

利用EEM自動向使用者傳送安全電子郵件

目錄

[簡介](#)

[使用案例](#)

[背景](#)

[Gmail帳戶設定](#)

[基本EEM配置](#)

[僅安裝預設證書時出現問題](#)

[用於保護SMTP安全的證書](#)

[查詢證書的更簡單方法](#)

[再次使用安全SMTP測試EEM](#)

[其他注意事項和注意事項](#)

[具有@符號的使用者名稱](#)

[結論](#)

簡介

本檔案介紹在Cisco IOS® XE內嵌式事件管理員(EEM)中使用「郵件伺服器」動作，以使用連線埠587上的傳輸層安全性(TLS)將安全電子郵件傳送至簡單郵件傳輸通訊協定(SMTP)伺服器所需的程式。

在此過程中，您可能會遇到許多警告，因此撰寫本文的目的是記錄完成此任務所需的步驟。

使用案例

許多客戶認為，在某個事件發生後自動接收電子郵件通知很有價值。EEM子系統是網路事件檢測和板載自動化的強大工具，它提供了一種在Cisco IOS XE裝置上自動傳送電子郵件通知的有效方法。例如，您可能想要監控IPSLA跟蹤，並響應指示狀態更改的系統日誌，採取某種操作並透過電子郵件向網路管理員發出事件警報。此「電子郵件通知」的想法可以套用至許多其他案例，以吸引您對想要標示的任何特定事件的注意。

背景

PEM代表「隱私增強型郵件」，是一種通常用於表示證書和金鑰的格式。這是Cisco IOS XE裝置使用的證書格式。安全應用程式（如HTTPS或安全SMTP）通常具有「堆疊PEM」，其中涉及多個證書，包括：

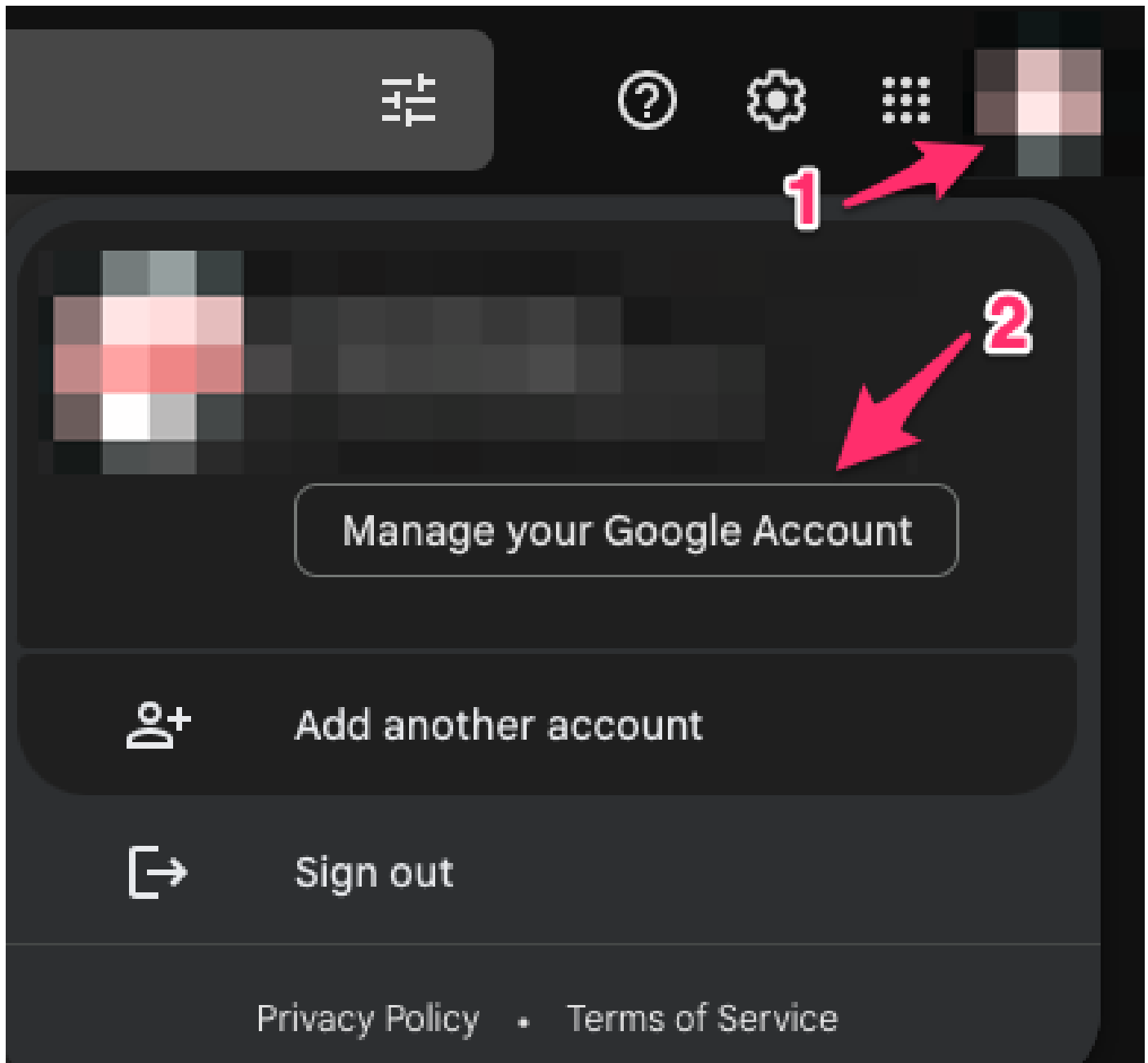
- 根證書
- 簽署（中間）憑證
- 一般使用者（或伺服器）憑證

Gmail帳戶設定

本文以Google的SMTP服務為例。 前提條件是您之前設定了Gmail帳戶。

谷歌允許您從遠端客戶端向Gmail傳送電子郵件。 在Gmail中，以前有一個用於「不安全的應用」的設定，如果不允許在Google端使用此設定，該應用將面臨錯誤。 該設定已刪除，取而代之的是「安全應用程式」選項。可透過以下方式訪問：

mail.google.com > 按一下您的設定檔(#1) > 管理您的Google帳戶(#2) > 安全性(#3) > 如何登入Google > 2步驟驗證(#4)



- Home
- Personal info
- Data & privacy
- Security**
- People & sharing
- Payments & subscriptions
- About

Security

Settings and recommendations to help you keep your account secure

You have security tips

Security tips found in the Security Checkup



[Review security tips](#)

Recent security activity

New sign-in on Mac

3:55 PM



[Review security activity](#)

How you sign in to Google

Make sure you can always access your Google Account by keeping this information up to date

2-Step Verification



On since Jul 20, [blurred]



在此頁面上，確保「兩步驗證」處於打開狀態。

← 2-Step Verification

2-Step Verification is ON since Jul 20, [blurred]

然後，您可以向下滾動到「應用密碼」，讓Gmail生成一個密碼，該密碼可用於從不支援兩步驗證的應用程式登入到您的Google帳戶。

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

← 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](#)

Your app passwords

Name	Created	Last used
------	---------	-----------

MyRouter	4:03 PM	-
----------	---------	---



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

Select app

Select device

GENERATE

Generated app password

Your app password for your device



How to use it

Go to the settings for your Google Account in the application or device you are trying to set up. Replace your password with the 16-character password shown above. Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.

DONE

此螢幕截圖中的16個字元的應用程式密碼被模糊了，因為它與一個個人Gmail帳戶相關聯。

現在您已經有Gmail的應用程式密碼，您可以將此密碼與Gmail帳戶名稱一起使用來作為電子郵件伺

伺服器來轉寄電子郵件。 指定伺服器的格式為「username : password@host」。

基本EEM配置

有許多方法可以自定義EEM指令碼以滿足您的確切需求，但此示例是一個基本EEM指令碼，用於使安全電子郵件功能運行：

```
(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 "$_email_from" cc "$_
```

配置首先建立三個EEM環境變數：_email_from、_email_to和_email_server。 每個變數都定義在一個變數中，以便更輕鬆地更改配置。 然後建立SendSecureEmailEEM指令碼。 此處的觸發事件為「無」，以便您可以使用「#事件管理器運行SendSecureEmailEEM」（而不是等待特定事件觸發）隨時手動運行EEM指令碼。 接下來，您只需執行一個「郵件伺服器」操作即可生成電子郵件。「安全tls」和「埠587」選項告知裝置在埠587上協商TLS，Gmail伺服器將偵聽該埠。

您還需要確保「從」欄位有效。 如果您認證為「Alice」，但嘗試從「Bob」傳送電子郵件，則由於Alice欺騙了其他人的電子郵件地址，該郵件將出錯。「寄件者」欄位必須與伺服器上用來傳送電子郵件的帳戶一致。

僅安裝預設證書時出現問題

EEM利用openssl與SMTP伺服器建立連線。 為了安全通訊，伺服器會將憑證傳回到Cisco IOSd中執行的openssl。 然後，IOSd將查詢與該證書關聯的信任點。

在Cisco IOS XE裝置上，預設情況下不安裝Gmail SMTP伺服器的證書。 必須手動匯入它們才能建立信任。 如果沒有安裝證書，TLS握手將由於「證書錯誤」而失敗。

這些調試對於調試任何證書問題都非常有用：

```
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
```

您可以在路由器上啟動嵌入式資料包捕獲(EPC)，在EEM觸發時捕獲電子郵件伺服器之間的任何流量：

```
! 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
```

最後，openssl無法與SMTP伺服器建立安全TLS會話，因此會拋出「證書錯誤」錯誤，導致EEM停止運行：

```
*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
```

從此交換中記錄的資料包捕獲附加為「NoCertificateInstalled.pcap」。從路由器(10.122.x.x)到Gmail SMTP伺服器(142.251.163.xx)的最終TLS資料包顯示TLS協商已終止，原因是與之前調試中看到的一致「證書錯誤」消息。


```
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)
```

用於保護SMTP安全的證書

由於缺少允許Cisco IOS XE裝置信任Gmail伺服器的證書，因此解決方法是將這些證書中的一個/所有安裝在裝置上的信任點中。

例如，上一個測試的完整調試顯示發生的這些證書查詢：

```
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=
```

需要在信任點下為每台發行者安裝證書，以便裝置可以與Gmail SMTP伺服器建立安全會話。 可以使用以下配置為每個頒發者建立信任點：

```
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
```

您現在已針對每個頒發者設定了一個信任點；但是，目前尚無與其相關聯的實際證書。它們基本上是空白的信任點：

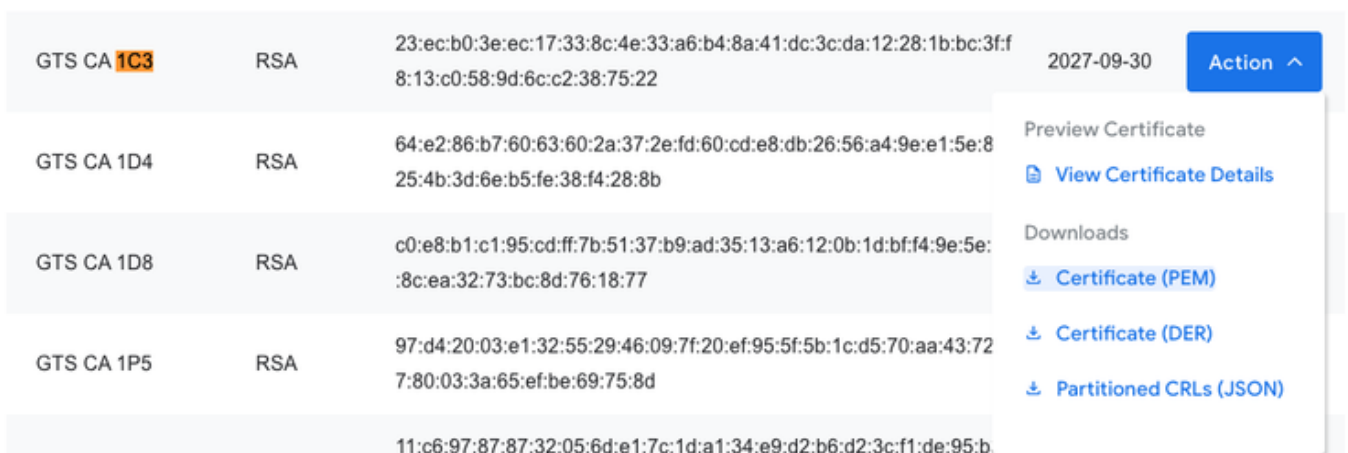
```
# show run | sec crypto pki certificate chain CA-  
crypto pki certificate chain CA-GTS-1C3  
crypto pki certificate chain CA-GTS-Root-R1  
crypto pki certificate chain CA-GlobalSign-Root  
crypto pki certificate chain CA-gmail-SMTP
```

您必須追蹤這些憑證的位置，然後將它們安裝在裝置上。

在網上搜尋「Google Trust Services 1C3」，我們很快就能找到Google Trust Services證書儲存庫：

<https://pki.goog/repository/>

展開該頁面上的所有證書後，您可以搜尋查詢「1C3」，點選「操作」下拉選單，然後下載PEM證書：



CA Name	Key Type	Serial Number	Expiration Date	Action
GTS CA 1C3	RSA	23:ec:b0:3e:ec:17:33:8c:4e:33:a6:b4:8a:41:dc:3c:da:12:28:1b:bc:3f:8:13:c0:58:9d:6c:c2:38:75:22	2027-09-30	Action ^
GTS CA 1D4	RSA	64:e2:86:b7:60:63:60:2a:37:2e:fd:60:cd:e8:db:26:56:a4:9e:e1:5e:825:4b:3d:6e:b5:fe:38:f4:28:8b		Preview Certificate View Certificate Details
GTS CA 1D8	RSA	c0:e8:b1:c1:95:cd:ff:7b:51:37:b9:ad:35:13:a6:12:0b:1d:bf:f4:9e:5e:8c:ea:32:73:bc:8d:76:18:77		Downloads Certificate (PEM) Certificate (DER) Partitioned CRLs (JSON)
GTS CA 1P5	RSA	97:d4:20:03:e1:32:55:29:46:09:7f:20:ef:95:5f:5b:1c:d5:70:aa:43:727:80:03:3a:65:ef:be:69:75:8d		
		11:c6:97:87:87:32:05:6d:e1:7c:1d:a1:34:e9:d2:b6:d2:3c:f1:de:95:b		

使用文本編輯器打開下載的PEM檔案會顯示，這只是一個證書，可以在您之前建立的信任點下導入到Cisco IOS XE裝置：

```
-----BEGIN CERTIFICATE-----  
MIIF1jCCA36gAwIBAgINAgO8U11rNMcy9QFQZjANBgkqhkiG9w0BAQsFADBHMQsw  
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2x1IFRydXN0IFN1cnZpY2VzIEExMQzEU  
<snip>  
AJ2xDx8hcFH1mt0G/FX0Kw4zd8NLQsLxdxP8c4CU6x+7Nz/OAipmsHMdMqUybDKw  
juDEI/9bfU11cKwrmz302+BtjKAvpafkm0817tdufThcV4q508DIrGKZTqPwJN1  
1IXNDw9bg1kWRxYtnCQ6yICmJhSFm/Y3m6xv+cXDB1Hz4n/FsRC6UfTd  
-----END CERTIFICATE-----
```

您可以在「CA-GTS-1C3」信任點下使用配置命令導入它：

```
(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

```
MIIFljCCA36gAwIBAgINAg08U1lrNmCY9QFQZjANBgkqhkiG9w0BAQsFADBHMQsw  
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2x1IFRydXN0IFN1cnZpY2VzIExMQzEU  
<snip>  
juDEI/9bfU1lcKwrmz302+BtjjKAvpafkm08l7tdufThcV4q508DIrGKZTqPwJN1  
1IXNDw9bg1kWRxYtnCQ6yICmJhSFm/Y3m6xv+cXDB1Hz4n/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)#
```

然後您可以確認已安裝了憑證：

```
# 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 B110BA51 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 ECBOE38D 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
```

接著，您可以為其他兩個發行者安裝憑證。

CA-GTS-Root-R1 :

組態:

[擾流器](#) (反白顯示以讀取)

```
(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

MIIFVzCAAz+gAwIBAgINAgP1k28xsBNJiGuiFzANBgkqhkiG9w0BAQwFADBHMQsw
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2x1IFRydXN0IFN1cnZpY2VzIEExMQZEU
<snip>
2tIMPNUzjSmhDYAPexZ3FL//2wmUsp08IFgV6dtxQ/PeEMMA3Kgq1bbC1j+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-R1輸入base 64編碼的CA證書。以空白行或單詞「quit」結束，單單行為
MIIFVzCCAz+gAwIBAgINAgPlk28xsBNJiGuiFzANBgkqhkiG9w0BAQwFADBHMQswCQYDVQQQQQGEVzEiMCAGA1UEChMZR29vZ2xiIFRydXN0IFNlcnZpY2VzIExMQzEU<snip>2tIMPuzjsmhDYAPexZ3FL//2wbbbP6MvPJwNQzcmRk13NfIRmPVNnGuV/u3gm3cCertificate具有以下屬性：指紋MD5：
05FED0BF 71A8A376 63DA01E0 D852DC40指紋SHA1： E58C1CC4 913B3863 4BE9106E
E3AD8E6B 9DD9814A%您接受此證書嗎？[yes/no]： yesTrustpoint CA證書已接受。% Certificate
successfully imported(config)# end
```

運行配置驗證：

[擾流器](#) (反白顯示以讀取)

```
# 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
```

```
# show run | sec crypto pki certificate chain CA-GTS-Root-R1crypto pki certificate chain CA-GTS-
Root-R1 certificate ca 0203E5936F31B01349886BA217 30820557 3082033F A0030201
02020D02 03E5936F 31B01349 886BA217 300D0609 2A864886 F7 d0101 0C050030 47310B30
09060355 04061302 55533122 30200603 <snip> 6775C119 3A2B474E D3428EFD 31C81666
DAD20C3C DBB38EC9 A10D800F 7B167714 BFFFDB09 94B293BC 205815E9 DB7 143F3
DE10C300 DCA82A95 B6C2D63F 906B76DB 6CFE8CBC F270350C DC991935 DCD7C846
63D53671 AE57FBB7 826DDC結束
```

顯示加密驗證：

[擾流器](#) (反白顯示以讀取)

```
# 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
```

```
# show crypto pki certificates verbose CA-GTS-Root-R1CA證書狀態：可用版本：3證書序列號
（十六進位制格式）：0203E5936F31B01349886BA217證書使用情況：簽名頒發者：cn=GTS根
R1 o=Google Trust Services LLC c=US主題：cn=GTS根R1 o=Google Trust Services LLC
c=US有效日期：日期：00:00:00 UTC 6月22日2016年結束日期：00:00:00 UTC 6月22日2036主題
金鑰資訊：公鑰演算法：rsaEncryption RSA公鑰：（4096位）簽名演算法：帶RSA加密指紋的
SHA384 MD5：05FED0BF 71A8A376 6 63DA01E0 852DC40指紋SHA1：E58C1CC4 913B3863
4BE9106E E3AD8E6B 9DD9814A X509v3擴展：X509v3金鑰用法：86000000數位簽章金鑰證書
簽名CRL簽名X509v3主題金鑰ID：E4AF2B 26 711A2B48 27852F52 662CEFF0 8913713E
X509v3基本限制：CA：TRUE Authority資訊訪問：證書安裝時間：14:39:38 UTC Mar 13
2023證書安裝時間（以秒為單位）：1678718378546968064關聯信任點：CA-GTS-Root-R1
Trustpool
```

CA-GlobalSign-Root :

在此位置找到此證書：

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

組態:

[擾流器](#) (反白顯示以讀取)

```
(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

```
MIIDdTCCA12gAwIBAgILBAAAAAABFUtaW5QwDQYJKoZIhvcNAQEFBQAwVzELMAKGA1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
<snip>
DKqC5J1R3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbME
HMUfpIBvFSDJ3gyICh3WZ1Xi/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-Root輸入base 64編碼的CA證書。以空白行或單詞「quit」結束，在行上單獨使用

```
MIIDdTCCAII2gAwIBAgILBAAAAAABFUtaW5QwDQYJKoZIhvcNAQEFBQAwwVzELMAkGA1UEBhMCQk
gNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv<snip>DKqC5JIR3XC321Y9YeRq4VzW9
MEHMUfpIBvFSDJ3gyICh3WZIXi/EjKJSZp4A==證書具有以下屬性：指紋MD5：3E455215
095192E1 B75D33 79F B187298A指紋SHA1：B1BC968B D4F49D62 2AA89A81 F2150152
A41D829C%您接受此證書嗎？[yes/no]：yesTrustpoint CA證書已接受。% Certificate successfully
imported(config)# end
```

運行配置驗證：

[擾流器](#) (反白顯示以讀取)

```
# 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
```

```
# show run | sec crypto pki certificate chain CA-GlobalSign-Rootcrypto pki certificate chain CA-
GlobalSign-Root certificate ca 040000000001154B5AC394 30820375 3082025D A0030201
02020B04 00000000 01154B5A C394300D 06092A86 <snip> 2AC45631 95D06789 852BF96C
A65D469D 0CAA82E4 951DD 70 B7DB563D 61E46AE1 5CD6F6FE 3DDE41CC 07AE6352
BF5353F4 2BE9C7FD B6F7825F 85D24118 DB81B304 1CC51FA4 806F1520 9DE0C88
0A1DD666 55E2FC48 C9292669 E0結束
```

顯示加密驗證：

[擾流器](#) (反白顯示以讀取)

```
#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 certificates verbose CA-GlobalSign-RootCA CertificateStatus :
AvailableVersion : 3Certificate Serial Number (hex) : 040000000001154B5AC394證書用法 :
SignatureIssuer : cn=GlobalSign Root CAou=Root CAo=GlobalSign nv-sac=BEsubject :
cn=GlobalSign Root CAou=Root CAo=GlobalSign日期 : 開始日期 : 12 00:00 UTC Sep 1998結束
日期 : 12:00:00 UTC Jan 28 2028主題金鑰資訊 : 公鑰演算法 : rsaEncryptionRSA公鑰
: ( 2048位 ) 簽名演算法 : 帶RSA加密的SHA1指紋MD5 : 3E455215 095192E1 B75D379F
B187298A指紋SHA1 : B1BC96 8B D4F49D62 2AA89A81 F2150152 A41D829C X509v3擴展
: X509v3金鑰用法 : 6000000金鑰證書簽名CRL簽名X509v3主題金鑰ID : 607B661A 450D97CA
89502F7D 04CD3 A8 FFFCFD4B X509v3基本限制 : CA : TRUEAauthority資訊訪問 : 證書安裝時
間 : 03:03:01 UTC Mar 16 2023證書安裝時間 ( 以秒為單位 ) : 1678935781942944000關聯信任
點 : CA-GlobalSign-Root
```

CA-gmail-SMTP :

Gmail伺服器(CA-gmail-SMTP)的TLS憑證是依照以下說明步驟找到的 : [使用TLS憑證進行安全傳輸](#)

組態:

[擾流器](#) (反白顯示以讀取)

```
(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
```

```
MIIEnhjCCA26gAwIBAgIQUofgQKT+9wcSaLBP3d3w9DANBgkqhkiG9w0BAQsFADBG
MQswCQYDVQQGEWVUzEiMCAGA1UEChMZRR29vZ29udGVzZ2x1IFRydXN0IFN1cnZpY2VzIEExM
```



```
<snip>
b1J2gZAyjd4nfFRG1jeL5KrsfUR9hIXufqySv1PUoPuKSi3fvsIS21BYEXEe8uZ
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-SMTP輸入base64編碼的CA證書。以空白行或單詞「quit」結束

```
MIIEhJCCA26gAwIBAgIQUofgQKT+9wcSaLBP3d3w9DANBgkqhkiG9w0BAQsFADBGMQswCQYDVQQQ
zgBxJaeTUjncvow==信任點「CA-gmail-SMTP」是下級CA。但證書不是CA證書。需要手動驗證證書具有以下屬性：指紋MD5：19651FBE 906A414D 6D 57B783 946F30A2指紋SHA1：
4EF392CB EEB46D5E 47433953 AAEF313F 4C6D2825%您接受此證書嗎？[yes/no]：
yesTrustpoint CA證書已接受。%證書已成功導入(config)#
```

運行配置驗證：

[擾流器](#) (反白顯示以讀取)

```
# 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
```

```
# 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 310B 3009 06035504 06130255 <snip> 92ABB1F5 11F53312230 B9FAB24A
F94F5283 EE2928B7 7EFB084B 6D61217 416045 C47BCB99 801C4969 E4D48E77 2FA3結束
```

顯示加密驗證：

[擾流器](#) (反白顯示以讀取)

```
# 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

show crypto pki certificates verbose CA-gmail-SMTPCA CertificateStatus : AvailableVersion :
3Certificate Serial Number (hex) : 5287E040A4FEF7071268B04FDDDDF0F4證書用法 :
SignatureIssuer : cn=GTS CA 1C3o=Google Trust Services LLCc=USSsubject :
cn=smtp.gmail.comCRL分發點 : http://crls.pki.goog/gts1c3/moVDfISia2k.crlValidity日期 : 開始日
期 : 09 15:03 UTC 2023年2月20日結束日期 : 09:15:02 UTC 2023年5月15日主題金鑰資訊 : 公鑰
演算法 : ecEncryptionEC公鑰 : (256位) 簽名演算法 : 帶RSA加密的SHA256指紋MD5 :
19651FBE 906A414D 6D57B783 946F3 0A2指紋SHA1:4EF392CB EEB46D5E 47433953
AAEF313F 4C6D2825 X509v3擴展 : X509v3金鑰用法 : 80000000數位簽章X509v3主題金鑰
ID : 5CC36972 D07FE997 510E1A67 8A ECC 23 E40CFB68 X509v3基本限制
: CA : FALSEX509v3主題替代名稱 : smtp.gmail.com IP地址 : 其他名稱 : X509v3授權機構金鑰
ID : 8A747FAF 85CDEE95 CD3D9CD0 E24614F3 71351D27授權資訊訪問 : OCSP
URL : http://ocsp.pki.goog/gts1c3CA頒發者 : http://pki.goog/repo/certs/gts1c3.derX509v3證書策
略 : 策略 : 2.23.140.1.2.1擴展金鑰用法 : 伺服器AuthCert安裝時間 : 03:10:41 UTC Mar 16 2023證
書安裝時間 (以nsec為單位) : 1678936241822955008關聯信任點 : CA-gmail-SMTP

查詢證書的更簡單方法

或者，您也可以嘗試使用伺服器/筆記型電腦的openssl呼叫，以簡化方式從SMTP伺服器取得憑證，而不必使用偵錯並搜尋Google來追蹤憑證：

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

您也可訪問use smtp.gmail.com：

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

該呼叫的輸出將包括可用於「crypto pki authenticate <trustpoint>」配置的實際證書本身。

再次使用安全SMTP測試EEM

現在，證書已應用到Cisco IOS XE裝置，EEM指令碼將按預期傳送安全SMTP消息。

```
# event manager run SendSecureEmailEEM
```

檢查Spoiler以瞭解完整加密和ssl調試輸出：

[擾流器](#) (反白顯示以讀取)

```
# 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:pr
*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" s

*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 FO
*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:

486541296 #事件管理器運行SendSecureEmailEEM*Mar 16 03:28:50.673 :

CRYPTO_OPSSL : 為OPSSLContext*Mar 16 03:28:50.673 : CRYPTO_OPSSL : 為版本128*設定加密規範到掩碼0x02FC00000Mar 16 03:28:50.674 : 設定預設EC曲線清單 : 0X70設定EC曲線清單 : secp521r1 : secp384r1 : prime256v1*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-self -486541296 : 增量後的重新計數= 1*Mar 16 03:28:50.674 : CRYPTO_PKI : 開始本地證書鏈檢索。*Mar 16 03:28:50.674 : CRYPTO_PKI (證書查詢) issuer="cn=IOS-Self-Signed-Certificate-486541296" serial number= 01*Mar 16 03:28:50.674 : CRYPTO_PKI : 查詢控制代碼=7F 1EE523CE0 , 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 : 完成本地證書鏈獲取0.*Mar 16 03:28:50.675 : CRYPTO_PKI : 結束PKI會話9A066 B.*Mar 16 03:28:50.675 : CRYPTO_PKI : PKI會話A069B已結束。釋放所有資源。TP-self-signed-486541296 : unlocked trustpoint TP-self-signed-486541296 , refcount為0*Mar 16 03:28:50.675 : opssl_SetPKIInfo done.*Mar 16 03:28:50.675 : CRYPTO_OPSSL : 在此會話中停用通用標準。在SSL上停用CiscoSSL中的通用標準模式功能CTX 0F41F28EAF8 3月16日03:28:50.675 : CRYPTO_OPSSL : 密碼套件ECDHE-RSA-AES256-GCM-SHA384 : ECDHE-ECDSA-AES256-GCM-SHA384 : ECDHE-RSA-AES256-GCM-SHA384 : DHE-RSA-AES256-SHA256 : AES256-GCM-SHA384 : AES256-SHA256 : ECDHE-RSA-AES128-GCM-SHA256 : ECDHE-ECDSA-AES128-GCM-SHA256 : ECHE RSA-AES128-SHA256 : DHE-RSA-AES128-GCM-SHA256 : DHE-RSA-AES128-SHA256 : AES128-GCM-SHA256 : AES128-SHA256*Mar 16 03:28:50.676 : 握手開始 : 在SSL初始化之前*3月16日03:28:50.676 : SSL_connect : 在SSL初始化之前*3月16日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握手[length 0095] , ClientHello*Mar 16 03:28:50.676 : 0000 1 03 03 26 4B 9F B3 44 94 FD 5F FD A1<截圖>*3月16日03:28:50.679:03 03 01 02 01*3月16日0 3:28:50.679 : *Mar 16 03:28:50.679 : SSL_connect : SSLv3/TLS寫入客戶端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寫入客戶端hello*Mar 16 03:28:50.692 : << TLS 1.2握手[length 003 f] , 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 10

3:28:50.692 : 57 4E 47 52 44 01 00 C0 2B 00 00 13 00 17 00 00*3月16 03:28:50.693 : FF 01 00 00 00 0B 00 02 01 00 00 23 00 00*3月16 03:28:50.693 : 伺服器擴展 「unknown」
(id=23) , len=0TLS伺服器擴展 「renegotiate」 (id=65281) , len=1*Mar 16 03:28:50.693 : 00*Mar 16 03:28:50.693 : TLS伺服器擴展 「EC點格式」 (id=11) , len=2*Mar 16 03:28:50.693 : 01 00*Mar 16 03:28:50.693 : TLS伺服器擴展 「會話票證」 (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讀取伺服器hello*Mar 16 03:28:50.702 : << TLS 1.2握手[length9F00] , 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 10 52 87 E0 40 A4 FE F7<snip>*Mar 16 3:28:50.763 : 82 35 CF 62 8B C9 24 8B A5 B7 39 0C BB 7E 2A 41*3月16日03:28:50.763 : BF 52 CF FC A2 96 B6 C2 82 3F*Mar 16 03:28:50.763 : *3月16 03:28:28:28:50 765 : CC_DEBUG : 正在進入shim層應用程式回撥函式*Mar 16 03:28:50.765 : CRYPTO_PKI : (A069C)會話已啟動-未指定身份*Mar 16 03:28:50.765 : CRYPTO_PKI : (A069C)增加對等證書 *Mar 16 03:28:50.767 : CRYPTO_PKI : 已增加x 509對等證書- (1162)位元組*3月16日 03:28:50.767 : CRYPTO_PKI : (A069C)增加對等證書*3月16日03:28:50.768 : CRYPTO_PKI : 增加的x509對等證書- (1434)位元組*3月16日03:28:50.768 : CRYPTO_PKI : (A069C)增加對等證書*Mar 16 03:28:50.770 : CRYPTO_PKI : 增加的x509對等證書- (1382)位元組 *Mar 16 03:28:50.770 : CRYPTO_OPSSL : 驗證證書鏈回撥*Mar 16 03:28:50.770 : CRYPTO_PKI (證書查詢頒發者) ="cn=GTS 1CA C3 , o=Google Trust Services LLC , c=US" serial number= 52 87 E0 40 A4 FE F7 07 12 68 B0 4F DD F0 F4*Mar 16 03:28:50.770 : CRYPTO_PKI : 查詢控制代碼中的證書=7F41EE523CE0 , digest=A7 CC 4B 0F36 C3 AC 1 2F 77 DD 1D 9A 37 DC FC*Mar 16 03:28:50.770 : CRYPTO_PKI (證書查詢) 頒發者="cn=GTS根R1 , o=Google Trust Services LLC , c=US"序列號= 02 03 BC 53 59 6B 34 C7 18 F5 01 50 66*Mar 16 03:28:50.771 : CRYPTO_PKI : 正在查詢控制代碼中的證書 =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 (證書查詢) issuer="cn=GlobalSign Root CA , ou=Root CA , o=Global sign nv-sa , c=BE" serial number= 77 BD 0D 6C DB 36 F9 1A EA 21 0F C4 F0 58 D3 0D*Mar 16 03:28:50.771 : CRYPTO_PKI : 查詢控制代碼=7F41EE523CE0 , digest=94 40 D1 90 A0 35D 47 E5 B5 31 6 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 : 50.50 772 : CRYPTO_PKI : ip-ext-val : IP extension validation not required : Increasing refcount for context id-35 to 1*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 validation mar has 1 certs 16 03:28:50.773 : CRYPTO_PKI : (A069C)檢查相同的證書*Mar 16 03:28:50.773 : CRYPTO_PKI (證書查詢) issuer="cn=GlobalSign Root CA , ou=Root CA , o=GlobalSign-sa , c=BE"序列號= 77 BD 0D 6C DB 36 F9 1A EA 2 1 0F C4 F0 58 D3 0D*Mar 16 03:28:50.774 : CRYPTO_PKI : 尋找控制代碼中的證書=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 : 未找到頒發者串列裝置的證書記錄 。 *Mar 16 03:28:50.774 : CRYPTO_PKI : (A069C)正在驗證不受信任的證書*Mar 16 03:28:50.774 : CRYPTO_PKI : (A069C)建立合適的信任點清單*Mar 16 03:28:50.774 : CRYPTO_PKI : crypto_get_get_cert_record_by_issuer()*Mar 16 03:28:50.774 : CRYPTO_PKI : 發現頒發者匹配*Mar 16 03:28:50.774 : CRYPTO_PKI : (A069C)合適的信任點包括 : CA-GlobalSign-Root , *Mar 16 03:28:50.775 : CRYPTO_PKI : (A069C)嘗試驗證證書使用 CA-GlobalSign-Root策略*Mar 16 03:28:50.775 : CRYPTO_PKI : (A069C)使用CA-GlobalSign-Root驗證證書*Mar 16 03:28:50.775 : CRYPTO_PKI (建立受信任的證書鏈) *Mar 16

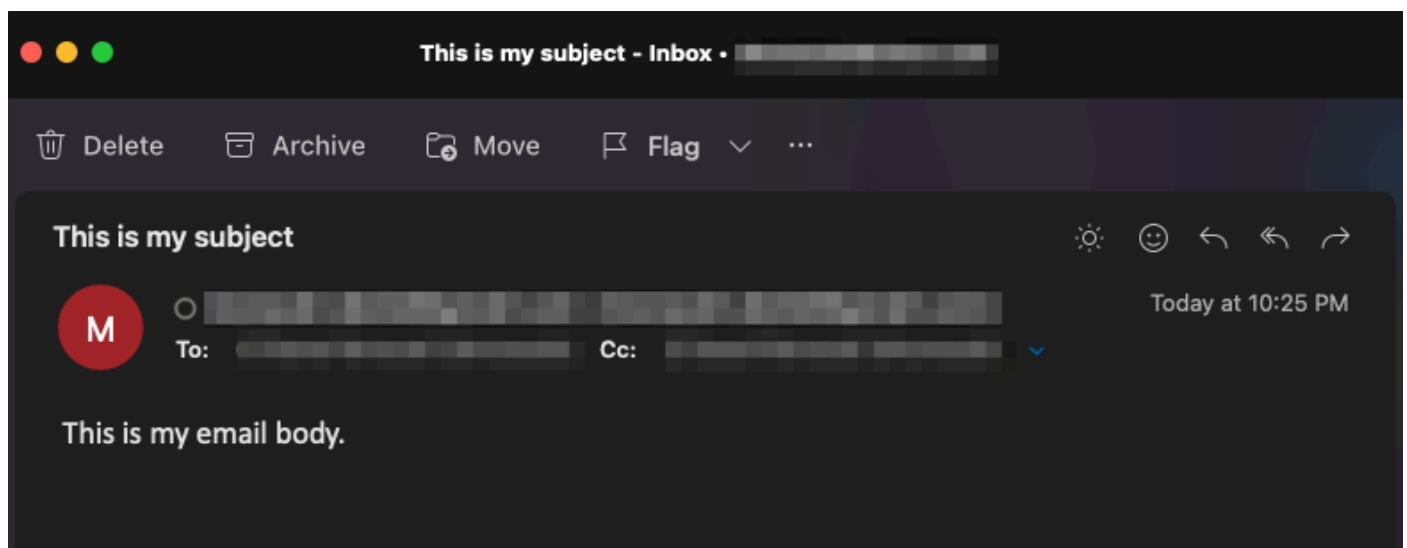
03:28:50.775 : CRYPTO_PKI : 1個證書增加到受信任的證書鏈。 16 03:28:50.775 :
CRYPTO_PKI : 準備會話撤銷服務提供商*3月16 03:28:50.776 : P11 : C_CreateObject : *Mar 16
03:28:50.776 : CKA_CLASS : PUBLIC KEY*Mar 16 03:28:50.776 : CKA_KEY_TYPE :
RSA*Mar 6 03:28:50.776 : CKA模數 : DA 0E E6 99 8D CE A3 E3 4F 8A 7E FB F1 8B 83 25 6B
EA 48 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 : 刪除具有金鑰ID的快取金鑰45*Mar 16 03:28:50.781 :
CRYPTO_PKI : 嘗試將對等體的公鑰插入到快取中*Mar 16 03:28:50.781 : CRYPTO_PKI : 成功插
入對等體的公用，金鑰id為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 : P1 : P1 : P1 : P1 : C_Get1 info slot 1型別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 : 在快取中使用索引找到公鑰= 46*Mar 16 03:28:50.781 : P 1 : 找到的公
鑰是 : 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 : 金鑰ID為46*Mar 16 03:28:50.788 : CRYPTO_PKI : (A069C)證
書已驗證*3月16日03:28:50.788 : CRYPTO_PKI : 刪除會話撤銷服務提供商*3月16日
03:28:50.788 : CRYPTO_PKI : 刪除會話撤銷服務提供商CA-GlobalSign-Root : validation status -
CRYPTO_VALID_CERT_WITH_WARNING*Mar 16 03:28:50.788 : CRYPTO_PKI : (A069C))未
經撤銷檢查而驗證的證書 : 增量後的cert refcount = 1*Mar 16 03:28:50.790 : CRYPTO_PKI : 填充
AAA身份驗證資料*Mar 16 03:28:50.790 : CRYPTO_PKI : 無法獲取主AAA清單授權的配置屬性。
*Mar 16 03:28:50.790 : PKI : Cert key-usage : Digital-Signature , Certificate-Signing , CRL-
Signing 16 03:28:50.790 : CRYPTO_PKI : (A069C)鏈式憑證已錨定至信任點CA-GlobalSign-
Root , 鏈式驗證結果為 : CRYPTO_VALID_CERT_WITH_WARNING*Mar 16 03:28:50.790 :
CRYPTO_PKI : (A069C)移除驗證內容*Mar 16 03:28:50.790 : CRYPTO_PKI : 銷毀
ca_req_context型別PKI_VERIFY_CHAIN_CONTEXT , ident 35 , ref count 1 : 減少上下文id-35的
refcount至0*Mar 16 03:28:50.790 : CRYPTO_PKI : ca_req_context released*Mar 16
03:28:50.790 : CRYPTO_PKI : (A069C)驗證TP is CA-Global sign-Root*Mar 16 03:28:50.790 :
CRYPTO_PKI : (A069C)憑證驗證成功*Mar 16 03:28:50.790 : CRYPTO_OPSSL : 憑證驗證成功
*Mar 16 03:28:50.790 : CRYPTO_PKI : Rcvd request to end PKI session A069C.*Mar 16 03:28
50.790 : CRYPTO_PKI : PKI會話A069C已結束。遞減後釋放所有資源。 : cert refcount = 0*3月
16日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讀取伺服器憑證*Mar 16
03:28:50.791 : << TLS 1.2交握[長度009 3] , 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 6 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
03:28:50.7 2 : 8D 36 C9 83 42 B0 4D AC 0C 04 03 00 46 30 44 02*3月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 a 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 : 公鑰3月16日03:28:50.794 :
CKA_KEY_TYPE : : 00 00 03*3月16日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 07000704 2 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 -找到的會話*Mar 16 03:28:50.796 : P11 : C_VerifyInit -金鑰id = 131073*Mar 6
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讀取伺服器金鑰交換*Mar 16
03:28:50.800 : << TLS 1.2交握[length 00 4] , 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讀取伺服器完成
*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握手[length 0046] , ClientKeyExchange*Mar
16 03:28:50.811 : 100 0 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 9D1 6A C0 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 03:28:50.81 2 : *Mar 16 03:28:50.812 :
SSL_connect : SSLv3/TLS寫入使用者端金鑰交換*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 : >>> ???[長度0005]*3月16日
03:28:51.116:17 03 00 35*3月16日03:28:51.116 : *3月16日03:28:51.116 : >> ???[長度0005]*3月
16日03:28:51.116:17 03 03 00 1A*3月16日03:28:51.116 : *3月16日03:28:51.116 : >> ???[長度
0005]*3月16日03:28:51.116:17 03 00 30*3月16日03:28:51.116 : *3月16日03:28:51.116 : >>
???[長度0005]*3月16日03:28:51.116:17 03 03 00 1B*3月16日03:28:51.117 : *3月16日
03:28:51.713 : <<< ???[長度0005]*3月16日03:28:51.713:17 03 03 00 6D*3月16日
03:28:51.713 : *3月16日03:28:51.714 : >> ???[長度0005]*3月16日03:28:51.714:17 03 03 00
1E*3月16日03:28:51.714 : *3月16日03:28:51.732 : <<< ???[長度0005]*3月16日03:28:51.732:17
03 00 71*3月16日03:28:51.732 :

```

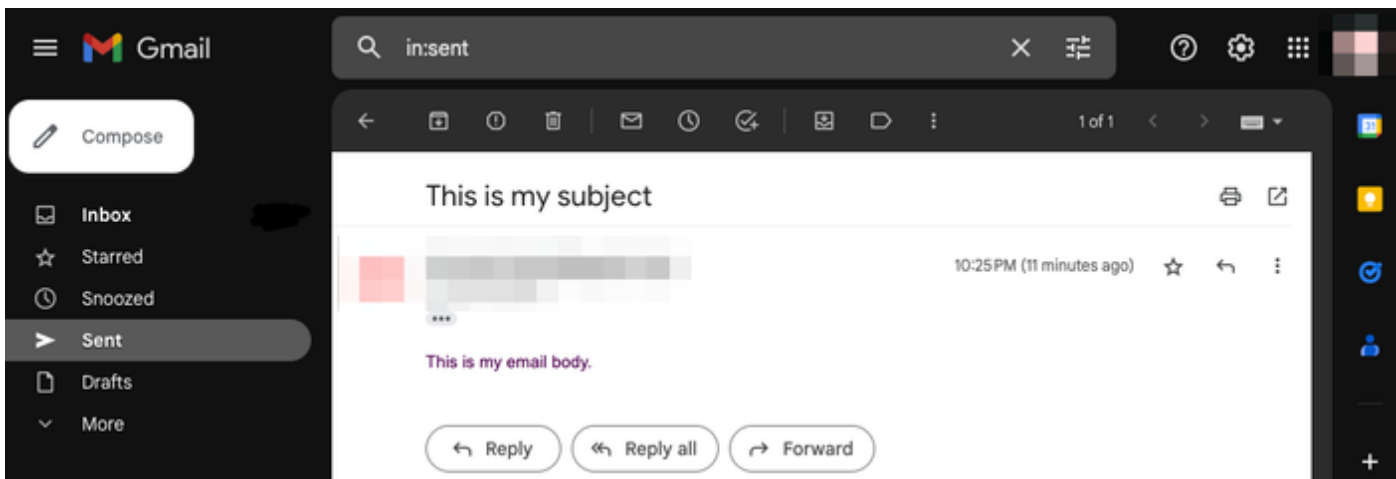
您可以驗證是否已接收電子郵件，以及所有欄位（收件人、發件人、抄送、主題、正文）是否都已正確填充：



您也可以驗證在Cisco IOS XE裝置上的資料包捕獲中發生的TLS握手和會話（附加為「WorkingSMTPwithTLS.pcap」）：

No.	Time	Source	Destination	Protocol	Length	ID	Info
11	2023-03-16 03:28:50...	10.122.144.150	142.251.163.109	TLSv1.2	208	0x8790 (34704)	Client Hello
12	2023-03-16 03:28:50...	142.251.163.109	10.122.144.150	TLSv1.2	590	0x7641 (30273)	Server Hello
32	2023-03-16 03:28:50...	142.251.163.109	10.122.144.150	TLSv1.2	439	0x7649 (30281)	Certificate, Server Key Exchange, Server Hello Done
33	2023-03-16 03:28:50...	10.122.144.150	142.251.163.109	TLSv1.2	180	0x879d (34717)	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
34	2023-03-16 03:28:50...	142.251.163.109	10.122.144.150	TLSv1.2	349	0x764a (30282)	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
36	2023-03-16 03:28:50...	10.122.144.150	142.251.163.109	TLSv1.2	107	0x879f (34719)	Application Data
38	2023-03-16 03:28:50...	142.251.163.109	10.122.144.150	TLSv1.2	306	0x764c (30284)	Application Data
39	2023-03-16 03:28:50...	10.122.144.150	142.251.163.109	TLSv1.2	116	0x87a0 (34720)	Application Data
41	2023-03-16 03:28:50...	142.251.163.109	10.122.144.150	TLSv1.2	101	0x764e (30286)	Application Data
42	2023-03-16 03:28:50...	10.122.144.150	142.251.163.109	TLSv1.2	109	0x87a1 (34721)	Application Data

您甚至可以驗證電子郵件是否反映在使用電子郵件帳戶的「已傳送」資料夾中：



其他注意事項和注意事項

具有@符號的使用者名稱

嘗試使用SMTP中繼時可能會出現問題。由於SMTP中繼，伺服器字串的格式如下（使用者名稱中為「@」）：

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

剖析使用者名稱和密碼的程式碼會在第一次出現「@」符號時分割字串。因此，系統認為伺服器主機名在第一個「@」符號後立即開始並貫穿字串的其餘部分，然後將之前的所有字元解釋為「username : password」。

SMTP的TCL實現使用正規表示式(regex)，以不同方式處理此使用者名稱/密碼/伺服器資訊。由於存在這種差別，TCL允許使用者名稱使用「@」符號；但是，Cisco IOS XE TCL不支援加密，因此沒有透過TLS傳送安全電子郵件的選項。

總結一下：

- 如果電子郵件需要安全，則不能與TCL一起傳送。
- 如果您的使用者名稱中有「@」，則不能使用EEM傳送。

透過存檔的思科漏洞ID [CSCwe75439](#)可藉此機會改進EEM電子郵件功能；但是，當前沒有針對此

增強請求的路線圖。

結論

如圖所示，使用嵌入式事件管理器(EEM)小程式，可以透過SMTP和TLS傳送安全電子郵件。它需要在伺服器端進行一些設定，並配置必要的證書以允許信任，但如果您想生成自動的、安全的電子郵件通知，它是可行的。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。