

ىلع لماشلا يئوشعلا ديربلا لزع دادعإ ليلد قراذإ ةزهجأو (ESA) ينورتكلإلا ديربلا نامأ ةزهجأ (SMA) نامألا

المحتويات

[المقدمة](#)

[الإجراء](#)

[تكوين عزل البريد العشوائي المحلي على ESA](#)

[تمكين منافذ العزل وتحديد URL عزل في الواجهة](#)

[قم بتكوين ESA لنقل البريد العشوائي الإيجابي و/أو البريد العشوائي المشتبه فيه إلى عزل البريد العشوائي](#)

[تكوين عزل البريد العشوائي الخارجي على SMA](#)

[تكوين إعلام عزل البريد العشوائي](#)

[تكوين وصول المستخدم النهائي إلى العزل العشوائي لعزل البريد العشوائي من خلال استعلام مصادقة المستخدم](#)

[النهائي لعزل البريد العشوائي](#)

[تكوين وصول المستخدم الإداري إلى عزل البريد العشوائي](#)

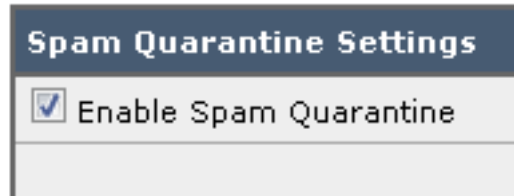
المقدمة

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

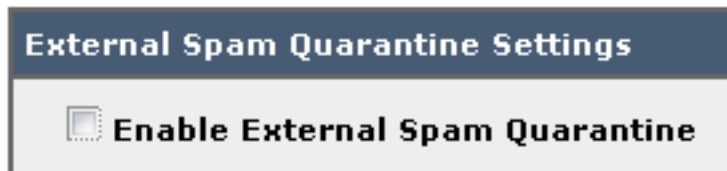
الإجراء

تكوين عزل البريد العشوائي المحلي على ESA

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



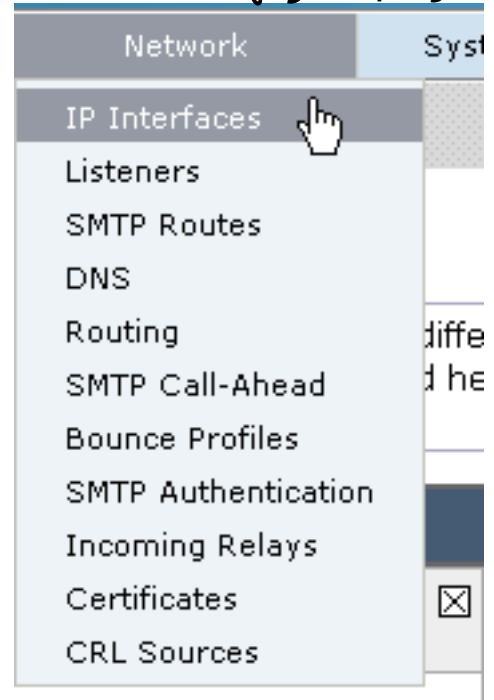
3. أختَر خدمات الأمان < عزل البريد العشوائي.
4. تأكد من إلغاء تحديد خانة الاختيار تمكين عزل البريد العشوائي الخارجي، إلا إذا كنت تخطط لاستخدام عزل البريد العشوائي الخارجي (انظر القسم أدناه).



5. إرسال التغييرات وتنفيذها.

تمكين منافذ العزل وتحديد URL عزل في الواجهة

1. أختار الشبكة < واجهات IP.



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

Spam Quarantine	
<input checked="" type="checkbox"/> Spam Quarantine HTTP	82
<input checked="" type="checkbox"/> Spam Quarantine HTTPS	83

3. حدد خانة الاختيار هذه هي الواجهة الافتراضية لإختبار عزل البريد العشوائي.

4. تحت "عنوان URL المعروف في الإعلانات"، 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

This is the default interface for Spam Quarantine
Quarantine login and notifications will originate on this interface.

URL Displayed in Notifications:

Hostname

(examples: <http://spamQ.url/>, <http://10.1.1.1:82/>)

يمكنك

الافتراضي. تحديد عنوان URL مخصص للوصول إلى عزل البريد

This is the default interface for Spam Quarantine
 Quarantine login and notifications will originate on this interface.
 URL Displayed in Notifications:
 Hostname

 (examples: http://spamQ.url/, http://10.1.1.1:82/)

ملاحظ

العشوائي. 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.com انتقل إلى عنوان URL الذي تم تكوينه مسبقا في مستعرض ويب للتحقق من إمكانية الوصول إلى

العزل: <https://quarantine.mydomain.com:83https://10.10.10.10:83>

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.

Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine <small>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</small>
Add Text to Subject:	Prepend [SPAM]
Advanced	Optional settings for custom header and message delivery.
Suspected Spam Settings	
Enable Suspected Spam Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Spam Quarantine <small>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</small>
Add Text to Subject:	Prepend [SUSPECTED SPAM]
Advanced	Optional settings for custom header and message delivery.

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. أختار الشاشة < المحاجر.
2. في ESA الخاص بك، أختار 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.

External Spam Quarantine Settings	
<input checked="" type="checkbox"/> Enable External Spam Quarantine	
Name:	aggies_spam_quarantine <small>(e.g. spam_quarantine)</small>
IP Address:	14.2.30.104
Port:	6025
Safelist/Blocklist:	<input checked="" type="checkbox"/> Enable End User Safelist/Blocklist Feature Blocklist Action: Quarantine
<input type="button" value="Cancel"/> <input type="button" value="Submit"/>	

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 ESMTD 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، أختَر 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.

Spam Notifications

 Enable Spam Notification

5. أختَر جدول الإعلّامات الخاص بك.

Notification Schedule:

Monthly (Sent the 1st of each month at 12am)

Weekly Monday (Sent at 12am)

Mon Tue Wed Thu Fri Sat Sun

12 1 2 3 4 5 6 7 8 9 10 11 AM

12 1 2 3 4 5 6 7 8 9 10 11 PM

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، أختَر 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.

Spam Quarantine End-User Authentication Query

Name:	<input type="text" value="myldap.isq_user_auth"/> <input checked="" type="checkbox"/> Designate as the active query
Query String:	<input type="text" value="{uid={u}}"/>
Email Attribute(s):	<input type="text" value="mail"/>

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

Spam Quarantine End-User Authentication Query

Query Definition and Attributes*

Query String:

Email Attribute(s):

**These items will be updated when the Update button below is clicked.*

Test Parameters

User Login:

User Password:

Connection Status

Query results for host:192.168.170.101

```
Query (uid=sbayer) to server myldap (192.168.170.101:389)
email_attributes: [mail] emails: sbayer@cisco.com
Query (uid=sbayer) lookup success, (192.168.170.101:389) returned 1
results
first stage smtp auth succeeded. query: myldap.isq_user_auth results:
['cn=Stephan Bayer,ou=user,dc=sbayer,dc=cisco']
Bind attempt to server myldap (192.168.170.101:389)
BIND (uid=sbayer) returned True result
second stage smtp auth succeeded. query: myldap.isq_user_auth
Success: Action: match positive.
```

6. إرسال التغييرات وتنفيذها.
7. في ESA، اختر 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. اختر LDAP من القائمة المنسدلة لمصادقة المستخدم النهائي.

End-User Quarantine Access	
<input checked="" type="checkbox"/> Enable End-User Quarantine Access	
End-User Authentication: ?	LDAP <i>End users will be authenticated against LDAP. Login without credentials can be configured messages. To configure an End User Authen</i>
Hide Message Bodies:	<input type="checkbox"/> Do not display message bodies to end-u

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، أختَر 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. أختَر 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 المستخدمين المصادق عليهم خارجيا أو أدوار المستخدم المخصصة).
8. إرسال التغييرات وتنفيذها.

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إلمءاد ءوچرلاب ةصوء و تاملرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنل اءل دن تسمل