTTPS الخاص بالعزل العشوائي

3. حدد **خانة الاختيار هذه هي الواجهة الافتراضية** لإختبار **عزل البريد العشوائي**.
4. تحت "عنوان URL المعروض في الإعلامات"، يستخدم الجهاز افتراضيا اسم مضيف النظام (cli:**sethostname**) ما لم يحدد خلاف ذلك في خيار زر الخيار الثاني وحقل النص. يحدد هذا المثال إعداد اسم المضيف

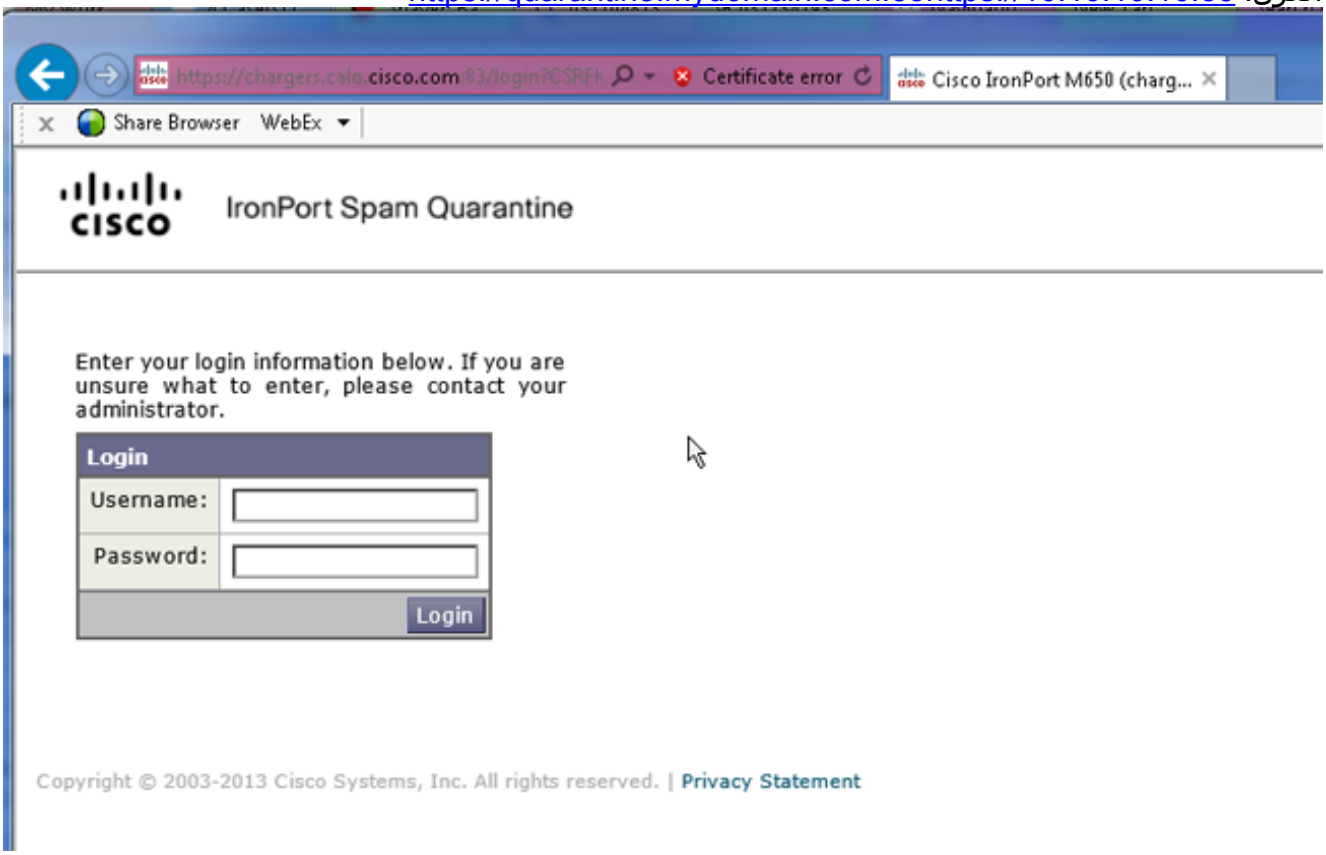


الافتراضي. يمكنك تحديد عنوان URL مخصص للوصول إلى عزل البريد



ملاحظة: إذا قمت بتكوين العزل للوصول الخارجي، فستحتاج إلى عنوان IP خارجي تم تكوينه على الواجهة أو عنوان IP خارجي يكون عنوان شبكة تمت ترجمته إلى عنوان IP داخلي.إذا لم تكن تستخدم اسم المضيف، فيمكنك إبقاء زر راديو Hostname مفحصا، لكن ما يزال بإمكانك الوصول إلى العزل بواسطة عنوان IP فقط. على سبيل المثال، https://10.10.10.10:83.

5. إرسال التغييرات وتنفيذها.
6. التحقق من الصحة. إذا قمت بتحديد اسم المضيف لإجراء عملية عزل البريد العشوائي، فتأكد من إمكانية حل اسم المضيف عبر نظام اسم المجال الداخلي (DNS) أو DNS الخارجي. سيقوم DNS بحل اسم المضيف إلى عنوان IP الخاص بك.إذا لم تحصل على نتيجة، تحقق من مسؤول الشبكة واستمر في الوصول إلى العزل بواسطة عنوان IP مثل المثال السابق حتى يظهر المضيف في DNS.>NSLOOKUP
quarantine.mydomain.comانتقل إلى عنوان URL الذي تم تكوينه مسبقا في مستعرض ويب للتحقق من إمكانية الوصول إلى العزل: https://10.10.10.10:83https://quarantine.mydomain.com:83

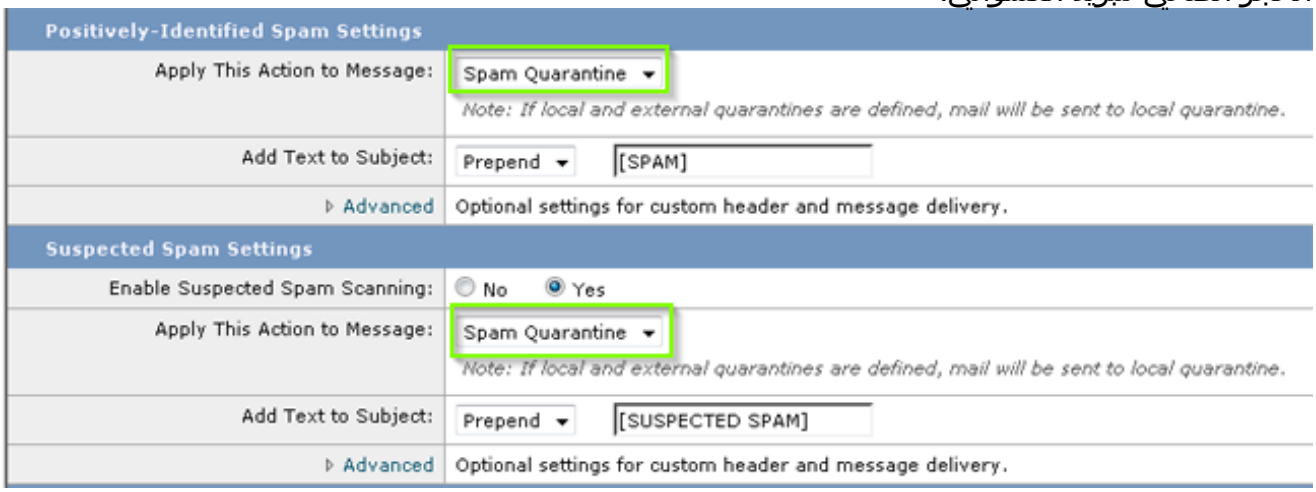


قم بتكوين ESA لنقل البريد العشوائي الإيجابي و/أو البريد العشوائي المشتبه فيه إلى عزل البريد العشوائي

من أجل عزل الرسائل غير المرغوب فيها و/أو الرسائل غير المرغوب فيها التي تم التعرف عليها بشكل إيجابي، أكمل الخطوات التالية:

1. في ESA، انقر فوق **نهج البريد > سياسات البريد الوارد** ثم فوق عمود مكافحة البريد العشوائي للنهج الافتراضي.

2. قم بتغيير إجراء البريد العشوائي أو البريد العشوائي المشبوه الذي تم التعرف عليه بشكل إيجابي لإرساله إلى الحجر الصحي للبريد العشوائي.

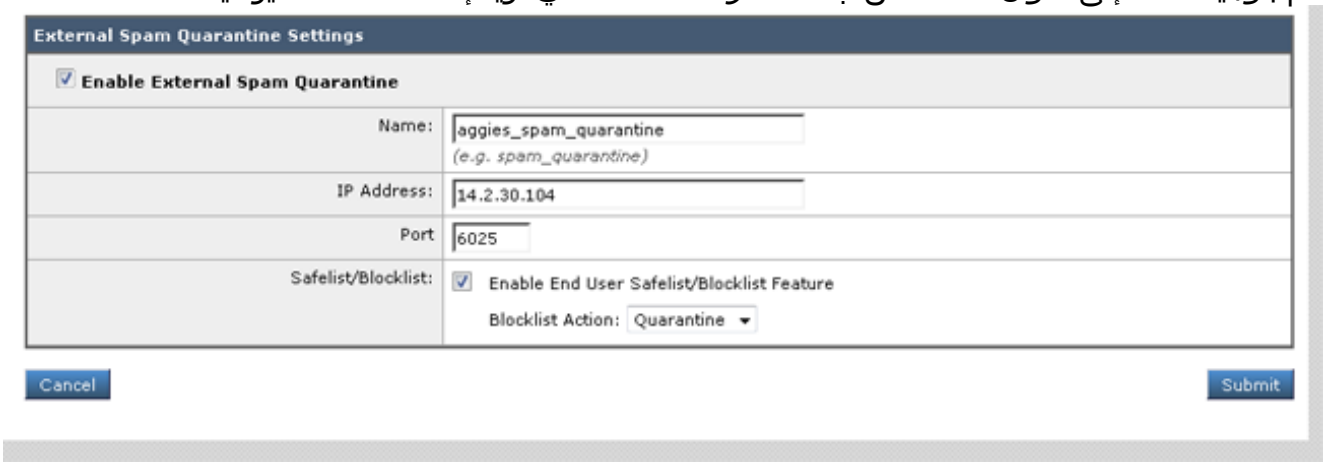


3. كرر العملية لأي ESAs أخرى قد تكون قمت بتكوينها لإجراء عزل البريد العشوائي الخارجي. إذا قمت بإجراء هذا التغيير على مستوى نظام المجموعة فلن تضطر إلى تكراره حيث سيتم تطبيق هذا التغيير على الأجهزة الأخرى في نظام المجموعة.
4. إرسال التغييرات وتنفيذها.
5. عند هذه النقطة، سيتم عزل البريد الذي كان سيتم تسليمه أو إسقاطه بطريقة أخرى.

تكوين عزل البريد العشوائي الخارجي على SMA

الخطوات الخاصة بتكوين عزل البريد العشوائي الخارجي على SMA هي نفس الخطوات الخاصة بالقسم السابق مع إستثناءات قليلة:

1. في كل من ESA الخاصة بك، ستحتاج إلى تعطيل العزل المحلي. أختر **الشاشة > المحاجر**.
2. في ESA الخاص بك، أختر **خدمات الأمان > عزل البريد العشوائي** وانقر فوق **تمكين عزل البريد العشوائي الخارجي**.
3. قم بتوجيه ESA إلى عنوان IP الخاص ب SMA وحدد المنفذ الذي تريد إستخدامه. التقصير ميناء 6025.



4. تأكد من فتح المنفذ 6025 من ESA إلى SMA. *الغرض من هذا المنفذ هو تسليم الرسائل المعزولة من ESA > SMA. يمكن التحقق من هذا الإجراء من خلال إختبار Telnet من واجهة سطر الأوامر على ESA على المنفذ 6025. إذا تم فتح اتصال وظل مفتوحا، فيجب تعيين هذا الاتصال.*

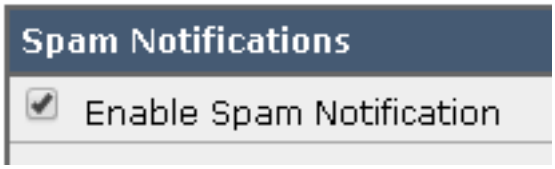
```
tarheel.rtp> telnet 14.2.30.116 6025
...Trying 14.2.30.116
.Connected to steelers.rtp
.'[^' Escape character is
steelers.rtp ESMTP 220
```

5. تأكد من تكوين IP/hostname للوصول إلى العزل العشوائي، مثل "تمكين منافذ العزل وتحديد URL عزل في الواجهة".

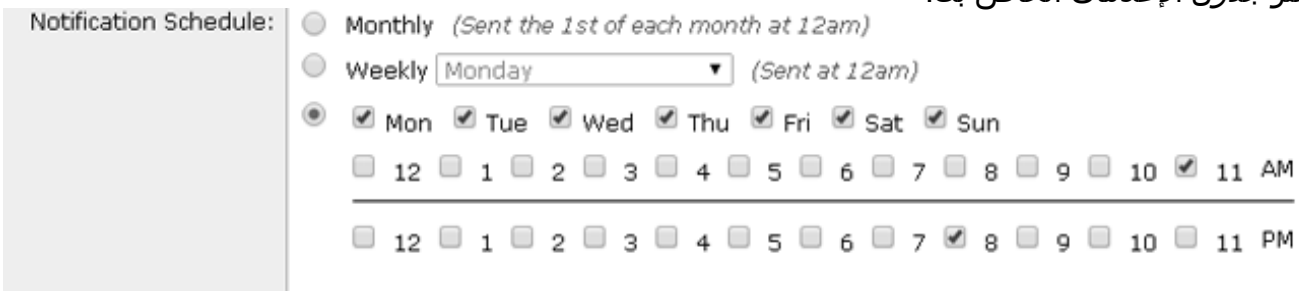
6. تحقق من وصول الرسائل إلى عملية عزل البريد العشوائي من ESA. إذا لم يظهر الفحص العشوائي أي رسائل، فقد يكون هناك مشكلة في الاتصال من SMA > ESA على المنفذ 6025 (راجع الخطوات السابقة).

تكوين إعلام عزل البريد العشوائي

1. في ESA، أختر **مراقبة > عزل البريد العشوائي**.
2. في SMA، يمكنك الانتقال إلى إعدادات "عزل البريد العشوائي" لتنفيذ الخطوات نفسها.
3. انقر فوق **عزل البريد العشوائي**.
4. حدد خانة الاختيار **تمكين إعلام البريد العشوائي**.



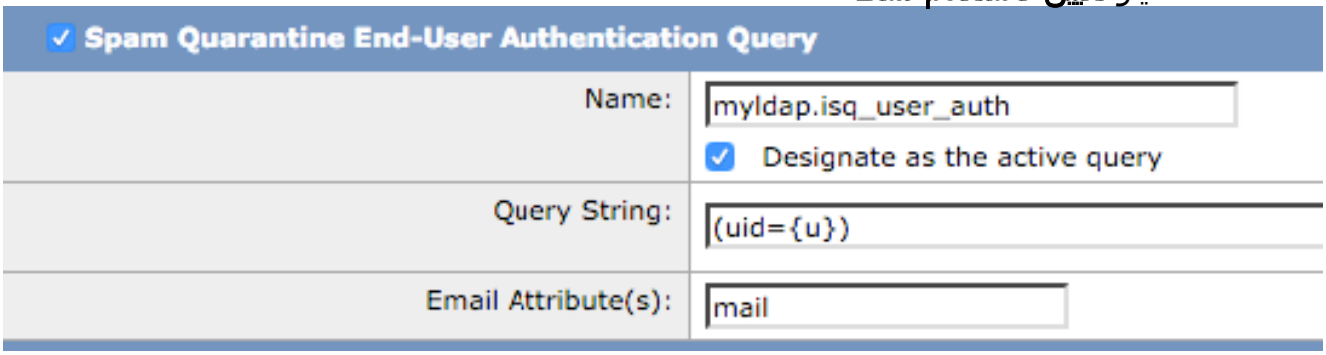
5. أختر جدول الإعلامات الخاص بك.



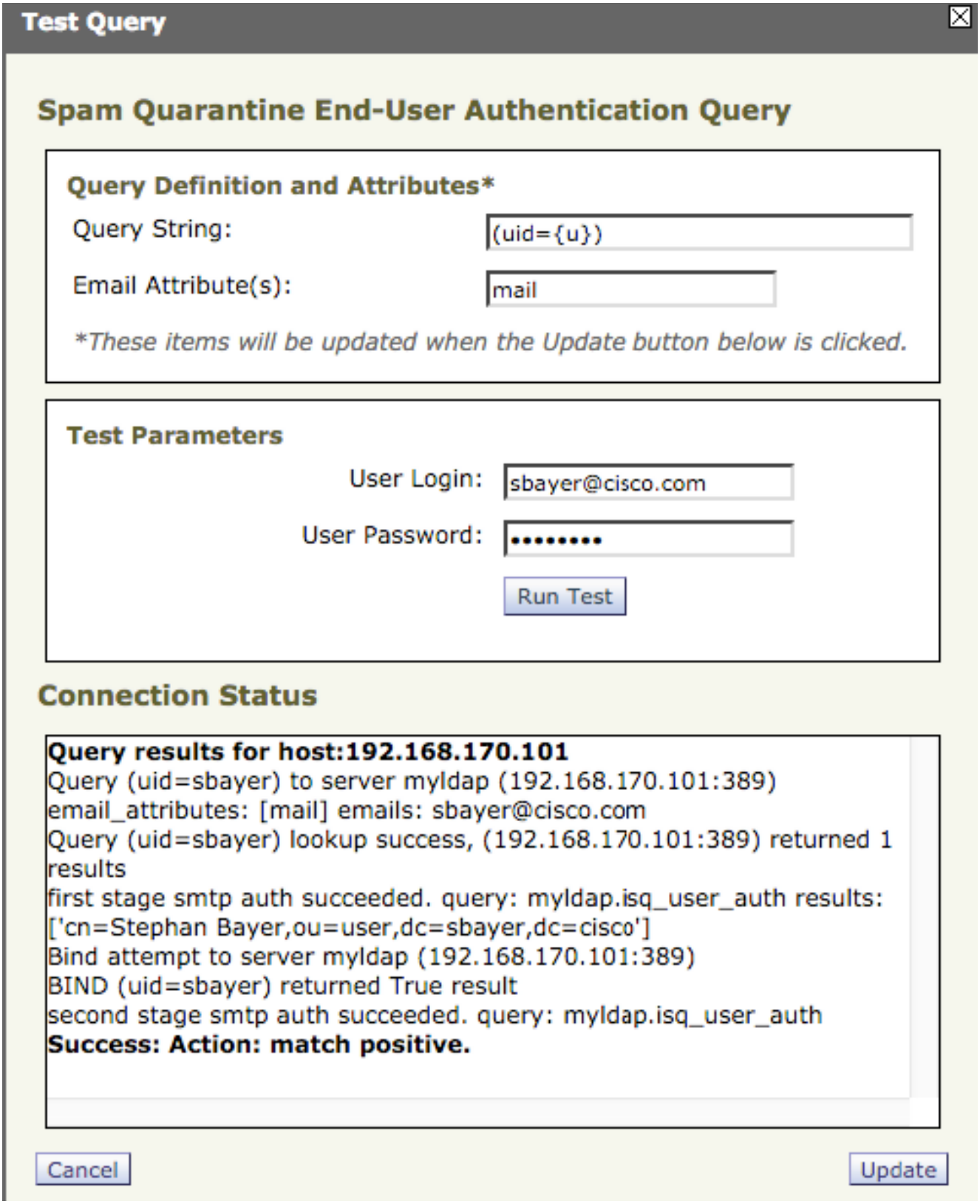
6. إرسال التغييرات وتنفيذها.

تكوين وصول المستخدم النهائي إلى العزل العشوائي لعزل البريد العشوائي من خلال استعلام مصادقة المستخدم النهائي لعزل البريد العشوائي

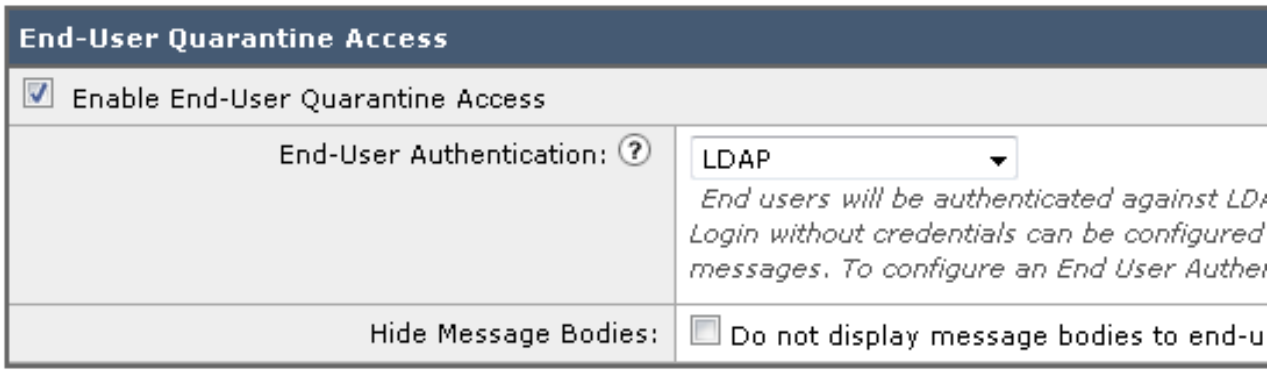
1. في SMA أو ESA، أختر **إدارة النظام > LDAP**.
2. افتح ملف تعريف خادم LDAP.
3. للتحقق من قدرتك على المصادقة باستخدام حساب Active Directory، تحقق من تمكين استعلام مصادقة المستخدم النهائي لعزل البريد العشوائي.
4. حدد خانة الاختيار **تعيين كاستعلام نشط**.



5. طقطقة **إختبار** in order to اختبرت الاستعلام. مطابقة الإيجابيات تعني نجاح المصادقة:



6. إرسال التغييرات وتنفيذها.
7. في ESA، أختر **مراقبة > عزل البريد العشوائي**. في SMA، انتقل إلى إعدادات عزل البريد العشوائي لتنفيذ الخطوات نفسها.
8. انقر فوق **عزل البريد العشوائي**.
9. حدد خانة الاختيار **تمكين وصول المستخدم النهائي إلى العزل**.
10. أختر **LDAP** من القائمة المنسدلة لمصادقة المستخدم النهائي.



11. إرسال التغييرات وتنفيذها.
12. تحقق من أن المصادقة الخارجية موجودة على ESA/SMA.
13. انتقل إلى عنوان URL الذي تم تكوينه مسبقا في مستعرض ويب للتحقق من إمكانية الوصول إلى العزل:
https://quarantine.mydomain.com:83
https://10.10.10.10:83
14. سجل الدخول باستخدام حساب LDAP الخاص بك. في حالة فشل هذا، تحقق من ملف تعريف LDAP للمصادقة الخارجية وقم بتمكين وصول المستخدم النهائي إلى العزل (راجع الخطوات السابقة).

تكوين وصول المستخدم الإداري إلى عزل البريد العشوائي

أستخدم الإجراء الوارد في هذا القسم للسماح للمستخدمين الإداريين الذين لديهم هذه الأدوار بإدارة الرسائل الموجودة في "عزل البريد العشوائي": عامل التشغيل أو عامل التشغيل للقراءة فقط أو مكتب المساعدة أو أدوار الضيوف وأدوار المستخدم المخصصة التي تتضمن الوصول إلى عزل البريد العشوائي.

يمكن دائما للمستخدمين على مستوى المسؤول، الذين يشملون مستخدم المسؤول الافتراضي ومستخدمي مسؤول البريد الإلكتروني، الوصول إلى العزل غير الهام ولا يحتاجون إلى الاقتران بميزة "عزل البريد العشوائي" باستخدام هذا الإجراء.

ملاحظة: يمكن للمستخدمين من غير المسؤولين الوصول إلى الرسائل الموجودة في "عزل البريد العشوائي"، ولكن لا يمكنهم تحرير إعدادات العزل. يمكن للمستخدمين على مستوى المسؤول الوصول إلى الرسائل وتحرير الإعدادات.

لتمكين المستخدمين الإداريين الذين ليس لديهم امتيازات المسؤول الكاملة لإدارة الرسائل في العزل العشوائي، أكمل الخطوات التالية:

1. تأكد من إنشاء مستخدمين وتعيين دور مستخدم لهم مع الوصول إلى "عزل البريد العشوائي".
2. في جهاز إدارة الأمان، أختر **جهاز الإدارة > الخدمات المركزية > عزل البريد العشوائي**.
3. انقر فوق **تمكين الإعدادات أو تحريرها** في قسم إعدادات عزل البريد العشوائي.
4. في قسم "المستخدمون الإداريون" في قسم "إعدادات عزل البريد العشوائي"، انقر فوق إرتباط التحديد للمستخدمين المحليين أو المستخدمين المصادق عليهم خارجيا أو أدوار المستخدمين المخصصة.
5. أختر المستخدمين الذين تريد منح حق الوصول إليهم لعرض الرسائل وإدارتها في "عزل البريد العشوائي".
6. وانقر فوق **OK**.
7. كرر إذا لزم الأمر لكل نوع من الأنواع الأخرى للمستخدمين الإداريين المدرجين في القسم (المستخدمون المحليون أو المستخدمون المصادق عليهم خارجيا أو أدوار المستخدم المخصصة).
8. إرسال التغييرات وتنفيذها.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).