كيفية معالجة رسائل البريد الإلكتروني من CTR

المحتويات

المقدمة

يوضح هذا المستند كيفية إصلاح رسائل البريد الإلكتروني من الاستجابة للتهديدات من Cisco (CTR).

معلومات أساسية

تم تحديث تحقيق CTR لدعم معالجة بريد OnDemand. يمكن للمسؤول البحث عن رسائل بريد إلكتروني معينة من علب بريد مستخدم O365 و OnPrem Exchange وإصلاحها من خلال جهاز أمان البريد الإلكتروني (ESA) أو جهاز إدارة الأمان (SMA).

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- حساب CTR
- تبادل خدمات الأمان من Cisco
- ESA ASYCNos 14.0.1-033

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

> **ملاحظة**: يتم دعم حل مشاكل البحث والبريد في عمليات النشر المختلطة لنظام O365 PreM 2013 على نظام التشغيل Exchange وعمليات النشر Exchange 2016 و 2019 فقط.

التكوين

1. تكوين إعدادات الحساب في ESA
2. تكوين ملف التعريف المتسلسل وتعيين المجال (المجالات) على ملف تعريف الحساب
3. دمج CTR مع ESA أو SMA

التحقق

يمكنك التحقيق في المخالفات في بوابة CTR وتحديد الرسالة للإصلاح باستخدام الخطوات التالية:

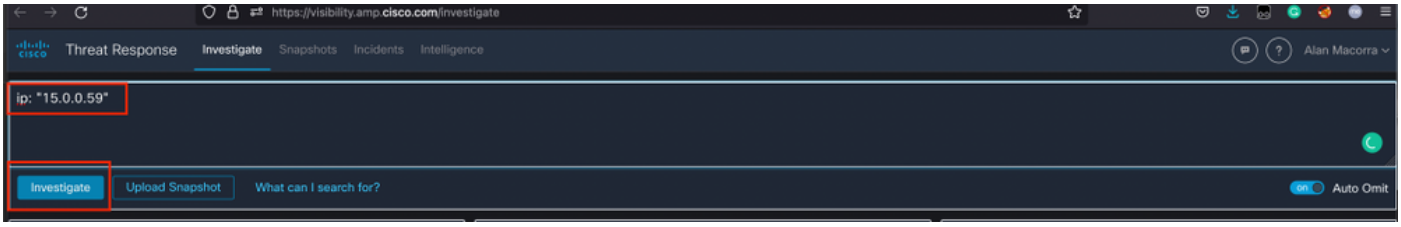
الخطوة 1. الوصول إلى بوابة CTR استنادا إلى الوصول إلى الخوادم المتوفرة والتحقيق

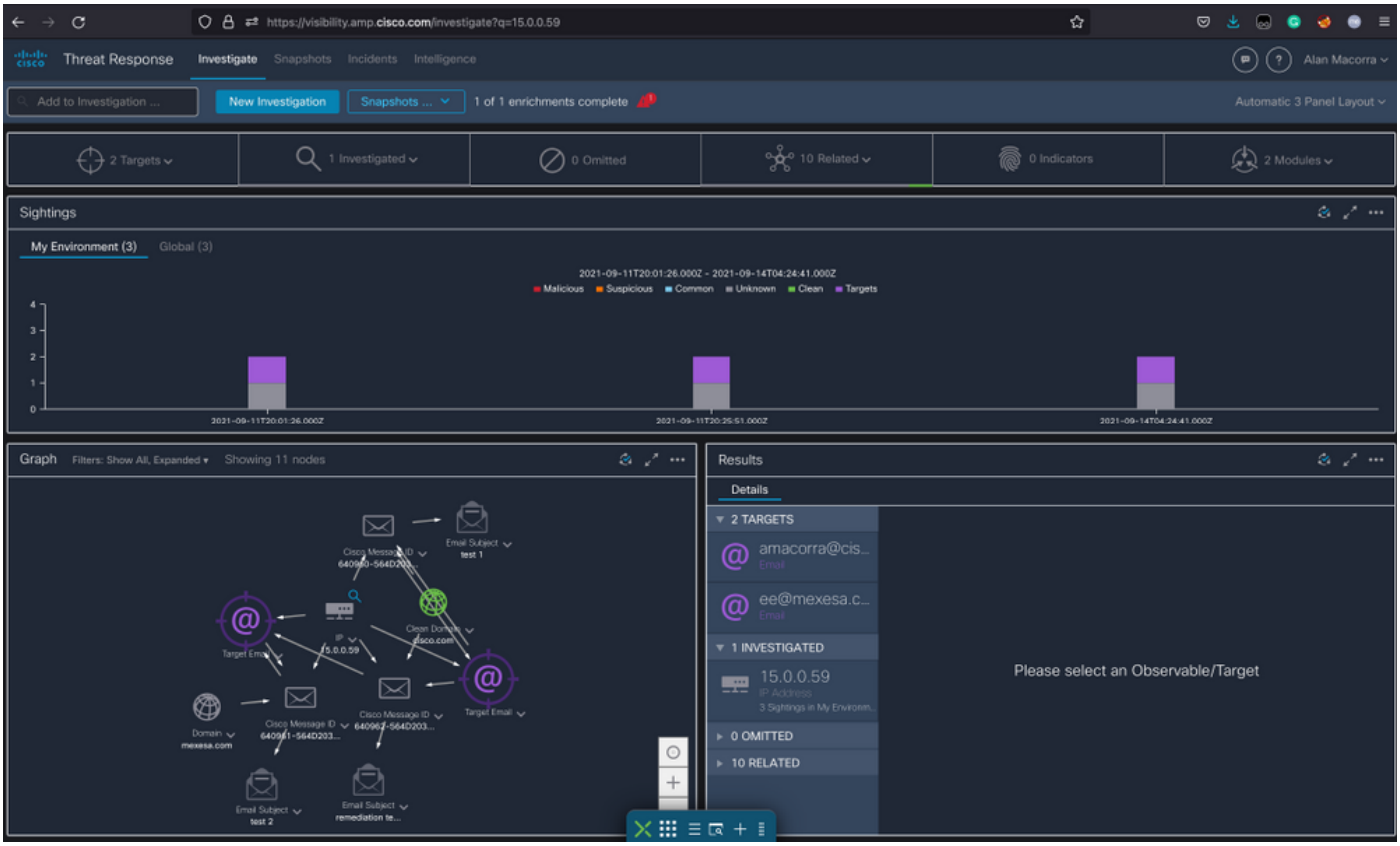
- الولايات المتحدة https://visibility.amp.cisco.com/investigate
- المركز الأفريقي للجوار https://visibility.apjc.amp.cisco.com/investigate
- الاتحاد الأوروبي https://visibility.eu.amp.cisco.com/investigate

الخطوة 2. تحقق من الرسائل التي تم تسليمها والتي يبدو أنها ضارة أو تشكل تهديدا باستخدام المخالفات المدعومة. يمكن البحث عن المخالفات بالمعايير التالية كما هو موضح في الصورة:

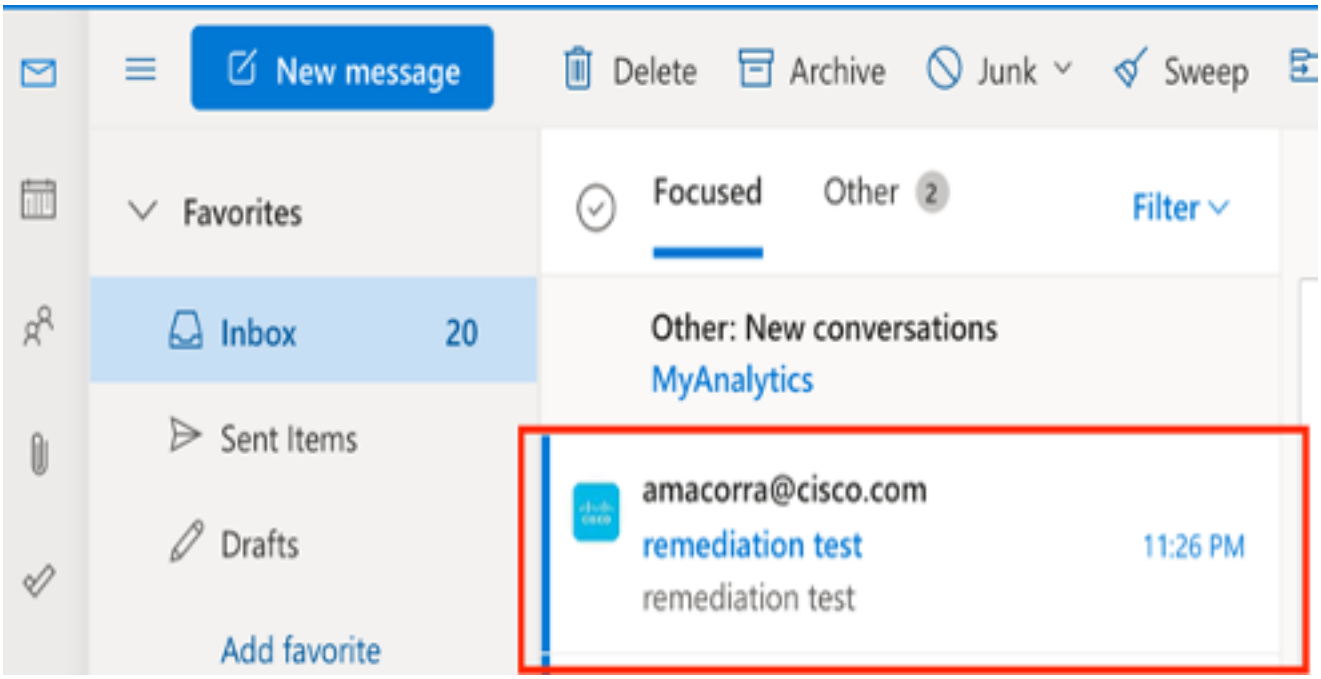
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file name	file_name:"invoice.pdf"

2-1 مثال على تحقيق الشرطة الدولية والتحقيق فيما يلي، كما هو مبين في الصور:

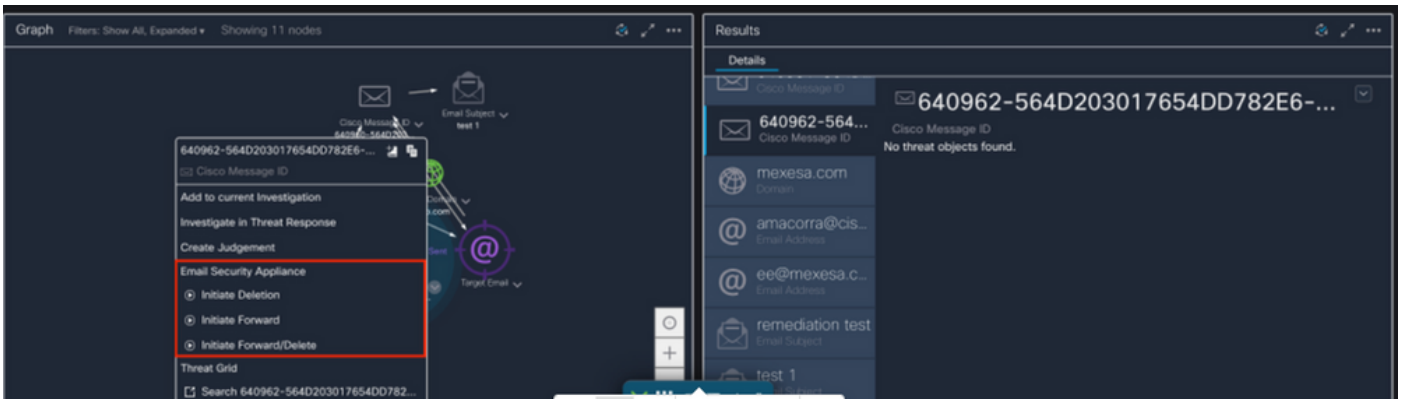




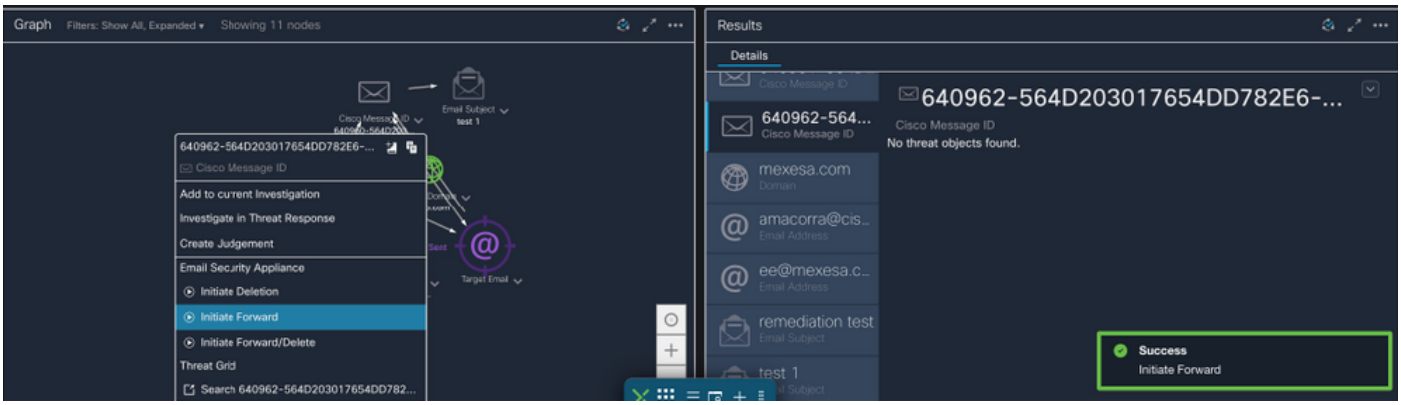
2.2 هذا ما تحصل عليه في علبة الوارد قبل إصلاح الرسالة، كما هو موضح في الصورة:



2.3 عند النقر فوق "معرف رسالة Cisco"، حدد من خيارات القائمة أي من "الإجراءات العلاجية المدعومة"، كما هو موضح في الصورة:



2.4 في هذا المثال، يتم تحديد "تقديم مبادرة" وتظهر نافذة منبثقة ناجحة في الركن السفلي الأيمن، كما هو موضح في الصورة:

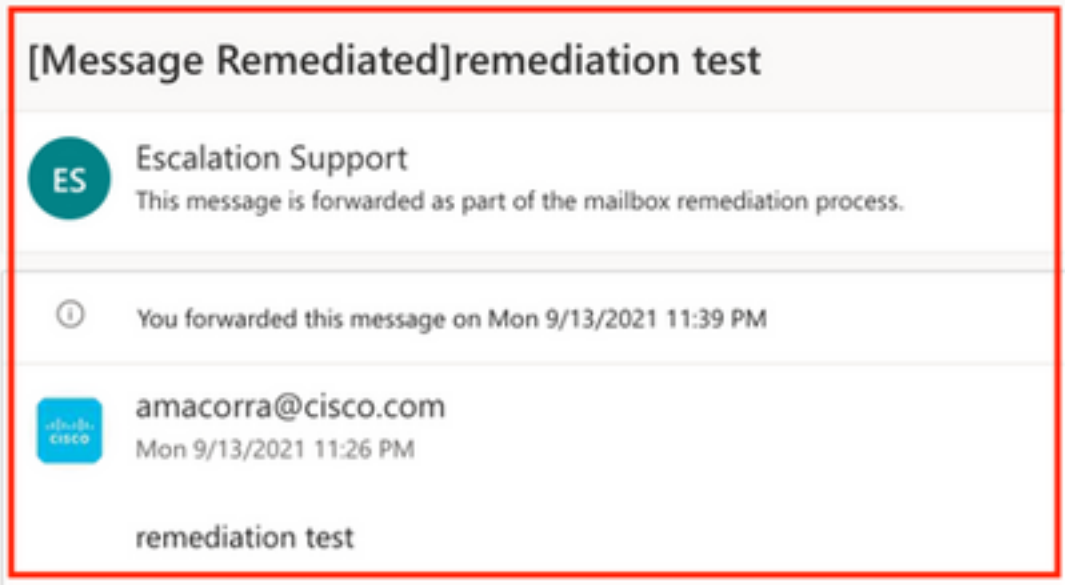


2.5 في ESA، يمكنك الاطلاع على السجلات التالية تحت "mail_log" التي تظهر أن إصلاح "CTR" يبدأ، والإجراء المحدد، والحالة النهائية.

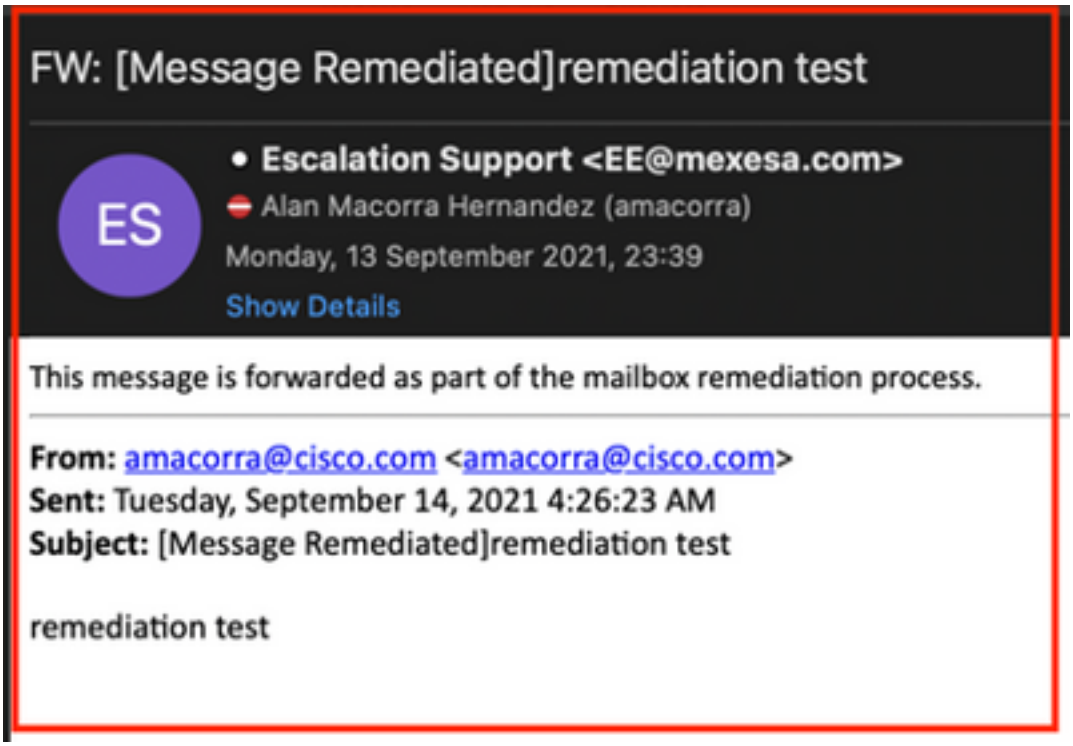
```
Mon Sep 13 23:38:03 2021 Info: Message 640962 was initiated for 'Forward' remedial action by
'admin' from source 'CTR' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'.

Mon Sep 13 23:38:06 2021 Info: Message 640962 was processed with 'Forward' remedial action for
recipient 'ee@mexesa.com' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'. Remediation status:
Remediated.
```

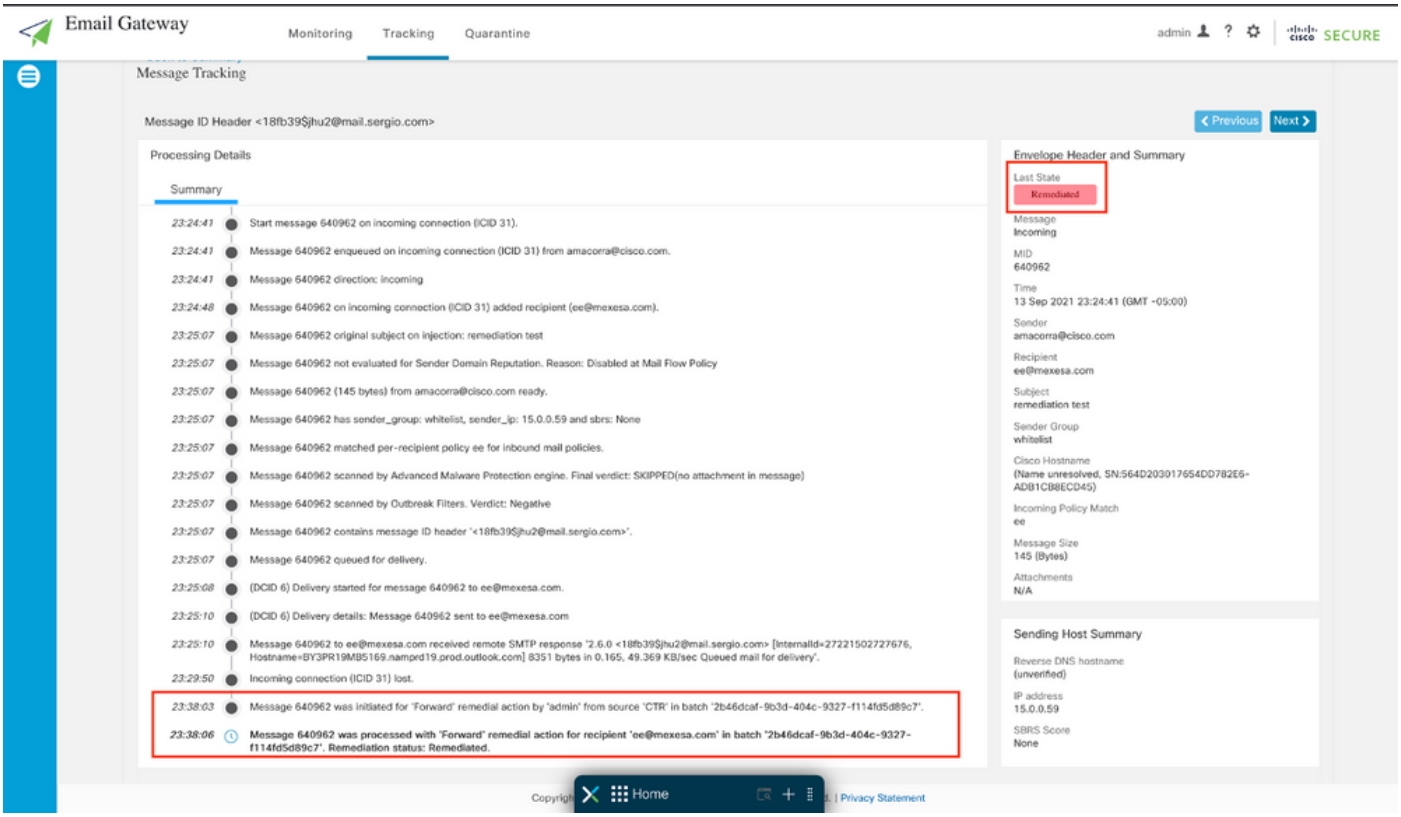
2-6 ترد العبارة "[الرسالة التي تم تصحيحها]" في موضوع الرسالة، كما هو مبين في الصورة:



2.7 عنوان البريد الإلكتروني الذي تكتبه عند تكوين وحدة ESA/SMA وه العنوان الذي يستقبل رسائل البريد الإلكتروني التي تم إصلاحها عند تحديد الخيار "إعادة توجيه" أو "إعادة توجيه/حذف"، كما وه موضح في الصورة:



2.8 أخيرا، إذا نظرت إلى تفاصيل تعقب الرسائل للواجهة الجديدة بين ESA/SMA، يمكنك أن ترى نفس السجلات التي تم الحصول عليها في "mail_log" و"Last State" على أنها "Remediated"، كما وه موضح في الصورة:



ملاحظة: يمكن إجراء عدة عمليات إصلاح، إذا قمت بتهيئة ميزة البحث والتعويض في ESA/SMA، يمكنك معالجة نفس الرسالة من CTR وكذلك من ESA/SMA. يمكن أن يتيح لك ذلك إعادة توجيه نفس الرسالة إلى عنوان بريد إلكتروني مختلف عن العنوان الذي تم تكوينه في وحدة التكامل النمطية.

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).