إستخدام IM لأتمتة رسائل البريد الإلكتروني الآمنة للمستخدم

المحتويات

المقدمة

يصف هذا المستند العملية اللازمة لاستخدام الإجراء "خادم البريد" في "مدير الحدث المضمن" (EEM) داخل Cisco IOS® XE لإرسال رسائل البريد الإلكتروني إلى خادم آمن (SMTP) باستخدام أمان طبقة النقل (TLS) على المنفذ بروتوكول نقل البريد البسيط 587.

هناك العديد من المحاذير التي يمكنك مواجهتها أثناء هذه العملية، ولهذا السبب تم كتابة هذه المقالة لتوثيق الخطوات اللازمة لتحقيق ذلك.

حالة الاستخدام

يرى العديد من العملاء قيمة في تلقي إعلام عبر البريد الإلكتروني تلقائيا بعد حدوث حدث معين. نظام IM الفرعي وهو أداة قوية لاكتشاف حدث الشبكة والأتمتة المدمجة، ويمكن أن يوفر طريقة فعالة لأتمتة إعلامات البريد الإلكتروني على جهاز Cisco IOS XE. على سبيل المثال، قد ترغب في مراقبة مسار IPSLA، واستجابة إلى syslog يشير إلى تغيير الحالة، قم باتخاذ نوع من الإجراءات وقم بتنبيه مسؤولي الشبكة للحدث عبر البريد الإلكتروني. يمكن تطبيق فكرة "الإعلام عبر البريد الإلكتروني" هذه على سيناريوهات أخرى عديدة كوسيلة لجذب الانتباه إلى أي حدث معين تريد تسليط الضوء عليه.

الخلفية

PEM تعني "بريد الخصوصية المحسن"، وهو تنسيق يستخدم غالبا لتمثيل الشهادات والمفاتيح. هذا هو تنسيق الشهادة الذي تستخدمه أجهزة Cisco IOS XE. غالبا ما تحتوي

التطبيقات الآمنة (مثل HTTPS وأ SMTP الآمن) على "PEM مكدس"، حيث تشتمل على شهادات متعددة، بما في ذلك:

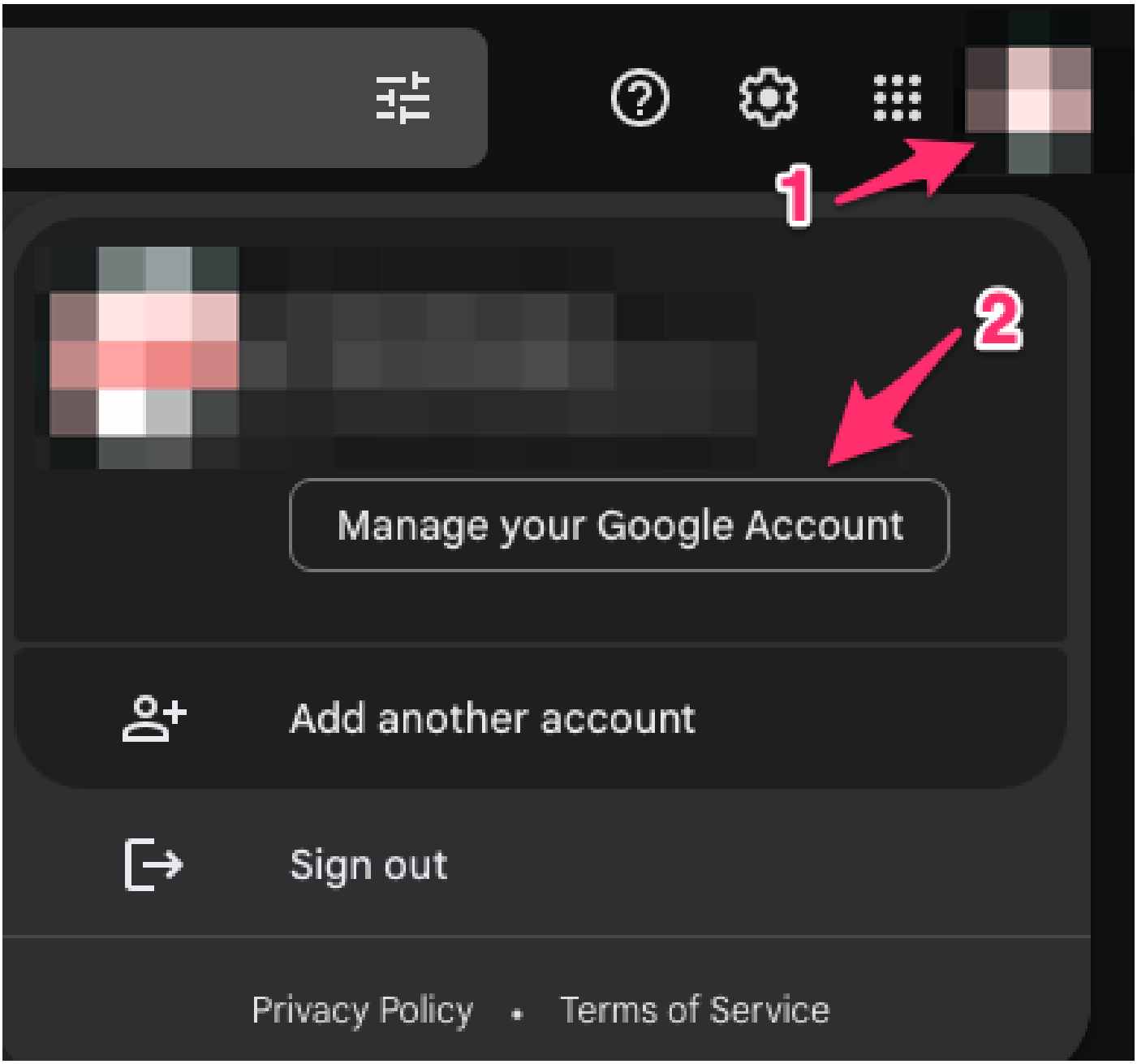
- الشهادة الجذر
- شهادة توقيع (وسيط)
- شهادة المستخدم النهائي (أو الخادم)

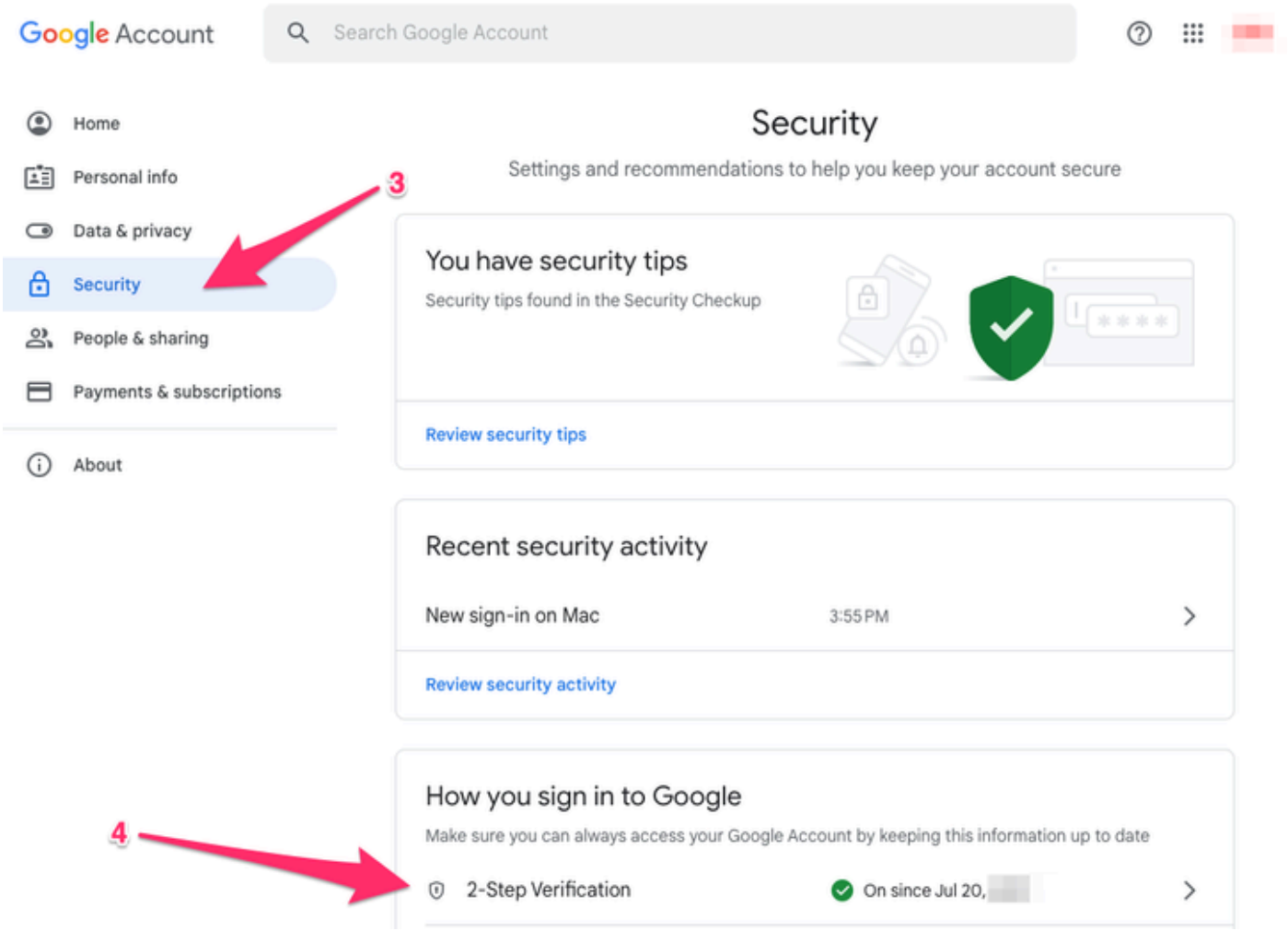
إعداد حساب Gmail

وستستخدم خدمات جوجل باك SMTP كمثال في هذه المقالة. المتطلبات الأساسية هي أن لديك حساب Gmail تم إعداده مسبقا.

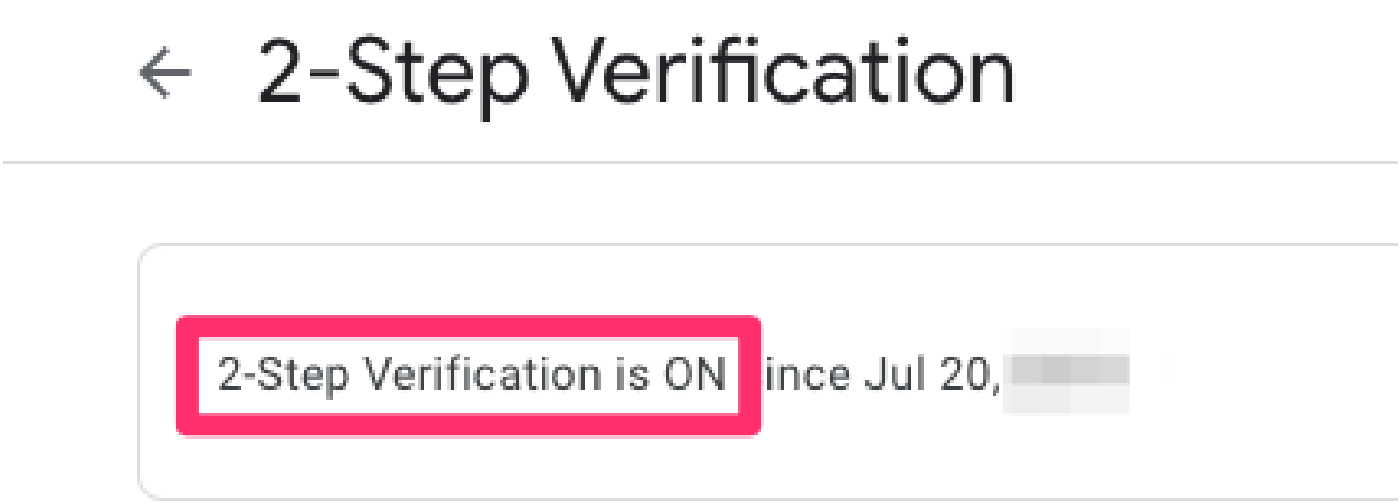
تسمح لك Google بإرسال رسائل بريد إلكتروني من عملاء بعيدين إلى Gmail. كان يوجد إعداد في Gmail لـ "التطبيقات غير الآمنة"، وسيواجه التطبيق خطأ إذا لم يكن هذا الإعداد مسموح به في نهاية Google. تمت إزالة هذا الإعداد، وفي مكانه خيار "التطبيقات الآمنة". يمكن الوصول إليه عبر:

mail.google.com>انقر فوق ملف التعريف الخاص بك (#1) > إدارة حساب Google الخاص بك (#2) > الأمان (#3) > كيفية تسجيل الدخول إلى Google > التحقق بخطوتين (#4)


1
2
Manage your Google Account
Add another account
Sign out
Privacy Policy • Terms of Service



من هذه الصفحة، تأكد من تشغيل التحقق ثنائي الخطوات.



يمكنك بعد ذلك التمرير لأسفل إلى "كلمات مرور التطبيق" لجعل Gmail يقوم بإنشاء كلمة مرور يمكن إستخدامها لتسجيل الدخول إلى حساب Google الخاص بك من تطبيق ال يدعم التحقق على خطوتين.

App passwords

App Passwords aren't recommended and are unnecessary in most cases. To help keep your account secure, use "Sign in with Google" to connect apps to your Google Account.

App passwords

None

← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. Learn more

You don't have any app passwords.

Select the app and device you want to generate the app password for.

Mail | Select device

- **iPhone**
- **iPad**
- **BlackBerry**
- **Mac**
- **Windows Phone**
- **Windows Computer**
- **Other *(Custom name)***

GENERATE

App passwords

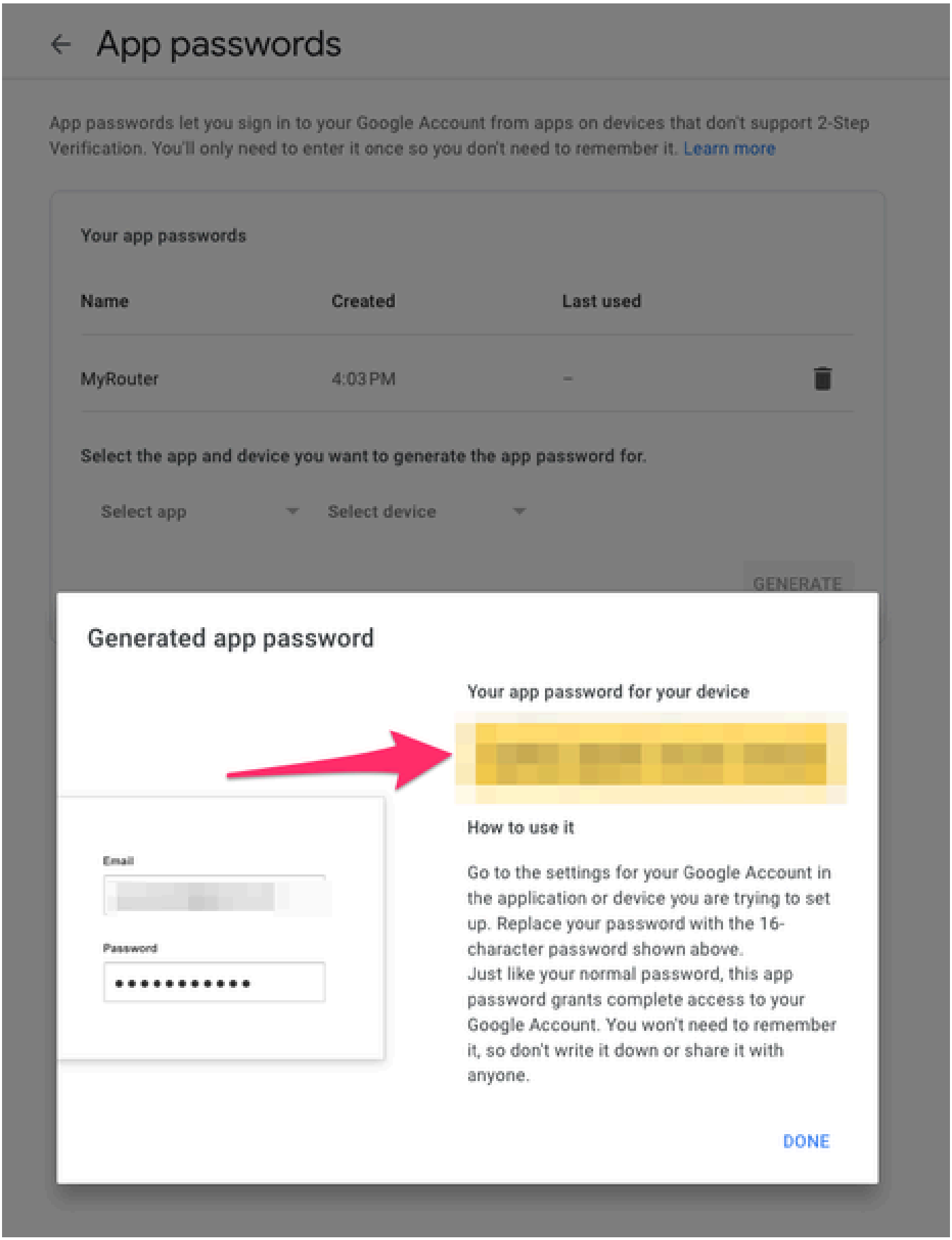
App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. Learn more

You don't have any app passwords.

Select the app and device you want to generate the app password for.

MyRouter

GENERATE



تم توضيح كلمة مرور التطبيق المكونة من 16 حرفا الموجودة في لقطة الشاشة هذه نظرا لارتباطها بحساب Gmail شخصي.

الآن بعد أن أصبح لديك كلمة مرور تطبيق ل Gmail، يمكنك إستخدام هذه الكلمة، بالإضافة إلى اسم حساب Gmail الخاص بك، كخادم بريد إلكتروني يستخدم لإعادة توجيه البريد الإلكتروني. التنسيق الذي سيتم تعيينه للخادم هو "username:password@host".

تكوين IM الأساسي

هناك العديد من الطرق التي يمكنك من خلالها تخصيص برنامج نصي ل IM لتلائم احتياجاتك المحددة، ولكن هذا المثال هو برنامج نصي ل IM أساسي لتشغيل وظيفة البريد الإلكتروني الآمن:

```
(config)# event manager environment _email_from <username@gmail.com>
(config)# event manager environment _email_to <EMAIL@domain.com>
(config)# event manager environment _email_server <username>:<password>@smtp.gmail.com

(config)# event manager applet SendSecureEmailEEM
(config-applet)#  event none
(config-applet)#    action 0010 mail server "$_email_server" to "$_email_to" from "$_email_from" cc "$_e
```

تنشئ التكوينات الأولى ثلاثة متغيرات بيئة EEM: _email_from و _email_to و _email_server. يتم تعريف كل واحد في متغير ليستهدف تغييرات التكوين. ثم قم بإنشاء البرنامج النصي SendSecureEmailEEM. حدث الإطلاق هنا هو "none" بحيث يمكنك تشغيل برنامج IM النصي يدويا باستخدام "# مدير الحدث تشغيل SendSecureEmailIM" (بدلا من انتظار حدث معين للتشغيل). بعد ذلك، يكون لديك إجراء واحد "خادم بريد" يتم إنشاء البريد الإلكتروني. يخبر الخياران "secure tls" و"port 587" الجهاز بالتفاوض على TLS على المنفذ 587، والذي تستمع إليه خوادم Gmail.

تحتاج أيضا إلى التأكد من أن حقل "من" صالح. إذا كنت تحاول الاتصال ك "أليس" لكنك تحاول إرسال بريد إلكتروني من "بوب"، مثل شخص لإرسال بريد إلكتروني بعنوان خادع موقت سيأتي من شخص آخر. يجب أن يتوافق الحقل "من" مع اسم الحساب المستخدم لإرسال البريد الإلكتروني على الخادم.

تم عرض المشكلة بالشهادات الافتراضية فقط المثبتة

يستخدم EEM OpenSSL لإجراء اتصال بخادم SMTP. لتأمين الاتصال، يرسل الخادم شهادة إلى OpenSSL قيد التشغيل في Cisco IOSd. وسيبحث IOS بعد ذلك عن نقطة ثقة مقترنة بتلك الشهادة.

على جهاز Cisco IOS XE، لا يتم تثبيت شهادات خوادم Gmail SMTP بشكل افتراضي. يجب إستيرادها يدويا لإنشاء الثقة. بدون الشهادات المثبتة، سيفشل تأكيد TLS بسبب "شهادة غير صحيحة".

تكون هذه الأخطاء مفيدة جدا لتصحيح أخطاء أي شهادة:

```
debug event manager action mail
debug crypto pki API
```

```
debug crypto pki callbacks
debug crypto pki messages
debug crypto pki scep
debug crypto pki server
debug crypto pki transactions
debug crypto pki validation
debug ssl openssl errors
debug ssl openssl ext
debug ssl openssl msg
debug ssl openssl states
```

يمكنك بدء التقاط حزمة مضمنة (EPC) على الموجه لالتقاط أي حركة مرور من وأ إلى خادم البريد الإلكتروني عند تشغيل IM:

```
! Trigger the EEM:
# event manager run SendSecureEmailEEM

<SNIP>

*Mar 15 21:51:32.798: CRYPTO_PKI: (A0693) Check for identical certs
*Mar 15 21:51:32.798: CRYPTO_PKI(Cert Lookup) issuer="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-

*Mar 15 21:51:32.798: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
94 40 D1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A

*Mar 15 21:51:32.799: CRYPTO_PKI: Cert record not found for issuer serial.
*Mar 15 21:51:32.799: CRYPTO_PKI : (A0693) Validating non-trusted cert
*Mar 15 21:51:32.799: CRYPTO_PKI: (A0693) Create a list of suitable trustpoints
*Mar 15 21:51:32.799: CRYPTO_PKI: crypto_pki_get_cert_record_by_issuer()
*Mar 15 21:51:32.799: CRYPTO_PKI: Unable to locate cert record by issuername
*Mar 15 21:51:32.799: CRYPTO_PKI: No trust point for cert issuer, looking up cert chain

*Mar 15 21:51:32.799: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
*Mar 15 21:51:32.799: CRYPTO_PKI: (A0693) No suitable trustpoints found
*Mar 15 21:51:32.799: CRYPTO_PKI: (A0693) Removing verify context

*Mar 15 21:51:32.799: CRYPTO_PKI: destroying ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 32, ref
*Mar 15 21:51:32.799: CRYPTO_PKI: ca_req_context released
*Mar 15 21:51:32.799: CRYPTO_OPSSL: Certificate verification has failed
*Mar 15 21:51:32.799: CRYPTO_PKI: Rcvd request to end PKI session A0693.
*Mar 15 21:51:32.799: CRYPTO_PKI: PKI session A0693 has ended. Freeing all resources.
*Mar 15 21:51:32.800: >>> ??? [length 0005]
*Mar 15 21:51:32.800: 15 03 03 00 02
*Mar 15 21:51:32.800:
*Mar 15 21:51:32.800: >>> TLS 1.2 Alert [length 0002], fatal bad_certificate
*Mar 15 21:51:32.800: 02 2A
*Mar 15 21:51:32.800:
*Mar 15 21:51:32.800: SSL3 alert write:fatal:bad certificate
*Mar 15 21:51:32.801: P11:C_OpenSession slot 1 flags 6
*Mar 15 21:51:32.801: SSL_connect:error in error
*Mar 15 21:51:32.801: 0:error:1416F086:SSL routines:tls_process_server_certificate:certificate verify f
```

في نهاية المطاف، الى يمكن ل OpenSSL إنشاء جلسة TLS الآمنة مع خادم SMTP، وبالتالي فإنها تتسبب في حدوث خطأ "شهادة غير صحيحة"، مما يتسبب في إيقاف تشغيل IM:

```
*Mar 15 21:51:32.801: %HA_EM-3-FMPD_SMTP: Error occurred when sending mail to SMTP server: username:pas
*Mar 15 21:51:32.802: %HA_EM-3-FMPD_ERROR: Error executing applet SendSecureEmailEEM statement 0010
```

يتم إرفاق التقاط الحزمة الموثقة من هذا التبادل ك "NoCertificateInstalled.pcap". تظهر الحزمة النهائية TLS من الموجه (10.122.x.x) إلى خادم Gmail SMTP (142.251.163.xx) أن تفاوض TLS تم إنهاؤه بسبب نفس رسالة "الشهادة السيئة" التي تم رؤيتها في تصحيح الأخطاء سابقا.

```
Frame 33: 61 bytes on wire (488 bits), 61 bytes captured (488 bits)
Ethernet II, Src: Cisco_a3:c5:f0 (74:86:0b:a3:c5:f0), Dst: Cisco_f0:44:45 (00:08:30:f0:44:45)
Internet Protocol Version 4, Src: 10.122.xx.xx, Dst: 142.251.163.xx
Transmission Control Protocol, Src Port: 13306, Dst Port: 587, Seq: 189, Ack: 4516, Len: 7
Transport Layer Security
TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Bad Certificate)
Content Type: Alert (21)
Version: TLS 1.2 (0x0303)
Length: 2
Alert Message
Level: Fatal (2)
Description: Bad Certificate (42)
```

شهادات تأمين SMTP

لأن الشهادات التي تسمح لجهاز Cisco IOS XE بالثقة في خوادم Gmail مفقودة، فإن الإصلاح هو تثبيت واحدة/كل تلك الشهادات في TrustPoint على الجهاز.

على سبيل المثال، تظهر التصحيح الكامل للاختبار السابق عمليات البحث عن الشهادات التي تمت:

```
CRYPTO_PKI(Cert Lookup) issuer="cn=GTS CA 1C3,o=Google Trust Services LLC,c=US" serial number= 52 87 E0
CRYPTO_PKI(Cert Lookup) issuer="cn=GTS Root R1,o=Google Trust Services LLC,c=US" serial number= 02 03 B
CRYPTO_PKI(Cert Lookup) issuer="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-sa,c=BE" serial number
```

يلزم تثبيت شهادة لكل من هذه المصدرين تحت نقطة ثقة حتى يتمكن الجهاز من إنشاء جلسة عمل آمنة باستخدام خوادم SMTP من Gmail. يمكنك إنشاء نقطة ثقة لكل مصدر باستخدام التكوينات التالية:

```
crypto pki trustpoint CA-GTS-1C3
  enrollment terminal
  revocation-check none
  chain-validation stop

crypto pki trustpoint CA-GTS-Root-R1
```

```
  enrollment terminal
  revocation-check none
  chain-validation stop

crypto pki trustpoint CA-GlobalSign-Root
  enrollment terminal
  revocation-check none
  chain-validation stop

crypto pki trustpoint CA-gmail-SMTP
  enrollment terminal
  revocation-check none
  chain-validation stop
```

تم الآن إعداد نقطة ثقة لكل مصدر، ومع ذلك، لا توجد شهادات فعلية مرتبطة بها حتى الآن. وهي في الأساس نقاط ثقة فارغة:

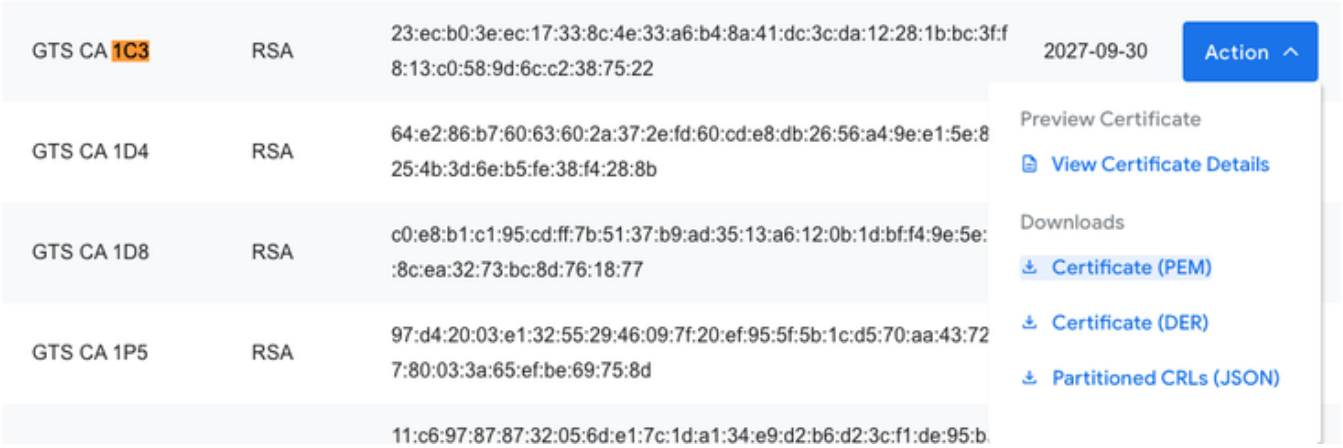
```
# show run | sec crypto pki certificate chain CA-
crypto pki certificate chain CA-GTS-1C3
crypto pki certificate chain CA-GTS-Root-R1
crypto pki certificate chain CA-GlobalSign-Root
crypto pki certificate chain CA-gmail-SMTP
```

يجب تعقب مكان هذه الشهادات ثم تثبيتها على الجهاز.

بالبحث عبر الإنترنت عن "Google Trust Services 1C3"، نأتي بسرعة عبر مستودع Google Trust Services للشهادات:

https://pki.goog/repository/

بعد تمديد كل التراخيص على تلك الصفحة، يمكنك البحث للعثور على "1C3"، انقر القائمة المنسدلة "الإجراء"، وقم بتنزيل شهادة PEM:



إن فتح ملف PEM الذي تم تنزيله باستخدام محرر نصي يظهر أن هذه مجرد شهادة يمكن إستيرادها على جهاز Cisco IOS XE تحت TrustPoint الذي أنشأته مسبقا:

```
-----BEGIN CERTIFICATE-----
MIIFljCCA36gAwIBAgINAgO8U1lrNMcY9QFQZjANBgkqhkiG9w0BAQsFADBHMQsw
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU
<snip>
AJ2xDx8hcFH1mt0G/FX0Kw4zd8NLQsLxdxP8c4CU6x+7Nz/OAipmsHMdMqUybDKw
juDEI/9bfU1lcKwrmz3O2+BtjjKAvpafkmO8l7tdufThcV4q5O8DIrGKZTqPwJNl
1IXNDw9bg1kWRxYtnCQ6yICmJhSFm/Y3m6xv+cXDBlHz4n/FsRC6UfTd
-----END CERTIFICATE-----
```

يمكنك إستيراده تحت نقطة الاعتماد "CA-GTS-1C3" باستخدام أوامر التكوين:

```
(config)# crypto pki authenticate CA-GTS-1C3

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIFljCCA36gAwIBAgINAgO8U1lrNMcY9QFQZjANBgkqhkiG9w0BAQsFADBHMQsw
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU
<snip>
juDEI/9bfU1lcKwrmz3O2+BtjjKAvpafkmO8l7tdufThcV4q5O8DIrGKZTqPwJNl
1IXNDw9bg1kWRxYtnCQ6yICmJhSFm/Y3m6xv+cXDBlHz4n/FsRC6UfTd

Certificate has the following attributes:
Fingerprint MD5: 178EF183 43CCC9E0 ECB0E38D 9DEA03D8
Fingerprint SHA1: 1E7EF647 CBA15028 1C608972 57102878 C4BD8CDC
Certificate validated - Signed by existing trustpoint CA certificate.

Trustpoint CA certificate accepted.
% Certificate successfully imported

(config)#
```

وبعد ذلك يمكنك تأكيد أن الشهادة قد تم تثبيتها:

```
# show run | sec crypto pki certificate chain CA-GTS-1C3
crypto pki certificate chain CA-GTS-1C3
 certificate ca 0203BC53596B34C718F5015066
  30820596 3082037E A0030201 02020D02 03BC5359 6B34C718 F5015066 300D0609
  2A864886 F70D0101 0B050030 47310B30 09060355 04061302 55533122 30200603
  55040A13 19476F6F 676C6520 54727573 74205365 72766963 6573204C 4C433114
  <snip>
  E1715E2A E4EF0322 B18A653A 8FC09365 D485CD0F 0F5B8359 1647162D 9C243AC8
  80A62614 859BF637 9BAC6FF9 C5C30651 F3E27FC5 B1100BA51 F4DD
    quit



#show crypto pki certificates verbose CA-GTS-1C3
CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 0203BC53596B34C718F5015066
```

```
  Certificate Usage: Signature
  Issuer:
    cn=GTS Root R1
    o=Google Trust Services LLC
    c=US
  Subject:
    cn=GTS CA 1C3
    o=Google Trust Services LLC
    c=US
  CRL Distribution Points:
    http://crl.pki.goog/gtsr1/gtsr1.crl
  Validity Date:
    start date: 00:00:42 UTC Aug 13 2020
    end date: 00:00:42 UTC Sep 30 2027
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA256 with RSA Encryption
  Fingerprint MD5: 178EF183 43CCC9E0 ECB0E38D 9DEA03D8
  Fingerprint SHA1: 1E7EF647 CBA15028 1C608972 57102878 C4BD8CDC
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 8A747FAF 85CDEE95 CD3D9CD0 E24614F3 71351D27
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: E4AF2B26 711A2B48 27852F52 662CEFF0 8913713E
    Authority Info Access:
        OCSP URL: http://ocsp.pki.goog/gtsr1
        CA ISSUERS: http://pki.goog/repo/certs/gtsr1.der
    X509v3 CertificatePolicies:
        Policy: 2.23.140.1.2.2
        Policy: 2.23.140.1.2.1
        Policy: 1.3.6.1.4.1.11129.2.5.3
            Qualifier ID: 1.3.6.1.5.5.7.2.1
            Qualifier Info: https://pki.goog/repository/
    Extended Key Usage:
        Client Auth
        Server Auth
  Cert install time: 02:31:20 UTC Mar 16 2023
Cert install time in nsec: 1678933880873946880
  Associated Trustpoints: CA-GTS-1C3
```

بعد ذلك، يمكنك تثبيت الشهادات للمصدرين الآخرين.

CA-GTS-Root-R1:

التكوين:

مفسد (إبراز إلى القراءة)

```
(config)# crypto pki authenticate CA-GTS-Root-R1

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

```
MIIFVzCCAz+gAwIBAgINAgPlk28xsBNJiGuiFzANBgkqhkiG9w0BAQwFADBHMQsw
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU
<snip>
2tIMPNuzjsmhDYAPexZ3FL//2wmUspO8IFgV6dtxQ/PeEMMA3KgqlbbC1j+Qa3bb
bP6MvPJwNQzcmRk13NfIRmPVNnGuV/u3gm3c

Certificate has the following attributes:
Fingerprint MD5: 05FED0BF 71A8A376 63DA01E0 D852DC40
Fingerprint SHA1: E58C1CC4 913B3863 4BE9106E E3AD8E6B 9DD9814A

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

(config)# end
```

(config)# crypto pki authenticate CA-GTS-Root-R1أدخل شهادة CA التي تم ترميزها للقاعدة
64.End باستخدام سطر فارغ وأ كلمة "quit" على سطر بحد ذاته
MIIFVzCCAz+gAwIBAgINAgPlk28xsBNJiGuiFzANBgkqhkiG9w0BAQwFADBHMQswCYDVQQQQGEwV
EiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU<snip>2tIMPNuzjsmhDYAPexZ3FL//2w
تحتوي على السمات التالية:FingerMD5: 05FED0BF 71A8A3763DA01E0 D852DC40
FingerSha1: E58C1CC4 913B38634BE99913BE99913 06E3AD8E6B 9DD9814A٪ هل تقبل هذه
الشهادة؟ [YES/NO]: تم قبول شهادة CA ل YesTrustPoint. تم إستيراد شهادة٪ (config)# بنجاح

التحقق من صحة running-config:

مفس (إبراز إلى القارعة)

```
# show run | sec crypto pki certificate chain CA-GTS-Root-R1
crypto pki certificate chain CA-GTS-Root-R1
 certificate ca 0203E5936F31B01349886BA217
  30820557 3082033F A0030201 02020D02 03E5936F 31B01349 886BA217 300D0609
  2A864886 F70D0101 0C050030 47310B30 09060355 04061302 55533122 30200603
  <snip>
  6775C119 3A2B474E D3428EFD 31C81666 DAD20C3C DBB38EC9 A10D800F 7B167714
  BFFFDB09 94B293BC 205815E9 DB7143F3 DE10C300 DCA82A95 B6C2D63F 906B76DB
  6CFE8CBC F270350C DC991935 DCD7C846 63D53671 AE57FBB7 826DDC
    quit
```

تشغيل العرض | sec crypto pki شهادة سلسلة CA-GTS-Root-R1crypto PKI شهادة سلسلة
شهادة CA-GTS-Root-R1 شهادة 0203E5936F31B01349886BA217 3082057 3082033F
A003202020D020D203E59333333 6F 31B01349 886BA217 300D0609 2a86486 F70d0101
0c05030 47310b30090603504061302 553312202020200060033333033333033330330333333033
p> 6775c119 3a2b474e d3428EFD 31c81666 dad20c3c dbb38ec9 a10d800f 7b167714
bffdb094b293bc 205815e9 db7143f3 DE10C300 DCA82A95 B6C2D63F 906B76DB 6CFE8CBC
F270350C DC991935 DCD7C8463D53671 AE57FBB7 826DDC quit

إظهار التحقق من التشفير:

مفس (إبراز إلى القارعة)

```
# show crypto pki certificates verbose CA-GTS-Root-R1
```

```
CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 0203E5936F31B01349886BA217
  Certificate Usage: Signature
  Issuer:
    cn=GTS Root R1
    o=Google Trust Services LLC
    c=US
  Subject:
    cn=GTS Root R1
    o=Google Trust Services LLC
    c=US
  Validity Date:
    start date: 00:00:00 UTC Jun 22 2016
    end date: 00:00:00 UTC Jun 22 2036
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (4096 bit)
  Signature Algorithm: SHA384 with RSA Encryption
  Fingerprint MD5: 05FED0BF 71A8A376 63DA01E0 D852DC40
  Fingerprint SHA1: E58C1CC4 913B3863 4BE9106E E3AD8E6B 9DD9814A
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: E4AF2B26 711A2B48 27852F52 662CEFF0 8913713E
    X509v3 Basic Constraints:
        CA: TRUE
    Authority Info Access:
  Cert install time: 14:39:38 UTC Mar 13 2023
Cert install time in nsec: 1678718378546968064
  Associated Trustpoints: CA-GTS-Root-R1 Trustpool
```

عرض شهادات crypto pki verbose ca-GTS-root-R1CA حالة شهادة: الإصدار المتوفر: 3 شهادة رقم تسلسلي (hex): 0203E5936F31B01349886BA217 إستخدام شهادة: مصدر التوقيع: cn=GTS root R1=Google Trust Services LLC=الموضوع الأمريكي: cn=GTS Root R1=Google Trust Services=c تاريخ الصلاحية في الولايات المتحدة: تاريخ البدء: 00:00:00 بالتوقيت العالمي في 22 يونيو 2016 تاريخ الانتهاء: 00:00:00 بالتوقيت العالمي في 22 يونيو 2036 معلومات مفتاح الموضوع: خوارزمية مفتاح التعريف العام: (4096 بت) خوارزمية التوقيع: SHA384 مع بصمة تشفير RSA MD5: 05FED0BF 71A8A3763DA0 E0 D852DC40 بصمة الإصبع SHA1: E58C1CC4 913B3863 4BE9106e E3AD8E6B 9DD9814A x509v3 إستخدام مفتاح x509v3: 8600000 توقيع مفتاح التوقيع الرقمي توقيع CRL x509v3 مفتاح الموضوع: E4AF2B26 711a2B48 27852F52 662CEF0 8913713e x509v3 القيود الأساسية: CA: TRUE Authority Info Access: وقت تثبيت CERT: 14:39:38 UTC MAR 132023 وقت تثبيت Cert في nsec:
167871885469868886888686888686888686868888868688866868888868688866886868866888886688
064 Associated TrustPoints: CA-GTS-Root-R1 TrustPool

جذر CA-GlobalSign:

تم العثور على هذه الشهادة في هذا الموقع:

https://support.globalsign.com/ca-certificates/root-certificates/globalsign-root-certificates

التكوين:

مفسد (إبراز إلى القارعة)

```
(config)# crypto pki authenticate CA-GlobalSign-Root

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
<snip>
DKqC5Jl R3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbME
HMUfpIBvFSDJ3gyICh3WZlXi/EjJKSZp4A==

Certificate has the following attributes:
Fingerprint MD5: 3E455215 095192E1 B75D379F B187298A
Fingerprint SHA1: B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

(config)# end
```

(config)# crypto pki authenticate CA-GlobalSign-RootEnter شهادة CA المرمزة للقاعدة 64.End باستخدام سطر فارغ أو كلمة "quit" على سطر بواسطة نفسه
MIIDdTCCAl2gAwIBAgILBAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkGA1UEBhMCQkUxG
FpIBvFSDJ3gyICh3WZlXi/EjJKSZp4A==Certificate تحتوي على السمات التالية:FingerMD5:
3E455215 095192E1 B75D379F B187298A Finger Sha1: B1BC968B4D4F49D62AA28 9A81
F2150152 A41D829C٪ هل تقبل هذه الشهادة؟ [YES/NO]: تم قبول شهادة CA ل YesTrustPoint.
تم إستيراد شهادة٪ (config)# بنجاح

التحقق من صحة running-config:

مفسد (إبراز إلى القارعة)

```
# show run | sec crypto pki certificate chain CA-GlobalSign-Root
crypto pki certificate chain CA-GlobalSign-Root
 certificate ca 040000000001154B5AC394
  30820375 3082025D A0030201 02020B04 00000000 01154B5A C394300D 06092A86
  <snip>
  2AC45631 95D06789 852BF96C A65D469D 0CAA82E4 9951DD70 B7DB563D 61E46AE1
  5CD6F6FE 3DDE41CC 07AE6352 BF5353F4 2BE9C7FD B6F7825F 85D24118 DB81B304
  1CC51FA4 806F1520 C9DE0C88 0A1DD666 55E2FC48 C9292669 E0
    quit
```

تشغيل العرض | sec crypto pki شهادة سلسلة CA-GlobalSign-Rootcrypto PKI شهادة
سلسلة CA-GlobalSign-Root CA 040000001154B5AC394 30820375 3082025D
A030201020B0400001154B3035A C394300D 06092A86 <snip> 2AC45631 95D06789 852BF96C
A65D469D 0CAA82E4 9951DD70 B7DB563D 61E4e6AE1 5CD6F6FE 3DE4 1CC 07AE6352
BF5353F4 2BE9C7FD B6F7825F 85D24118 DB81B304 1CC51FA4 806f1520
C9DE0C88A1DD6655E2FC48 C92922222222 إنهاء 69 E0

إظهار التحقق من التشفير:

مفسد (إبراز إلى القراءة)

```
#show crypto pki certificates verbose CA-GlobalSign-Root
CA Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 040000000001154B5AC394
Certificate Usage: Signature
Issuer:
cn=GlobalSign Root CA
ou=Root CA
o=GlobalSign nv-sa
c=BE
Subject:
cn=GlobalSign Root CA
ou=Root CA
o=GlobalSign nv-sa
c=BE
Validity Date:
start date: 12:00:00 UTC Sep 1 1998
end date: 12:00:00 UTC Jan 28 2028
Subject Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: 3E455215 095192E1 B75D379F B187298A
Fingerprint SHA1: B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C
X509v3 extensions:
X509v3 Key Usage: 6000000
Key Cert Sign
CRL Signature
X509v3 Subject Key ID: 607B661A 450D97CA 89502F7D 04CD34A8 FFFCFD4B
X509v3 Basic Constraints:
CA: TRUE
Authority Info Access:
Cert install time: 03:03:01 UTC Mar 16 2023
Cert install time in nsec: 1678935781942944000
Associated Trustpoints: CA-GlobalSign-Root
```

#show crypto pki الشهادات verbose ca-GlobalSign-RootCA CertificateStatus: AvailableVersion: 3Certificate Serial Number (hex): 040000001154B5AC394Certificate Use: SignatureIssuer: cn=GlobalSign root caOu=Root CAo=GlobalSign nv-sac=BESubject: cn=GlobalSign Root CAo=CA=CAGlobalSign nv-sac=BEValbility التاريخ: تاريخ البدء: 12:00:00 UTC Sep 1998 تاريخ الانتهاء: 12:00:00 UTC يناير 28 2028Subject Key Info:خوارزمية المفتاح العام: rsaEncryptionRSA المفتاح العام: (2048 بت)خوارزمية التوقيع: SHA1 مع تشفير RSA FingerMD5: 3e455215095199199 E1 B75D379F B187298A بصمة الإصبع SHA1: B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C x509v3: إستخدام مفتاح x509v3: 600000Key CERT CRL SignatureX509v3 Subject Key ID: 607B661A 450D97CA 89502F7D 04CD34A8 FFFCFD4B X509v3 القيود الأساسية:CA: CA: TRUEAuexpansion Information Access:وقت تثبيت Cert: 03:03:01 UTC Mar 162023 وقت تثبيت Cert في nsec: 16798 35781942944000 نقاط الثقة المرتبطة: CA-GlobalSign-Root

CA-gmail-SMTP:

تم العثور على شهادة TLS لخوادم Gmail (CA-Gmail-SMTP) باستخدام الخطوات الموثقة هنا: [استخدام شهادات TLS للتنقل الآمن]

التكوين:

[مفرس] (إزارب إلى القارءة)

```
(ca-trustpoint)# crypto pki authenticate CA-gmail-SMTP

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIEhjCCA26gAwIBAgIQUofgQKT+9wcSaLBP3d3w9DANBgkqhkiG9w0BAQsFADBG
MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
<snip>
b1J2gZAyjyd4nfFRG1jeL5KrsfUR9hIXufqySvlPUoPuKSi3fvsIS21BYEXEe8uZ
gBxJaeTUjncvow==

Trustpoint 'CA-gmail-SMTP' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required
Certificate has the following attributes:
Fingerprint MD5: 19651FBE 906A414D 6D57B783 946F30A2
Fingerprint SHA1: 4EF392CB EEB46D5E 47433953 AAEF313F 4C6D2825

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

(config)#
```

(ca-trustPoint)# crypto pki authenticate CA-gmail-SMTPEnter القاعدة 64 المرمزة للشهادة CA.End مع خط فارغ أو كلمة "quit" على خط بنفسها
MIIEhjCCA26gAwIBAgIQUofgQKT+9wcSaLBP3d3w9DANBgkqhkiG9w0BAQsFADBGMQswCYDVQQQQQ
21BYEXEE8U GBXJaETUjncvow==TrustPoint 'CA-gmail-SMTP' هي شهادة CA ثانوية.ولكن
الشهادة ليست شهادة CA.التحقق اليدوي المطلوب تحتوي الشهادة على السمات
التالية:Finger Print MD5: 19651FBE 906A414D 6D57B783 946F30A2 Finger SHA1: 4EF392CB
EEB46D5E 7433953 AEF313F 4C6D2825٪ هل تقبل هذه الشهادة؟ [نعم/لا]: تم قبول شهادة
CA لـ YesTrustPoint.٪ تم إستيراد الشهادة بنجاح(config)#

التحقق من صحة running-config:

[مفرس] (إزارب إلى القارءة)

```
# show run | sec crypto pki certificate chain CA-gmail-SMTP
 crypto pki certificate chain CA-gmail-SMTP
  certificate ca 5287E040A4FEF7071268B04FDDDDF0F4
  30820486 3082036E A0030201 02021052 87E040A4 FEF70712 68B04FDD DDF0F430
  0D06092A 864886F7 0D01010B 05003046 310B3009 06035504 06130255 53312230
  <snip>
  92ABB1F5 11F61217 B9FAB24A F94F5283 EE2928B7 7EFB084B 6D416045 C47BCB99
  801C4969 E4D48E77 2FA3
```

```
quit
```

تشغيل العرض | sec crypto pki شهادة سلسلة ca-gmail-smtp crypto pki شهادة سلسلة CA-gmail-SMTP شهادة ca 5287E040A4FEF7071268B04FDDDDF0F4 30820486 3082036E A003020202105287E040A4A40A4 f70712 68b04fdd ddf0f430 0d06092a 86488f7 0d01010b 05003046 310b300960350406130255312230 <snip> 92abb06 F5 11F61217 B9FAB24A F94F5283 EE2928B7 7EFB084B 6D416045 C47BCB99801C4969 E4D48E77 2FA3 إستقال

إظهار التحقق من التشفير:

مفسد (إبراز إلى القراءة)

```
# show crypto pki certificates verbose CA-gmail-SMTP
CA Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 5287E040A4FEF7071268B04FDDDDF0F4
Certificate Usage: Signature
Issuer:
cn=GTS CA 1C3
o=Google Trust Services LLC
c=US
Subject:
cn=smtp.gmail.com
CRL Distribution Points:
http://crls.pki.goog/gts1c3/moVDfISia2k.crl
Validity Date:
start date: 09:15:03 UTC Feb 20 2023
end date: 09:15:02 UTC May 15 2023
Subject Key Info:
Public Key Algorithm: ecEncryption
EC Public Key: (256 bit)
Signature Algorithm: SHA256 with RSA Encryption
Fingerprint MD5: 19651FBE 906A414D 6D57B783 946F30A2
Fingerprint SHA1: 4EF392CB EEB46D5E 47433953 AAEF313F 4C6D2825
X509v3 extensions:
X509v3 Key Usage: 80000000
Digital Signature
X509v3 Subject Key ID: 5CC36972 D07FE997 510E1A67 8A8ECC23 E40CFB68
X509v3 Basic Constraints:
CA: FALSE
X509v3 Subject Alternative Name:
smtp.gmail.com
IP Address :
OtherNames :
X509v3 Authority Key ID: 8A747FAF 85CDEE95 CD3D9CD0 E24614F3 71351D27
Authority Info Access:
OCSP URL: http://ocsp.pki.goog/gts1c3
CA ISSUERS: http://pki.goog/repo/certs/gts1c3.der
X509v3 CertificatePolicies:
Policy: 2.23.140.1.2.1
Extended Key Usage:
Server Auth
Cert install time: 03:10:41 UTC Mar 16 2023
Cert install time in nsec: 1678936241822955008
Associated Trustpoints: CA-gmail-SMTP
```

عرض شهادات crypto pki verbose ca-gmail-smtpca CertificateStatus: AvailableVersion: 3Certificate Serial Number (hex): 5287E040A4FEF7071268B04FDDDDF0F4Certificate Use: SignatureIssuer: cn=GTS CA 1C3o=Google Trust Services LLC=USSubject: cn=smtp.gmail.crl نقاط التوزيع: http://crls.pki.goog/gts1c3/moVDfISia2k.crlValidity التاريخ: تاريخ البدء: 09:15:03 UTC فبراير 2023 تاريخ الانتهاء: 09:15:02 UTC مايو 15 2023 معلومات مفتاح الموضوع:خوارزمية مفتاح عام: ecEncryption مفتاح عام: (256 بت(خوارزمية التوقيع: SHA256 بصمة MD5: 19651FBE 906A414D 6D57B87 3 946F30A2 بصمة الإصبع RSA مع تشفير الإصبع SHA1: 4EF392CB EEB46D5E 47433953 AEF313F 4C6D2825 x509v3:استخدام مفتاح x509v3: 800000 التوقيع الرقمي X509v3 معرف مفتاح الموضوع: 5CC3699 2 D07FE997 510E1A67 8A8ECC23 E40CFB68 x509v3 القيود الأساسية:CA: FALSEX509v3 Subject Alternative Name:smtp.gmail.com عنوان IP: OtherNames: X509v3 Authority Key ID: 8A747FAF 85CDEE95 CD3D9CD0 E4 614F3 71351D27 Authority Info Access:OCSP URL: http://ocsp.pki.goog/gts1c3CA Issuers: http://pki.goog/repo/certs/gts1c3.derX509v3 CertificatePolicies:Policy: 2.23.140.1.2.1Extended Key Use:Server AuthCert time: 03:10:41 UTC Mar 16:2023 وقت تثبيت CERT في NSEC: 1678936241822955008AssociatedContacts8AssociatedPointsAssociatedTtttttrPoints: CA-gmail-SMTP

طريقة أسهل للعثور على التراخيص

وبدلا من ذلك، يمكنك مواصلة إستخدام كاملة OpenSSL من خادم/كمبيوتر محمول كطريقة لتصحيح الأخطاء دون الاضطرار إلى إستخدام خادم SMTP من الشهادات على الحصول أسهل للبحث في Google تتبعهم:

```
openssl s_client -showcerts -verify 5 -connect gmail-smtp-in.l.google.com:25 -starttls smtp
```

يمكنك أيضا زيارة الموقع use smtp.gmail.com:

```
openssl s_client -showcerts -verify 5 -connect smtp.gmail.com:25 -starttls smtp
```

وتستتضمن مخرجات هذا الاستدعاء الشهادات الفعلية نفسها التي يمكن إستخدامها لتكوينات "crypto pki authenticate <trustPoint>".

إختبار IM باستخدام SMTP الآن مرة أخرى

الآن بعد أن يتم تطبيق الشهادات على جهاز Cisco IOS XE، يرسل برنامج IM النصي رسائل SMTP الآمنة كما هو متوقع.

```
# event manager run SendSecureEmailEEM
```

تحقق من المخزن الخاص بمخرجات التشفير الكامل وتصحيح SSL:

مفسد (إبراز إلى القراءة)

```
# event manager run SendSecureEmailEEM

*Mar 16 03:28:50.673: CRYPTO_OPSSL: Allocated the memory for OPSSLContext
*Mar 16 03:28:50.673: CRYPTO_OPSSL: Set cipher specs to mask 0x02FC0000 for version 128
*Mar 16 03:28:50.674: Set the Default EC Curve list: 0x70Set the EC curve list: secp521r1:secp384r1:pri
*Mar 16 03:28:50.674: opssl_SetPKIInfo entry
*Mar 16 03:28:50.674: CRYPTO_PKI: (A069B) Session started - identity selected (TP-self-signed-486541296)
*Mar 16 03:28:50.674: CRYPTO_PKI: Begin local cert chain retrieval.
*Mar 16 03:28:50.674: CRYPTO_PKI(Cert Lookup) issuer="cn=IOS-Self-Signed-Certificate-486541296" serial

*Mar 16 03:28:50.674: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
1C 7F 3D 52 67 66 D5 59 E2 66 58 E7 8B E7 9B 8E

*Mar 16 03:28:50.675: CRYPTO_PKI: Done with local cert chain fetch 0.
*Mar 16 03:28:50.675: CRYPTO_PKI: Rcvd request to end PKI session A069B.
*Mar 16 03:28:50.675: CRYPTO_PKI: PKI session A069B has ended. Freeing all resources.TP-self-signed-486
*Mar 16 03:28:50.675: opssl_SetPKIInfo done.
*Mar 16 03:28:50.675: CRYPTO_OPSSL: Common Criteria is disabled on this session.Disabling Common Criter

*Mar 16 03:28:50.675: CRYPTO_OPSSL: ciphersuites ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA
*Mar 16 03:28:50.676: Handshake start: before SSL initialization
*Mar 16 03:28:50.676: SSL_connect:before SSL initialization
*Mar 16 03:28:50.676: >>> ??? [length 0005]
*Mar 16 03:28:50.676: 16 03 01 00 95
*Mar 16 03:28:50.676:
*Mar 16 03:28:50.676: >>> TLS 1.2 Handshake [length 0095], ClientHello
*Mar 16 03:28:50.676: 01 00 00 91 03 03 26 4B 9F B3 44 94 FD 5F FD A1
<snip>
*Mar 16 03:28:50.679: 03 03 01 02 01
*Mar 16 03:28:50.679:
*Mar 16 03:28:50.679: SSL_connect:SSLv3/TLS write client hello
*Mar 16 03:28:50.692: <<< ??? [length 0005]
*Mar 16 03:28:50.692: 16 03 03 00 3F
*Mar 16 03:28:50.692:
*Mar 16 03:28:50.692: SSL_connect:SSLv3/TLS write client hello
*Mar 16 03:28:50.692: <<< TLS 1.2 Handshake [length 003F], ServerHello
*Mar 16 03:28:50.692: 02 00 00 3B 03 03 64 12 7E 05 25 F6 7A BD A0 2E
*Mar 16 03:28:50.692: 58 83 12 7F 90 CD F4 AB E2 69 53 A8 C7 FC 44 4F
*Mar 16 03:28:50.692: 57 4E 47 52 44 01 00 C0 2B 00 00 13 00 17 00 00
*Mar 16 03:28:50.693: FF 01 00 01 00 00 0B 00 02 01 00 00 23 00 00
*Mar 16 03:28:50.693: TLS server extension "unknown" (id=23), len=0
TLS server extension "renegotiate" (id=65281), len=1

*Mar 16 03:28:50.693: 00
*Mar 16 03:28:50.693: TLS server extension "EC point formats" (id=11), len=2

*Mar 16 03:28:50.693: 01 00
*Mar 16 03:28:50.693: TLS server extension "session ticket" (id=35), len=0

*Mar 16 03:28:50.693: <<< ??? [length 0005]
*Mar 16 03:28:50.693: 16 03 03 0F 9A
*Mar 16 03:28:50.694:
*Mar 16 03:28:50.702: SSL_connect:SSLv3/TLS read server hello
*Mar 16 03:28:50.702: <<< TLS 1.2 Handshake [length 0F9A], Certificate
*Mar 16 03:28:50.702: 0B 00 0F 96 00 0F 93 00 04 8A 30 82 04 86 30 82
*Mar 16 03:28:50.702: 03 6E A0 03 02 01 02 02 10 52 87 E0 40 A4 FE F7
```

```
<snip>
*Mar 16 03:28:50.763: 82 35 CF 62 8B C9 24 8B A5 B7 39 0C BB 7E 2A 41
*Mar 16 03:28:50.763: BF 52 CF FC A2 96 B6 C2 82 3F
*Mar 16 03:28:50.763:
*Mar 16 03:28:50.765: CC_DEBUG: Entering shim layer app callback function
*Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) Session started - identity not specified
*Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) Adding peer certificate
*Mar 16 03:28:50.767: CRYPTO_PKI: Added x509 peer certificate - (1162) bytes
*Mar 16 03:28:50.767: CRYPTO_PKI: (A069C) Adding peer certificate
*Mar 16 03:28:50.768: CRYPTO_PKI: Added x509 peer certificate - (1434) bytes
*Mar 16 03:28:50.768: CRYPTO_PKI: (A069C) Adding peer certificate
*Mar 16 03:28:50.770: CRYPTO_PKI: Added x509 peer certificate - (1382) bytes
*Mar 16 03:28:50.770: CRYPTO_OPSSL: Validate Certificate Chain Callback
*Mar 16 03:28:50.770: CRYPTO_PKI(Cert Lookup) issuer="cn=GTS CA 1C3,o=Google Trust Services LLC,c=US" s

*Mar 16 03:28:50.770: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
A7 CC 4B 0F 36 C3 AC D1 2F 77 DD 1D 9A 37 DC FC

*Mar 16 03:28:50.770: CRYPTO_PKI(Cert Lookup) issuer="cn=GTS Root R1,o=Google Trust Services LLC,c=US" 

*Mar 16 03:28:50.771: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
03 9F CF 59 82 EE 09 CC 4F 53 AE D8 02 7E 4B AF

*Mar 16 03:28:50.771: CRYPTO_PKI(Cert Lookup) issuer="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-

*Mar 16 03:28:50.771: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
94 40 D1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A

*Mar 16 03:28:50.771: CRYPTO_PKI: Cert record not found for issuer serial.
*Mar 16 03:28:50.772: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
*Mar 16 03:28:50.772: CRYPTO_PKI: Found a subject match
*Mar 16 03:
#28:50.772: CRYPTO_PKI: ip-ext-val: IP extension validation not required:Incrementing refcount for cont
*Mar 16 03:28:50.773: CRYPTO_PKI: create new ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 35
*Mar 16 03:28:50.773: CRYPTO_PKI: (A069C)validation path has 1 certs

*Mar 16 03:28:50.773: CRYPTO_PKI: (A069C) Check for identical certs
*Mar 16 03:28:50.773: CRYPTO_PKI(Cert Lookup) issuer="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-

*Mar 16 03:28:50.774: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
94 40 D1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A

*Mar 16 03:28:50.774: CRYPTO_PKI: Cert record not found for issuer serial.
*Mar 16 03:28:50.774: CRYPTO_PKI : (A069C) Validating non-trusted cert
*Mar 16 03:28:50.774: CRYPTO_PKI: (A069C) Create a list of suitable trustpoints
*Mar 16 03:28:50.774: CRYPTO_PKI: crypto_pki_get_cert_record_by_issuer()
*Mar 16 03:28:50.774: CRYPTO_PKI: Found a issuer match
*Mar 16 03:28:50.774: CRYPTO_PKI: (A069C) Suitable trustpoints are: CA-GlobalSign-Root,
*Mar 16 03:28:50.775: CRYPTO_PKI: (A069C) Attempting to validate certificate using CA-GlobalSign-Root p
*Mar 16 03:28:50.775: CRYPTO_PKI: (A069C) Using CA-GlobalSign-Root to validate certificate
*Mar 16 03:28:50.775: CRYPTO_PKI(make trusted certs chain)
*Mar 16 03:28:50.775: CRYPTO_PKI: Added 1 certs to trusted chain.
*Mar 16 03:28:50.775: CRYPTO_PKI: Prepare session revocation service providers
*Mar 16 03:28:50.776: P11:C_CreateObject:
*Mar 16 03:28:50.776: CKA_CLASS: PUBLIC KEY
*Mar 16 03:28:50.776: CKA_KEY_TYPE: RSA
*Mar 16 03:28:50.776: CKA_MODULUS:
DA 0E E6 99 8D CE A3 E3 4F 8A 7E FB F1 8B 83 25
6B EA 48 1F F1 2A B0 B9 95 11 04 BD F0 63 D1 E2
<snip>

*Mar 16 03:28:50.780: CKA_PUBLIC_EXPONENT: 01 00 01
```

```
*Mar 16 03:28:50.780: CKA_VERIFY_RECOVER: 01
*Mar 16 03:28:50.780: CRYPTO_PKI: Deleting cached key having key id 45
*Mar 16 03:28:50.781: CRYPTO_PKI: Attempting to insert the peer's public key into cache
*Mar 16 03:28:50.781: CRYPTO_PKI:Peer's public inserted successfully with key id 46
*Mar 16 03:28:50.781: P11:C_CreateObject: 131118
*Mar 16 03:28:50.781: P11:C_GetMechanismInfo slot 1 type 3 (invalid mechanism)
*Mar 16 03:28:50.781: P11:C_GetMechanismInfo slot 1 type 1
*Mar 16 03:28:50.781: P11:C_VerifyRecoverInit - 131118
*Mar 16 03:28:50.781: P11:C_VerifyRecover - 131118
*Mar 16 03:28:50.781: P11:found pubkey in cache using index = 46
*Mar 16 03:28:50.781: P11:public key found is :
30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01
01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01
<snip>
CF 02 03 01 00 01

*Mar 16 03:28:50.788: P11:CEAL:CRYPTO_NO_ERR
*Mar 16 03:28:50.788: P11:C_DestroyObject 2:2002E
*Mar 16 03:28:50.788: CRYPTO_PKI: Expiring peer's cached key with key id 46
*Mar 16 03:28:50.788: CRYPTO_PKI: (A069C) Certificate is verified
*Mar 16 03:28:50.788: CRYPTO_PKI: Remove session revocation service providers
*Mar 16 03:28:50.788: CRYPTO_PKI: Remove session revocation service providersCA-GlobalSign-Root:validat
*Mar 16 03:28:50.788: CRYPTO_PKI: (A069C) Certificate validated without revocation check:cert refcount
*Mar 16 03:28:50.790: CRYPTO_PKI: Populate AAA auth data
*Mar 16 03:28:50.790: CRYPTO_PKI: Unable to get configured attribute for primary AAA list authorization
*Mar 16 03:28:50.790: PKI: Cert key-usage: Digital-Signature , Certificate-Signing , CRL-Signing
*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C)chain cert was anchored to trustpoint CA-GlobalSign-Root, and
*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Removing verify context

*Mar 16 03:28:50.790: CRYPTO_PKI: destroying ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 35, ref
*Mar 16 03:28:50.790: CRYPTO_PKI: ca_req_context released
*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Validation TP is CA-GlobalSign-Root
*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Certificate validation succeeded
*Mar 16 03:28:50.790: CRYPTO_OPSSL: Certificate verification is successful
*Mar 16 03:28:50.790: CRYPTO_PKI: Rcvd request to end PKI session A069C.
*Mar 16 03:28:50.790: CRYPTO_PKI: PKI session A069C has ended. Freeing all resources.:cert refcount aft
*Mar 16 03:28:50.791: <<< ??? [length 0005]
*Mar 16 03:28:50.791: 16 03 03 00 93
*Mar 16 03:28:50.791:
*Mar 16 03:28:50.791: SSL_connect:SSLv3/TLS read server certificate
*Mar 16 03:28:50.791: <<< TLS 1.2 Handshake [length 0093], ServerKeyExchange
*Mar 16 03:28:50.791: 0C 00 00 8F 03 00 17 41 04 3D 49 34 A3 52 D4 EB
*Mar 16 03:28:50.791: DE A2 9E CC B0 91 AA CB 1B 39 D0 26 1B 7D FF 31
*Mar 16 03:28:50.792: E0 D7 D5 9C 75 C0 7D 5B D6 B2 0A B5 CC EA E1 4B
*Mar 16 03:28:50.792: 4E E5 72 7B 54 5D 9B B2 95 91 E0 CC D6 A5 8E CE
*Mar 16 03:28:50.792: 8D 36 C9 83 42 B0 4D AC 0C 04 03 00 46 30 44 02
*Mar 16 03:28:50.792: 20 67 B3 F1 DA D1 BF 13 72 DD B6 B2 11 3B 6E 6F
*Mar 16 03:28:50.793: 87 52 D9 00 F7 44 31 C3 C2 5E BE 2D FF 93 4E F0
*Mar 16 03:28:50.793: A8 02 20 24 42 91 BE B7 10 1C D1 C0 12 28 FB 1F
*Mar 16 03:28:50.793: E4 DE 81 0B AA 66 19 CD 28 5A A0 30 7D 3C 4A 56
*Mar 16 03:28:50.793: 0D 94 E2
*Mar 16 03:28:50.793:
*Mar 16 03:28:50.794: P11:C_FindObjectsInit:
*Mar 16 03:28:50.794: CKA_CLASS: PUBLIC KEY
*Mar 16 03:28:50.794: CKA_KEY_TYPE: : 00 00 00 03

*Mar 16 03:28:50.794: CKA_ECDSA_PARAMS:
30 59 30 13 06 07 2A 86 48 CE 3D 02 01 06 08 2A
86 48 CE 3D 03 01 07 03 42 00 04 63 B6 D3 1A 28
<snip>

*Mar 16 03:28:50.796: P11:C_FindObjectsFinal
```

```
*Mar 16 03:28:50.796: P11:C_VerifyInit - Session found
*Mar 16 03:28:50.796: P11:C_VerifyInit - key id = 131073
*Mar 16 03:28:50.796: P11:C_Verify
*Mar 16 03:28:50.800: P11:CEAL:CRYPTO_NO_ERR
*Mar 16 03:28:50.800: <<< ??? [length 0005]
*Mar 16 03:28:50.800: 16 03 03 00 04
*Mar 16 03:28:50.800:
*Mar 16 03:28:50.800: SSL_connect:SSLv3/TLS read server key exchange
*Mar 16 03:28:50.800: <<< TLS 1.2 Handshake [length 0004], ServerHelloDone
*Mar 16 03:28:50.801: 0E 00 00 00
*Mar 16 03:28:50.801:
*Mar 16 03:28:50.801: SSL_connect:SSLv3/TLS read server done
*Mar 16 03:28:50.810: >>> ??? [length 0005]
*Mar 16 03:28:50.810: 16 03 03 00 46
*Mar 16 03:28:50.811:
*Mar 16 03:28:50.811: >>> TLS 1.2 Handshake [length 0046], ClientKeyExchange
*Mar 16 03:28:50.811: 10 00 00 42 41 04 26 C3 EF 02 05 6C 82 D1 90 B3
*Mar 16 03:28:50.811: 17 31 9A CD DD 8C 81 91 BA E8 C0 86 40 7B 2C E4
*Mar 16 03:28:50.811: 9A 2C 18 9D D1 6A C0 56 A0 98 2E B7 3B AB B3 EB
*Mar 16 03:28:50.811: BB CD 5E 42 C5 76 C0 C4 BF 15 F4 87 F2 7C AD 74
*Mar 16 03:28:50.812: 97 0A 97 2B 06 B5
*Mar 16 03:28:50.812:
*Mar 16 03:28:50.812: SSL_connect:SSLv3/TLS write client key exchange
*Mar 16 03:28:50.812: >>> ??? [length 0005]
*Mar 16 03:28:50.812: 14 03 03 00 01
*Mar 16 03:28:50.812:
*Mar 16 03:28:50.812: >>> TLS 1.2 ChangeCipherSpec [length 0001]
*Mar 16 03:28:51.116: >>> ??? [length 0005]
*Mar 16 03:28:51.116: 17 03 03 00 35
*Mar 16 03:28:51.116:
*Mar 16 03:28:51.116: >>> ??? [length 0005]
*Mar 16 03:28:51.116: 17 03 03 00 1A
*Mar 16 03:28:51.116:
*Mar 16 03:28:51.116: >>> ??? [length 0005]
*Mar 16 03:28:51.116: 17 03 03 00 30
*Mar 16 03:28:51.116:
*Mar 16 03:28:51.116: >>> ??? [length 0005]
*Mar 16 03:28:51.116: 17 03 03 00 1B
*Mar 16 03:28:51.117:
*Mar 16 03:28:51.713: <<< ??? [length 0005]
*Mar 16 03:28:51.713: 17 03 03 00 6D
*Mar 16 03:28:51.713:
*Mar 16 03:28:51.714: >>> ??? [length 0005]
*Mar 16 03:28:51.714: 17 03 03 00 1E
*Mar 16 03:28:51.714:
*Mar 16 03:28:51.732: <<< ??? [length 0005]
*Mar 16 03:28:51.732: 17 03 03 00 71
*Mar 16 03:28:51.732:
```

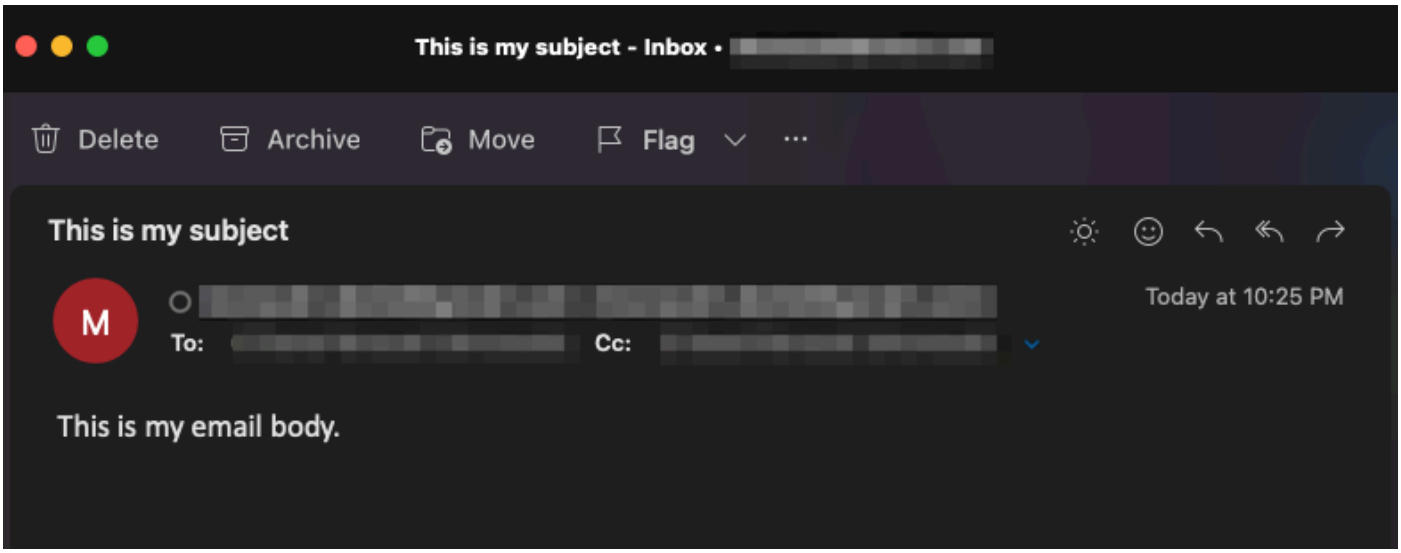
مدير الأحداث يقوم بتشغيل SendSecureEmailEEM*Mar 16 03:28:50.673: crypto_openssl: الذاكرة المخصصة ل OPSSLContext*Mar 1603:28:50.673: crypto_openssl: مجموعة أوامص افات التشفير إلى قناع 0x02FC000 لإصدار 128*Mar 1603:28:50.674: تعيين المنحنى ل EC: 0x70Set قائمة منحنيات EC: secp521r1:secp384r1:prime256v1*mar 16 03:28:50.674: opssl_SetPKIInfo entry*Mar 1603:28:50.674: crypto_PKI: (A069B) بدأت جلسة - الهوية المحددة (TP-ذاتية التوقيع-4865412966x)x TP-Signature-486541296:refcount بعد الزيادة = 1*mar 16 03:28:50.674: crypto_PKI: أبدا الاسترداد المحلي لسلسلة النتائج.*mar 1603:28:50.674: crypto_PKI(cert lookup) المصدر="cn=ios-self-signed-certificate-486541296" الرقم التسلسلي= 01*mar10 3:28:50.674: crypto_pki: البحث عن مؤشر في

المؤشر=7f41e523ce0، digest=1c 7f 3d 52 67 66 d5 59 e2 66 58 e7 8b e7 9b*m 1603:28:50.675: crypto_pki: تم باستخدام سلسلة المرجع المحلي جلب 0.*mar 1603:280 crypto_pki: RCVD طلب إنهاء جلسة PKI A069B.*Mar 16 03:28:50.675: crypto_PKI: PKI جلسة A069B انتهت. تحرير جميع المواردTP-sign-486541296:Unlock TrustPoint TP-SIGNATURE-486541296، refCount وه 0*Mar 1603:28:50.675: opssl_setPKIInfo تم.*Mar 1603:28:50.675: CRYPTO_OPSSL: تم تعطيل المعايير المشتركة في هذه الجلسة.تعطيل وظيفة المعايير العامة في Cisco ssssl L على SSL CTX 0x7F41F28EAFF8*m 16 03:28:50.675: crypto_opssl: ciphersuites ecdhe-rsa-aes256-gcm-sha384:ecdhe-ecdsa-aes256-gcm-sha384:ECDHE-RSA-AES256-HP sha384:dhe-rsa-aes256-gcm-sha384:dhe-rsa-aes256-sha256:AES256-GCM-SHA384:AES256-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-DECDECDECD-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES1288-SHA256:AES128-SHA26 56*سرام 16 03:28:50.676: قبل :قحاصفلا عدب :>>> SSL*سرام 16 03:28:50.676: SSL_connect:قبل تءيئة SSL*سرام 16 03:28:50.676: تءيئة ؟؟؟ [الوطل 005]*سرام 16 03:28:50.676: 16 0301 00 95*سرام 16 03:28:50.676: سرام* 1603:28:50.676: >>> TLS 1.2 قحاصفم [الوطل 0095]، ClientHello*m 1603:28:50.676: 010000910333 6 4B 9F B3 44 94 FD 5F FD A1<snip>*m 16 03:28:50.679: 03 03010201*m 1603:28:50.679: *Mar 1603:28:50.679: SSL_Connect:SSLv3/TLS write hello*Mar 1603:280.6992<: ؟؟؟ [الوطل 005]*سرام 16 03:28:50.692: 16 03 03 00 3F*سرام 1603:28:50.692: سرام* 1603:28:50.692: SSL_connect:SSLv3/TLS اكتب client hello*سرام 1603:28:50.692: <<</TLS 1.2 قحاصفم الي [03F]، الخادم رحاب*m 16:03:28:50.692: 02 000 3b 03 03 64 12 e 05 25 F6 7a bd a0 2e*m 1603:28:50.692: 583 12 F 90 CD f4 AB E2 6953 A8 C7 FC 44 4F*m 1603:28:50.69: 57 4e 47 52 44 01 00 c0 2b 000 13 00 17 000*Mar 16 03:28:50.693: FF 01 001 000 0b 0020010023000*Mar 1603:28:50.693: مداخ دادتما TLS "فورعم ريغ" (id=23)، len=قحلم TLS "TLS" ضافت (id=65281)، len=1*m 16 03:28:50.693: 00*m 1603:28:50.693: مداخ قحلم TLS "تنسيقاتنقطة EC" (id=11)، len=2*m 1603:28:50.693: 010*m 1603:28:50.693: TLS Server Extension Session "Ticket" (id=35)، len=0 16 سرام 3:28:50.693: << ؟؟؟ [الوطل 005]*سرام 16 03:28:50.693: 16 03 030F 9a*سرام 16 03:28:50.694: سرام* 1603:28:50.702: SSL_connect:SSLv3/TLS اقرأ الداخل رحاب*سرام 1603:28:50.702: <<<<</TLS 1.2 قحاصفم الي [0F9A]، شهادة سرام 16 03:28:50.702: 0b 00 0f 96 000f 93 004 8a 30 82 04 86 30 82*mar 16 03:28:50.702: 03 6e a03 02 0102 102 10 52 87 e0 40 A4 FE f7<snip>*m 1603:28:50.73: 82 35 CF 62 8B C9 24 8B A5 B7 39 0c BB 7e 2a 41*m 1603:28:50.763: BF 52 CF FC A2 96 B6 C2 82 3F*Mar 1603:28:50.763: سرام* 1603:28:50.765: CC_DEBUG: الداخل ShiM وظيفة التراجع*Mar 16 03:28:50.765: تم عدب جلسة لمع CRYPTO_PKI: (A069C) - لم متي تحديد الهوية*Mar 1603:28:50.765: crypto_PKI: (A069C) إضافة شهادة النظير*Mar 1603:28:50.767: crypto_PKI: تمت إضافة شهادة نظير X509 - (162)*Bytes6666 03:28:50.767: crypto_PKI: (A069C) إضافة شهادة النظير*MAR 16 03:28:50.768: crypto_PKI: إضافة شهادة نظير x509 - (1434) bytes*mar 1603:28:50.768: crypto_PKI: (A069C) إضافة شهادة النظير*MAR163:280 CRYPTO_PKI: تمت إضافة شهادة نظير x509 - (1382) بايت*MAR 1603:28:50.770: CRYPTO_OPSSL: القحقحة*Mar 1603:28:50.770: CRYPTO_PKI(Cert Lookup) في نم اتصال سلسلة الشهادات المصدر="cn=GTS CA 1C3،o=Google Trust Services LLC،c=US" serial number= 5 87 E0 40 A4 FE F7 07 12 68 B0 4F DD F0 F4*Mar 16 03:28:50.770: CRYPTO_PKI: البحث عن مؤشر=7F41EE523CE0، digest=A7 CC 4B 0F 36 C3 AC D1 2F 77 DD 1D 9A 37 DC FC*Mar63 8:50.770: crypto_PKI(cert lookup) issuer="cn=GTS root R1، o=Google Trust Services LLC، c=US" serial number= 02 03 bc 53 59 6b 34 c7 18 f5 01 50 66*mar 1603:28:50.771: crypto_pki: البحث عن مؤشر=f41ee52ce0، digest=03 9F CF 59 82 EE 09 CC 4F 53 AE D8 02 7E 4B AF*Mar 1603:28:50.771: crypto_PKI(Cert Lookup) issuer="cn=GlobalSign root CA،o=Root CA،o=GlobalSign nv-sa،c=BE" serial number= 77 BD 0D 6D 6D d d 36 F9 1A 21 0F c4 F0 58 D3

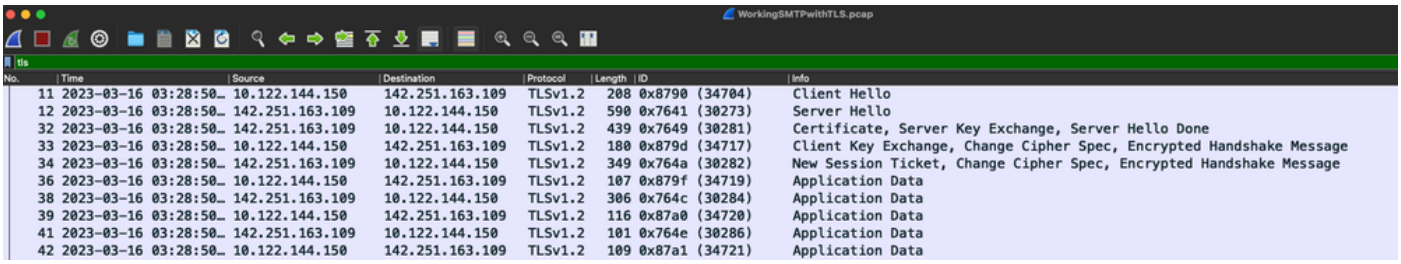
0D*Mar 16 03:28:50.771: crypto_PKI: البحث عن قيمة في المؤشر=7f41e523ce0، digest=940 D1 90 A0 A3 5d 47 E5 B5 31 F6 ad 1B 0A*m 1603:28:50.771: crypto_pki: لم يتم العثور على سجل المنتج الخاص بالمصدر التسلسلي.*Mar 16 03:28:50.772: crypto_PKI: crypto_pki_get_cert_record_by_subject()*Mar 1603:28:50.772: crypto_PKI: Mar 1603:#28:50.772: crypto_PKI: ip-ext-val: لم يتم طلب التحقق من مجال IP:زيادة عدد مرات معرف السياق-35*MAR 16 03:28:50.773: crypto_PKI: إنشاء عون ca_req_context جديد PKI_VERIFY_CHAIN_CONTEXT،ID 35*Mar 1603:28:50.773: crypto_PKI: (A069C)يحتوي مسار التحقق من الصحة على 1 certs*Mar 1603:28:50.773: CRYPTO_PKI: (A069C) فحص certs*Mar 1603:28:50.773: crypto_PKI(cert lookup) issuer="cn=GlobalSign Root CA، ou=root CA، o=GlobalSign nv-sa، c=BE" serial number= 77 BD 0d 6D d DB 36 F9 1A EA 21 0f4 F0 58 D3 0D*Mar 1603:28:50.74 CRYPTO: PKI: البحث عن مؤشر في المؤشر=7F41EE523CE0، المخلص=94 40 D1 90 A3 5D 47 E5 B5 31 F6 63 AD 1B 0a*Mar 16 03:28:50.774: تشفير_PKI: لم يتم العثور على سجل CERT المصدر التسلسل.*Mar 1603:28:50.774: crypto_PKI: (a0: 69C) التحقق من الصحة غير الموثوق به*Mar 1603:28:50.774: CRYPTO_PKI: (A069C) إنشاء قائمة بنقاط الثقة المناسبة*Mar 1603:28:50.774: crypto_PKI: crypto_pki_get_cert_record_by_issuer(*Mar 1603:28:50.774: crypto_PKI_PKI: تم العثور على مطابقة 603:28:50.774: crypto_PKI: (A069C) وجهات الاتصال المناسبة هي: CA-GlobalSign-Root،*Mar 16 03:28:50.775: crypto_PKI: (A069C) استخدام الشهادة باستخدام CA-GlobalSign-root policy*Mar 1603:28:50.775: crypto_PKI: (A60 9C) إستخدام CA-GlobalSign-Root للتحقق من صحة الشهادة*MAR 16:03:28:50.775: crypto_PKI(إنشاء سلسلة ثنائية موثوق بها)*MAR 16:03:28:50.775: crypto_PKI: تمت إضافة 1 شهادة إلى سلسلة موثوق بها.*Mar 1603:28:50.775: crypto_PKI: إعداد مفرخ للإطلاق الجلسات*MAR603:280.77 76: P11:C_CreateObject:*Mar 16 03:28:50.776: CKA_CLASS: المفاتيح العامة*Mar 1603:28:50.776: CKA_KEY_TYPE: RSA*Mar 1603:28:50.776: CKA_Modulus: DA 0E6 998D CE A3:5E3 4F 7E F1 8B 83 25 6B EA 48 1F1 2a b09 95 11 04 BD F0 63 D1 E2 <snip>*m 1603:28:50.780: CKA_PUBLIC_ENT: 01001*m 1603:28:50.780: CKA_VERIFY_RECOVERY: 01*MAR603:28 0.780: crypto_PKI: حذف المفاتيح المخزنة المؤقتة التي يحتوي على مفاتيح معرف 45*mar 16 03:28:50.781: crypto_pki: إزالة مفاتيح النظير العامة في ذاكرة التخزين المؤقت*m 1603:28:50.781: crypto_pki:PEER تم إدخاله بنجاح مع مفاتيح id 46*mar 1603:28:50.781: p11:c_createObject: 13: 118*Mar 16 03:28:50.781: P11:C_GetMechanismInfo slot 1 النوع 3 (آلية غير صالحة)*Mar 16 03:28:50.781: P11:C_GetMechanismInfo slot 1 type 1*Mar 1603:28:50.781: P11:C_VerifyRecoverInit - 13111118*Mar603:8:50.781: P11:C_VerifyRecover - 13118*Mar 16 03:28:50.781: P11:Found Pubkey في ذاكرة التخزين المؤقت باستخدام الفهرس = 46*Mar 16 03:28:50.781: P11:Public key الذي تم العثور عليه وه 30 8201 2230 D 0692A 8686 F7 0D 010151115 00 03 82 01 0F 00 30 82 01 0a2 82 01 01 <snip>cf 0203 001*mar 1603:28:50.788: p11:ceal:crypto_no_err*mar 1603:28:50.788: p1:c_destroyObject 2:2002E*188 603:28:50.788: crypto_PKI: حذف المفاتيح المخزنة المؤقتة التي تم تخزينها بمعرف المفاتيح 46*mar 16 03:28:50.788: crypto_pki: (A069C)*mar 1603:28:50.788: crypto_PKI: إزالة مفرخة الشهادة من التحقق من صحة الجلسات CA-GlobalSign-Root*m 1603:28:50.788: crypto pki: إزالة مفرخة الإطلاق الجلسات CA-GlobalSign-Root:حالة التحقق من صحة الشهادة - crypto_VALID_CERT_WITH_WARNING*Mar 1603:28:50.788: CRYPTO_PKI: (A069C) تم التحقق من صحة الشهادة دون إطلاق:إعادة حساب الصندوق بعد الزيادة = 1*Mar 1603:28:50.790: CRYPTO_PKI: تعيين بيانات المصادقة والتفويض*160:28:50.790: crypto_PKI: تعذر الحصول على سمة تم تكوينها للعميل والمحاسبة و AAA الأساسية.*Mar 16 03:28:50.790: PKI: Cert key-use: Digital-Signature و Certificate-signature و CRL-Signature*Mar 1603:28:50.790: CRYPTO_PKI: (A069C)تم ربط الشهادة بسلسلة TrustPoint CA-GlobalSign-Root وكانت النتيجة: crypto_valid_cert_with_warning*mar 16 03:28:50.790: crypto_pki: (A069C) إزالة التحقق من

السايق*mar 1603:28:50.790: crypto_pki: تدمير ca_req_context type pki_verify_chain_context،ident 35، ref 1:إلغاء الترتيب ل context id-35 إلى*m16:2 8:50.790: crypto_PKI: ca_req_context release*mar 16 03:28:50.790: crypto_pki: (A069C) التحقق من صحة TP وه ca-globalSign-root*Mar 1603:28:50.790: تم التحقق من صحة الشهادة crypto_PKI: (A069C)*Mar 1603:28:50.99 0: crypto_opssl: حجز التحقق من الشهادة*mar 16 03:28:50.790: crypto_pki: rcvd طلب إنهاء جلسة PKI a069c.*mar 16 03:28:50.790: crypto_pki: PKI جلسة A069c انتهت. تحرير جميع المواردإ:.إعادة حساب الرصيد بعد التأكد = 0*مارس 16 03:28:50.791: << ؟؟؟ [الوطل 005]*مارس 16 03:28:50.791: 16 03 00 93*مارس 16 03:28:50.791: *مارس 1603:28:50.791: SSL_connect:SSLv3/TLS قراءة الشهادة المرسلة*مارس 1603:28:50.791: <<</TLS 1.2 قصافحة الديد [الوطل 093]، الخادم يطلب المفاتيح*مارس 16 03:28:50.791: 0C 00 00 8F 03 00 17 41 04 3D 49 34 A3 52 D4 EB*مارس 1603:28:50.791: de A2 9e cc B0 91 aa CB 1b 39 D0 26 1B 7D ff 31*مارس 1603:280.7 92: E0 D7 D5 9C 75 D0 7B 5D6 B2 0A5 CC EA E1 4b*m 16:03:28:50.792: 4e e5 72 7b 54 5d 9b2 95 91 E0 CC D6 A5 8e CE*m 1603:28:50.792: 8d 36 C9 842 B0 D1 ac 0c 04 03 00 46 30 44 02*m 16 03:28:50.792: 20 67 B3 F1 DA D1 BF 13 72 DD B6 B2 11 3B 6e 6F*m 1603:28:50.793: 8752 D9 00 F7 4431 C3 5e e be 2D ff93 E0*مارس 1603:28:50.793: A8 02 20 24 42 91 BE B7 10 1C D1 C0 12 28 FB 1F*مارس 1603:28:50.793: E4 DE 81 0B AA 66 19 CD 285A0 307D 3C 4A 56*Mar 1603:28:50.793: 0D 94 E2*مارس 16 03:28:50.793: *مارس 16 03:28:50.794: P11:C_FindObjectsInit:*مارس 1603:28:50.794: CKA_CLASS: مرام*مع حاتفم 1603:28:50.794: CKA_KEY_TYPE: 0000003*13 603:28:50.794: CKA_ECDSA_PARAMS: 30 59 30 13 06 07 2a 86 48 CE 3d 02 01 06 08 2a 86 48 CE 3d 0301 0703 42004 63 b6 D3 1A 28 <snip>*m 1603:28:50.796: p1:11C FindObjectsFinal*Mar 16 03:28:50.796: P11:C_VerifyInit - جلسة العمل التي تم العثور عليها*Mar 16:03:28:50.796: P11:C_VerifyInit - تعريف المفاتح = 131073*Mar 1603:28:50.796: P11:C_Verify*Mar 1603:280.800.800000003: 11:CEAL:CRYPTO_NO_ERR*MAR 16 03:28:50.800: <<< ؟؟؟ [الوطل 005]*مارس 16 03:28:50.800: 1603 0004*مارس 16 03:28:50.800: *مارس 1603:28:50.800: SSL_connect:SSLv3/TLS قراءة المفاتح الخادم*مارس 1603:28:50.800: <<</TLS 1.2 قصافحة Handshake [004]، رحابDone*Mar 16 03:28:50.801: 0E 00 000*Mar 16 03:28:50.801: *Mar 16 03:28:50.801: SSL_Connect:SSLv3/TLS قراءة الخادم مت*Mar 16 03:28:50.810:> ؟؟ [الوطل 005]*مارس 16 03:28:50.810: 16 03 00 46*مارس 16 03:28:50.811: *مارس 1603:28:50.811: >>> TLS 1.2 قصافحة [الوطل 0046]، ClientKeyExchange*Mar 1603:28:50.811: 1000004441 4 26 C3 EF 02 05 6C 82 D1 90 B3*Mar 16 03:28:50.811: 17 31 9A CD DD 8C 81 91 BA E8 C0 86 40 7B 2C E4*Mar 1603:28:50.811: 9A 2C 189D1 A0 56 A0 98 2E7 B3 B b3 eb*m 1603:28:50.811: BB CD 5e 42 C5 76 C04 BF 15 F4 87 F2 7C ad 74*m 1603:28:50.812: 97 A 97 2B 06 B5*m 1603:28:50.812 مارس* 1603:28:500.812: SSL_connect:SSLv3/TLS تم حفظ بيانات المفاتح العميل*Mar 16 03:28:50.812: >>> ؟؟ [الوطل 005]*مارس 16 03:28:50.812: 14 03 000 1*مارس 16 03:28:50.812: *مارس 1603:28:50.812: >>> TLS 1.2 تغيير CipherSpec [الوطل 0001]*رام 1603:28:51.116:>؟؟؟ [الوطل 005]*مارس 16 03:28:51.116: 17 03 00 35*مارس 16 03:28:51.116: *مارس 1603:28:51.116: >>>> ؟؟؟ [الوطل 0005]*مارس 16 03:28:51.116: 17 03 00 1 أ*مارس 16 03:28:51.116: *مارس 1603:28:51.116: >>>> ؟؟؟ [الوطل 0005]*مارس 16 03:28:51.116: 17 03 00 03:28:51.116: *مارس 1603:28:51.116: >>>> ؟؟؟ [الوطل 0005]*مارس 16 03:28:51.116: 17 03 30*مارس 16 03:51.116:51.28:03:28:51.116: *مارس 1603:28:51.713: << ؟؟؟؟ [الوطل 0005]*مارس 16 03:28:51.117: *مارس 1603:28:51.714: >>>> ؟؟؟ [الوطل 0005]*مارس 16 03:28:51.713: 17 03 00 1b*مارس 16 03:28:51.713: *مارس 1603:28:51.714: << ؟؟؟؟ [الوطل 0005]*مارس 16 03:28:51.714: 17 03 03 00 6d*مارس 16 03:28:51.714: *مارس 1603:28:51.732: << ؟؟؟؟ [الوطل 0005]*مارس 16 03:28:51.732: 17 03 00 71*مارس 16 03:28:51.732:

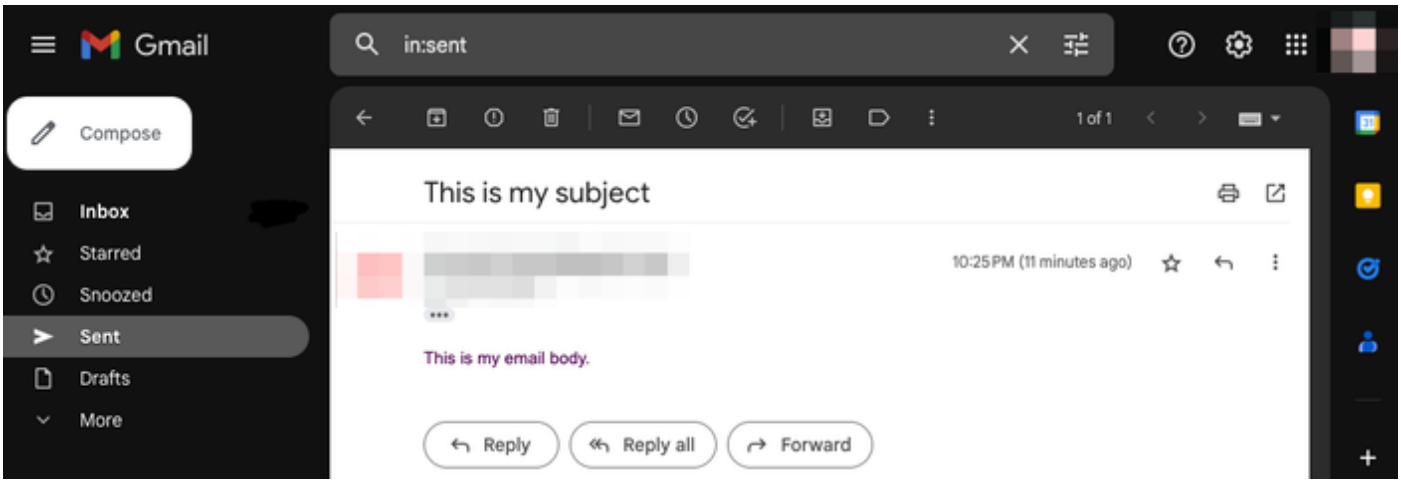
لا يمكنك التحقق من قيود البريد الإلكتروني ومن أن كافة الحقول (إلى، من، نسخة، موضوع، نص) تم تعبئتها بشكل صحيح:



يمكنك أيضا التحقق من حدوث مصافحة TLS والجلسة من التقاط الحزمة على جهاز Cisco IOS XE (المرفق ك "WorkingSMTPwithTLS.pcap"):



يمكنك حتى التحقق من أن رسائل البريد الإلكتروني معكوسة في المجلد "مرسل" لحساب البريد الإلكتروني المستخدم:



المحاذير والاعتبارات الأخرى

أسماء المستخدمين مع رموز @

يمكن رؤية المشاكل عند محاولة إستخدام ترحيل SMTP. بسبب ترحيل SMTP، تحتوي سلسلة الخادم على هذا التنسيق (a@" في اسم المستخدم):

```
event manager environment _email_server email.relay@My.Domain.Name:MyPasswordString@smtp-relay.gmail.com
```

يقسم الرمز لتحليل اسم المستخدم وكلمة المرور السلسلة في أول ظهور للرمز "@". ونتيجة لذلك، يعتقد النظام أن اسم المضيف للخادم يبدأ مباشرة بعد الرمز "@" الأول من "username:password". الخالل باقي السلسلة، ويقوم بترجمة كل شيء قبل ذلك على أنه

يستخدم تنفيذ TCL ل SMTP تعبير عادي (regex) يعالج معلومات اسم المستخدم/كلمة المرور/الخادم هذه بشكل مختلف. بسبب هذا الاختلاف، يسمح TCL بأسماء المستخدمين برمز "@"؛ وعم ذلك، ال يدعم Cisco IOS XE TCL التشفير، لذلك ال يوجد خيار لإرسال رسائل بريد إلكتروني آمنة عبر TLS.

للتلخيص:

- إذا كان البريد الإلكتروني بحاجة إلى تأمين، فال يمكنك إرساله مع TCL.
- في حالة وجود "@" في اسم المستخدم الخاص بك، ال يمكنك إرساله مع IM.

تم تصنيف معرف تصحيح الأخطاء من Cisco CSCwe75439 لمعالجة هذه الفرصة لتحسين ميزة بريد IM الإلكتروني، وعم ذلك، ال توجد خريطة طريق لطلب التحسين هذا حاليا.

القرار

كما هو موضح هنا، من الممكن إرسال رسائل بريد إلكتروني آمنة عبر بروتوكول SMTP باستخدام نظام TLS باستخدام التطبيق الصغير المدمج لإدارة الأحداث (EEM). ويتطلب ذلك بعض الإعداد على جانب الخادم، بالإضافة إلى تكوين الشهادات اللازمة للسماح بالثقة، ولكنه ممكن إذا كنت تريد إنشاء إعالمات بريد إلكتروني موثوقة وآمنة.

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).