Utilice EEM para automatizar los correos electrónicos seguros para el usuario

Contenido

Introducción

Este documento describe el proceso necesario para utilizar la acción "servidor de correo" en Embedded Event Manager (EEM) dentro de Cisco IOS® XE para enviar correos electrónicos seguros a un servidor de protocolo simple de transferencia de correo (SMTP) usando Transport Layer Security (TLS) en el puerto 587.

Hay muchas advertencias que puede encontrar durante este proceso, por lo que este artículo fue escrito para documentar los pasos necesarios para lograr esto.

caso de uso

Muchos clientes valoran recibir una notificación por correo electrónico automáticamente después de que se produzca un evento determinado. El subsistema EEM es una potente herramienta para la detección de eventos de red y la automatización integrada, y puede proporcionar una manera eficiente de automatizar las notificaciones de correo electrónico en un dispositivo Cisco IOS XE. Por ejemplo, es posible que desee supervisar una pista IPSLA y, en respuesta a un registro del sistema que indica un cambio de estado, realizar algún tipo de acción y alertar a los administradores de red del evento por correo electrónico. Esta idea de "notificación por correo electrónico" se podría aplicar a muchos otros escenarios como un medio para llamar la atención sobre cualquier evento en particular que desee resaltar.

Background

PEM significa "Privacy Enhanced Mail" (Correo de privacidad mejorada) y es un formato que se utiliza a menudo para representar certificados y claves. Este es el formato de certificado que utilizan los dispositivos Cisco IOS XE. Las aplicaciones seguras (como HTTPS o SMTP seguro) suelen tener un "PEM apilado", en el que intervienen varios certificados, entre los que se incluyen:

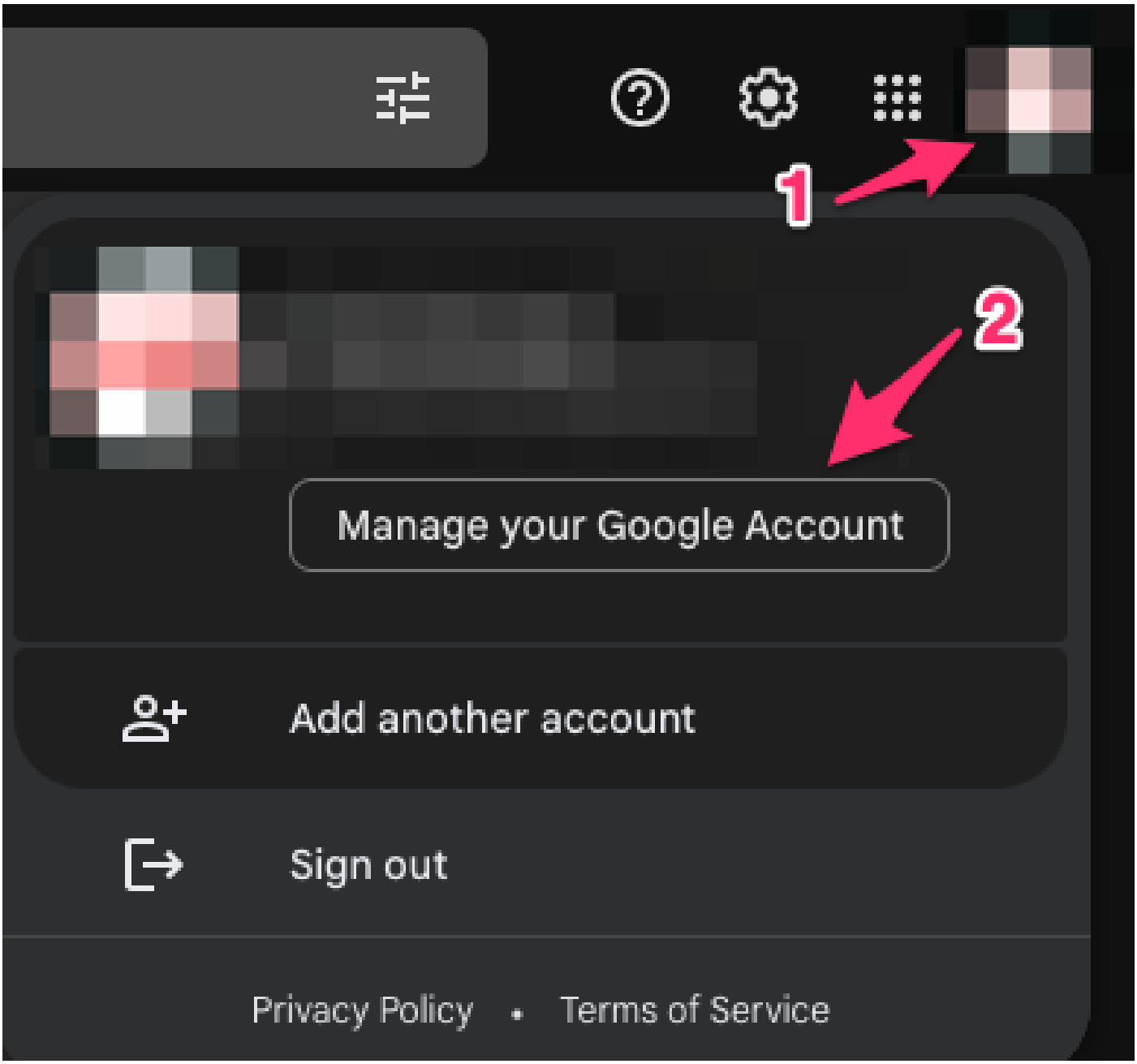
- Certificado raíz
- Certificado de firma (intermedio)
- Certificado de usuario final (o servidor)

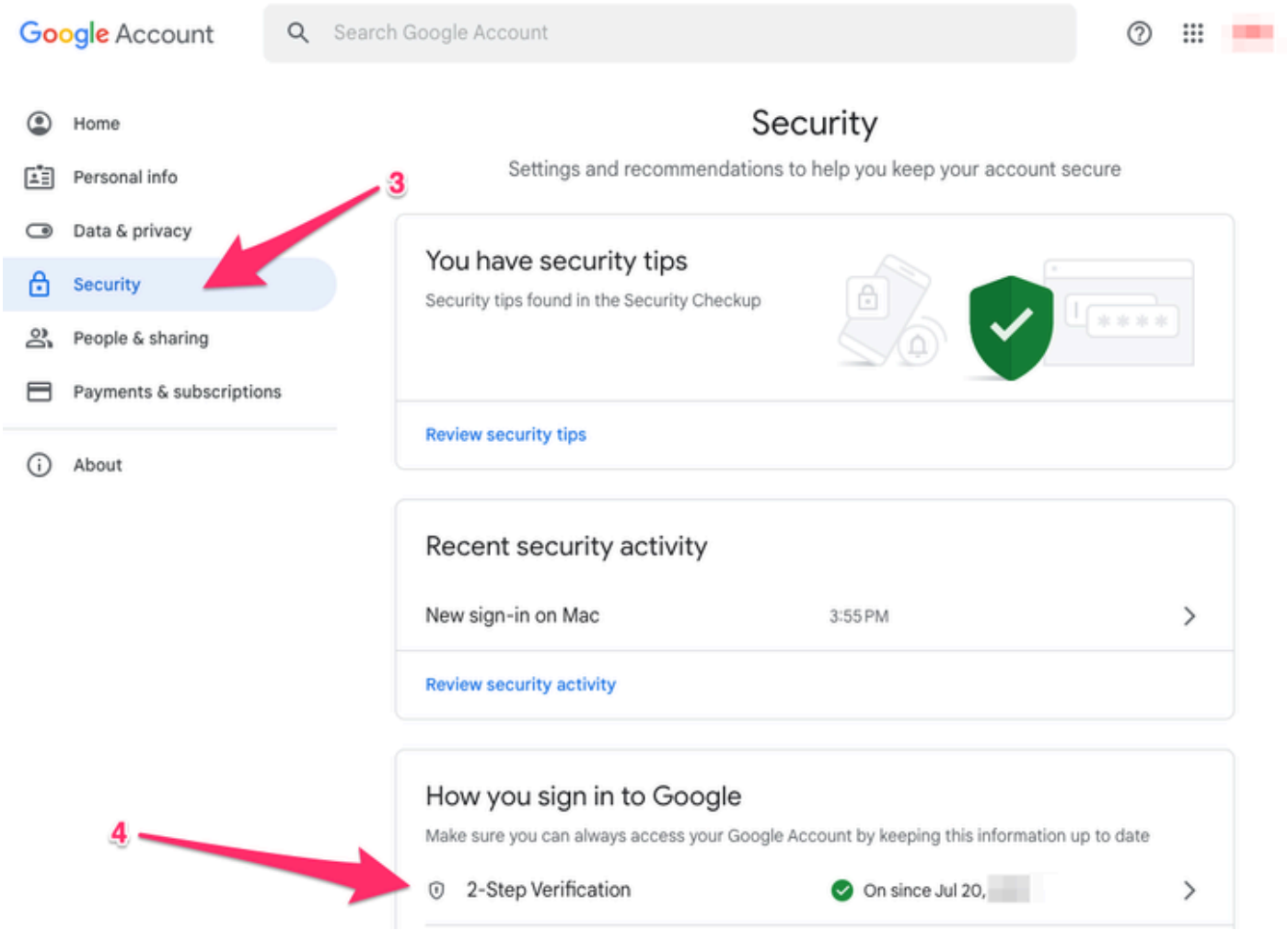
Configuración de cuenta de Gmail

Los servicios SMTP de Google se utilizarán como ejemplo en este artículo. Los requisitos previos son que tengas una cuenta de Gmail previamente configurada.

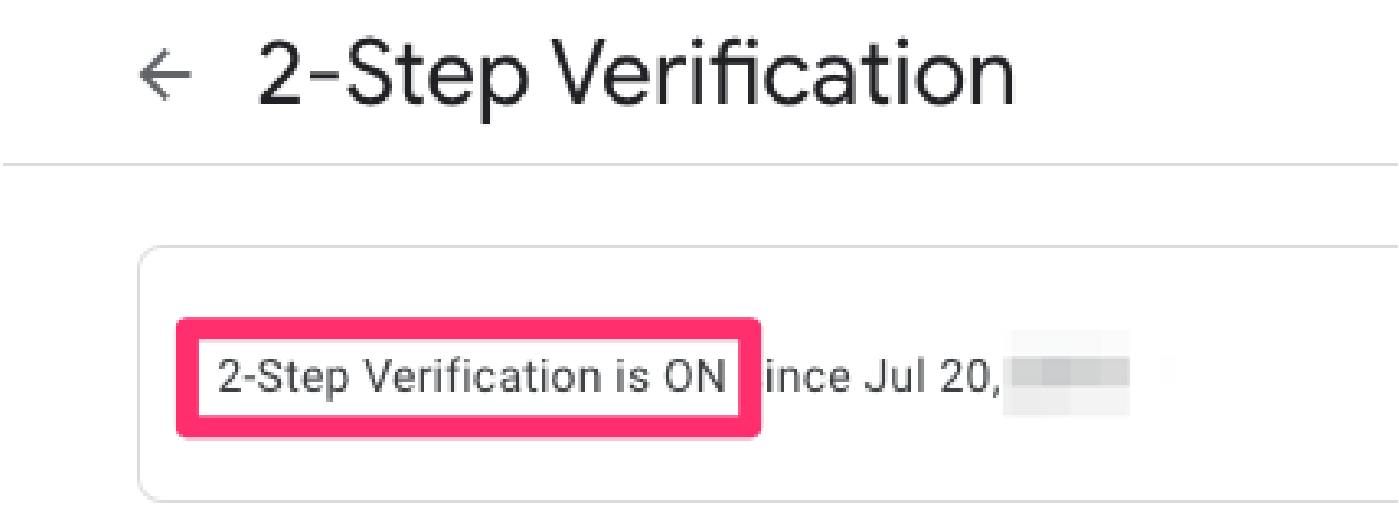
Google te permite enviar correos electrónicos de clientes remotos a Gmail. Solía haber una configuración en Gmail para "aplicaciones no seguras", y la aplicación se enfrentaría a un error si esta configuración no se permite en el extremo de Google. Esta configuración se ha eliminado y, en su lugar, se encuentra la opción "Aplicaciones seguras", a la que se puede acceder a través de:

mail.google.com > Haga clic en su perfil (#1) > Gestione su cuenta de Google (#2) > Seguridad (#3) > Cómo iniciar sesión en Google > Verificación en 2 pasos (#4)


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



En esta página, asegúrese de que la verificación en dos pasos está activada.



Luego, puedes desplazarte hasta "Contraseñas de la aplicación" para que Gmail genere una contraseña que se pueda usar para iniciar sesión en tu cuenta de Google desde una aplicación que no admita la verificación en 2 pasos.

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

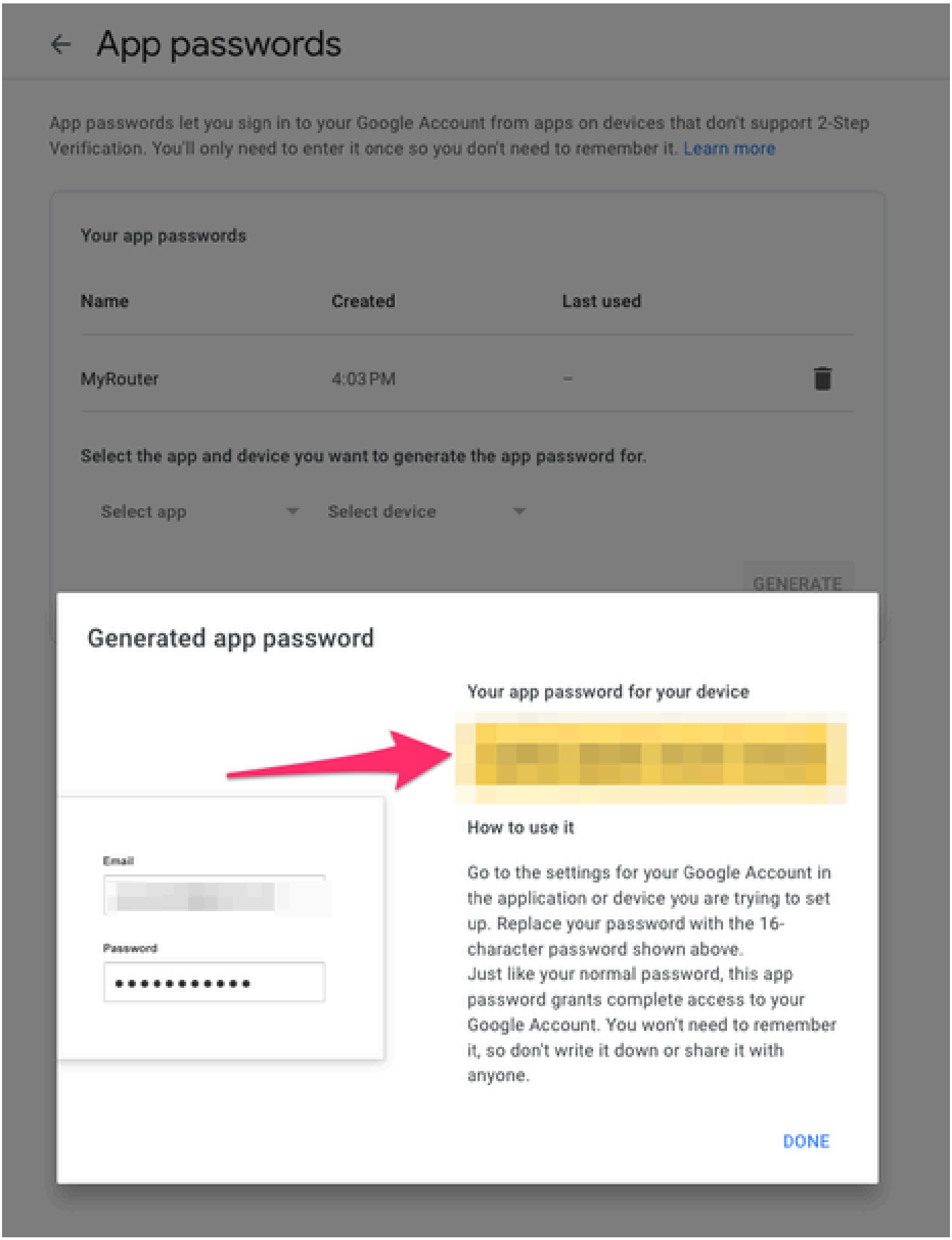
App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. Learn more

You don't have any app passwords.

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

MyRouter

GENERATE



La contraseña de la aplicación de 16 caracteres de esta captura de pantalla se ha borrado, ya que está vinculada a una cuenta personal de Gmail.

Ahora que tiene una contraseña de aplicación para Gmail, puede utilizarla, junto con el nombre de su cuenta de Gmail, como el servidor de correo electrónico que debe utilizar para reenviar el correo electrónico. El formato para especificar el servidor es "username:password@host".

Configuración de EEM base

Hay muchas maneras de personalizar un script EEM para que se ajuste a sus necesidades exactas, pero este ejemplo es un script EEM básico para ejecutar la funcionalidad de correo electrónico seguro:

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

En primer lugar, las configuraciones crean tres variables de entorno de EEM: _email_from, _email_to y _email_server. Cada una se define en una variable para facilitar los cambios de configuración. A continuación, se crea el script SendSecureEmailEEM. El evento desencadenante aquí es "none", de modo que puede ejecutar manualmente el script EEM cuando lo desee mediante "# event manager run SendSecureEmailEEM" (en lugar de esperar a que se desencadene un evento específico). A continuación, solo tiene una acción de "servidor de correo" que se ocupa de la generación de correo electrónico. Las opciones "secure tls" y "port 587" le indican al dispositivo que negocie TLS en el puerto 587, en el cual los servidores de Gmail estarán escuchando.

También debe asegurarse de que el campo "De" es válido. Si se está autenticando como "Alice" pero está intentando enviar un correo electrónico desde "Bob", se producirá un error porque Alice está suplantando la dirección de correo electrónico de otra persona. El campo "De" debe alinearse con la cuenta que se está utilizando para enviar el correo electrónico en el servidor.

Problema detectado con solo certificados predeterminados instalados

EEM utiliza openssl para establecer una conexión con el servidor SMTP. Para una comunicación segura, el servidor devuelve un certificado a openssl que se ejecuta en Cisco IOSd. IOSd buscará un punto de confianza asociado a ese certificado.

En un dispositivo Cisco IOS XE, los certificados de los servidores SMTP de Gmail no se instalan de forma predeterminada. Deben importarse manualmente para que se establezca la confianza. Sin los certificados instalados, el intercambio de señales TLS fallará debido a un "certificado incorrecto".

Estas depuraciones son extremadamente útiles para depurar cualquier problema de certificado:

```
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
```

Puede iniciar una captura de paquetes integrada (EPC) en el router para capturar el tráfico que entra o sale del servidor de correo electrónico cuando se activa el EEM:

```
! 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
```

En última instancia, openssl no puede establecer la sesión TLS segura con el servidor SMTP, por lo que arroja un error de "certificado incorrecto", que hace que EEM deje de ejecutarse:

```
*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
```

La captura de paquetes documentada de este intercambio se adjunta como "NoCertificateInstalled.pcap". El paquete TLS final del router (10.122.x.x) al servidor SMTP de Gmail (142.251.163.xx) muestra que la negociación TLS se finalizó debido al mismo mensaje de "Certificado erróneo" visto en las depuraciones anteriores.

```
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)
```

Certificados para proteger SMTP

Debido a que faltan los certificados que permiten que el dispositivo Cisco IOS XE confíe en los servidores de Gmail, la solución es instalar uno o todos esos certificados en un punto de confianza en el dispositivo.

Por ejemplo, las depuraciones completas de la prueba anterior muestran estas búsquedas de certificados que tuvieron lugar:

```
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
```

Es necesario instalar un certificado para cada uno de estos emisores bajo un punto de confianza para que el dispositivo pueda establecer una sesión segura con los servidores SMTP de Gmail. Puede crear un punto de confianza para cada emisor utilizando estas configuraciones:

```
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
```

Ahora tiene un punto de confianza para cada emisor configurado; sin embargo, aún no hay certificados reales asociados a ellos. Básicamente, son puntos de confianza en blanco:

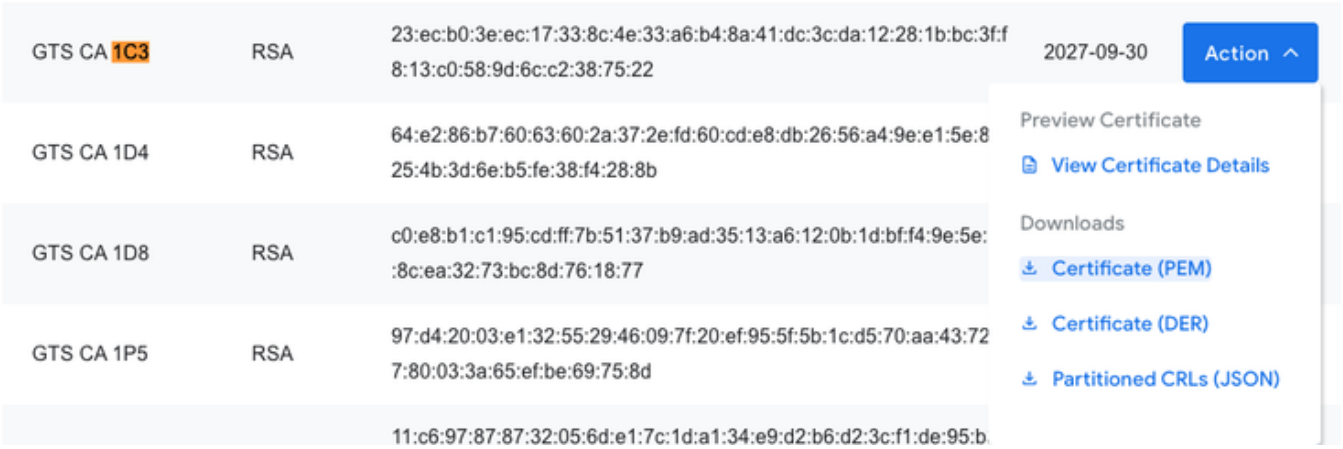
```
# show run | sec crypto pki certificate chain CA-
crypto pki certificate chain CA-GTS-1C3
crypto pki certificate chain CA-GTS-Root-R1
crypto pki certificate chain CA-GlobalSign-Root
crypto pki certificate chain CA-gmail-SMTP
```

Debe rastrear dónde se encuentran esos certificados y, a continuación, instalarlos en el dispositivo.

Buscando en línea "Google Trust Services 1C3", nos encontramos rápidamente con el repositorio de certificados de servicios de confianza de Google:

https://pki.goog/repository/

Después de expandir todos los certificados de esa página, puede buscar "1C3", hacer clic en el menú desplegable "Acción" y descargar el certificado PEM:



Al abrir el archivo PEM descargado con un editor de texto, se muestra que se trata simplemente de un certificado que se puede importar al dispositivo Cisco IOS XE bajo el punto de confianza que creó anteriormente:

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

Puede importarlo bajo el punto de confianza "CA-GTS-1C3" utilizando los comandos de configuración:

```
(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)#
```

Y luego puede confirmar que el certificado fue instalado:

```
# 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 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
```

A continuación, puede instalar los certificados para los otros dos emisores.

CA-GTS-Root-R1:

Configuración:

Deflector (Destaque para leer)

```
(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-R1Introduzca el certificado de CA codificado base 64.Termine con una línea en blanco o la palabra "quit" en una línea por sí mismaMIIFVzCCAz+gAwIBAgINAgPlk28xsBNJiGuiFzANBgkqhkiG9w0BAQwFADBHMQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU<snip>2tIMPNuzjsmhDYAPexZ3FL/2wmUspO8IFgV6dtxQ/PeEMMA3KgqlbbC1j+Qa3bbbP6MvPJwNQzcmRk13NfIRmPVNnGuV/u3gm3cCertificate tiene los siguientes atributos:Fingerprint MD5: 05FED0BF 71A8A376 63DA01E0 D852DC40 Fingerprint SHA1: E58C1CC4 913B3863 4BE9106E E3AD8E6B 9B DD9814A% ¿Acepta este certificado? [yes/no]: síSe aceptó el certificado de CA de Trustpoint.% El certificado se importó correctamente(config)# end

Verificación de configuración en ejecución:

Deflector (Destaque para leer)

```
# 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 F70D010 1 0C050030 47310B30 09060355 04061302 55533122 <snip> 6775C119 3A2B474E D3428EFD 31C30200603 DAD20C3C DBB38EC9 A10D800F 7B81666 BFFFDB09 94B293BC 167714E9 DB7143DE3 DE10C3 00 DCA82A95 B6C2D63F 906B76DB 6CFE8CBC F205815C DC270350 DCD7C846 63D991935 53671 AE57FBB7 826DDC salir

Mostrar verificación criptográfica:

Deflector (Destaque para leer)

```
# 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 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 22 201 Fecha de finalización: 00:00:00 UTC 22 de junio de 2036 Información de clave del asunto: Clave pública Algoritmo: rsaEncryption RSA Public Key: (4096 bit) Algoritmo de firma: SHA384 with RSA Encryption Fingerprint MD5: 05FED0BF 71A8A376 63DA01E0 D852DC40 Fingerprint SHA1: E58C4 CC1CC 913B3863 4BE9106E E3AD8E6B 9DD9814A Extensiones X509v3: Uso de claves X509v3: 86000000 Firma de clave de firma digital Firma CRL ID de clave del asunto X509v3: E4AF2B26 711A2B48 27852F52 662CEF0 8913713E X509v3 Restricciones básicas CA: TRUE Authority Info Acceso: hora de instalación del certificado: 14:39:38 UTC 13 de marzo de 2023 Hora de instalación del certificado en nsec: 1678718378546968064 Puntos de confianza asociados: CA-GTS-Root-R1 Trustpool

CA-GlobalSign-Root:

Este certificado se encontró en esta ubicación:

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

Configuración:

Deflector (Destaque para leer)

```
(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>
DKqC5JlR3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/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-RootIngrese el certificado CA codificado base 64.End con una línea en blanco o la palabra "quit" en una línea por sí mismaMIIDdTCCAl2gAwIBAgILBAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkGA1UEBhMCQ
oTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv<snip>DKqC5JlR3XC321Y9YeRq4VzW9v493kH
El certificado SDJ3gyICh3WZlXi/EjJKSZp4A== tiene los siguientes atributos:Fingerprint MD5: 3E455215 095192E1 B75D379F B187298A Fingerprint SHA1: B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C% ¿Acepta este certificado? [yes/no]: síSe aceptó el certificado de CA de Trustpoint.% El certificado se importó correctamente(config)# end

Verificación de configuración en ejecución:

Deflector (Destaque para leer)

```
# 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 9951DD70 B7DB56 3D 61E46AE1 5CD6F6FE 3DDE41CC 07AE6352 BF5353F4 2BE9C7FD B6F7825F 85D24118 DB81B304 1CC51FA4 806F1520 C9DE0C88 0A1DD6655E2FC48 9292669 E0 quit

Mostrar verificación criptográfica:

Deflector (Destaque para leer)

```
#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): 040000000001154B5AC394Certificate Usage: SignatureIssuer: cn=GlobalSign Root CAou=Root CAo=GlobalSign nv-sac=BESubject: cn=GlobalSign Root CAou=Root CAo=GlobalSign nv-sac=BEValidity Date: start date: 12:00:00 UTC Sep 1998end Fecha: 12:00:00 UTC 28 de enero de 2028Información sobre la clave del asunto:Algoritmo de clave pública: rsaEncryptionClave pública RSA: (2048 bits)Algoritmo de firma: SHA1 con cifrado RSAFingerprint MD5: 3E455215 095192E1 B75D379F B187298A Fingerprint SHA1: B1BC968B D4F49D62 2AA89A888 1 F2150152 A41D829C X509v3 extensiones:Uso de clave X509v3: 6000000Signo de certificado de claveFirma CRLX509v3 Id. de clave de asunto: 607B661A 450D97CA 89502F7D 04CD34A8 FFFCFD4B X509v3 Restricciones básicas:CA: TRUEesceso de información de autoridad:Tiempo de instalación del certificado: 0 3:03:01 UTC 16 de marzo de 2023 Hora de instalación del certificado en nsec: 1678935781942944000Puntos de confianza asociados: CA-GlobalSign-Root

CA-gmail-SMTP:

El certificado TLS para los servidores de Gmail (CA-gmail-SMTP) se encontró siguiendo los pasos que se describen a continuación: Usar certificados TLS para transporte seguro

Configuración:

Deflector (Destaque para leer)

```
(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 9O6A414D 6D57B783 946F3OA2
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-SMTPEntroduzca el certificado CA codificado base 64.Termine con una línea en blanco o la palabra "quit" en una línea por sí mismaMIIEhjCCA26gAwIBAgIQUofgQKT+9wcSaLBP3d3w9DANBgkqhkiG9w0BAQsFADBGMQswCQYD EzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM<snip>b1J2gZAyjyd4nfFRG1jeL5KrsfUR9I jncvow==Trustpoint 'CA-gmail-SMTP' es una CA subordinada, pero el certificado no es una CA.Se requiere verificación manualEl certificado tiene los siguientes atributos:Fingerprint MD5: 19651FBE 906A414D 6D57B783 946F30A2 Fingerprint SHA1: 4EF392CB EEB46D5E 47433953 AAEF313F 4C6D2825 % ¿Acepta este certificado? [sí/no]: síSe aceptó el certificado de CA de Trustpoint.% El certificado se importó correctamente(config)#

Verificación de configuración en ejecución:

Deflector (Destaque para leer)

```
# 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 5287E040A4FEF7071268B04FDDDF0F4 30820486 3082036E A0030201 02021052 87E040A4 FEF70712 68B04FDD DDF0F430 0D06092A 864886F7 0D01010B 05003046 310B3009 06035504 06130255 p> 92ABB1F5 11F53312230 B9FAB24A F94F5283 EE2928B7 7EFB084B 6D61217 416045 C47BCB99 801C4969 E4D48E77 2FA3 quit

Mostrar verificación criptográfica:

Deflector (Destaque para leer)

```
# 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): 5287E040A4FEF7071268B04FDDDF0F4Certificate Usage: SignatureIssuer: cn=GTS CA 1C3o=Google Trust Services LLCc=USSubject: cn=smtp.gmail.comCRL Distribution Points: http://crls.pki.goog/gts1c3/moVDfISia2k.crlValidity Date: start date: 09:15:03 UTC Feb 20 2023fecha de finalización: 09:15:02 UTC 15 de mayo de 2023Información sobre la clave del asunto:Algoritmo de clave pública: ecEncryptionEC Public Key: (256 bit)Algoritmo de firma: SHA256 con cifrado RSAHuella dactilar MD5: 19651FBE 906A414D 6D57B783 946F30A2 Huella dactipoética SHA1: 4EF3999 2CB EEB46D5E 47433953 AAEF313F 4C6D2825 Extensiones X509v3:Uso de clave X509v3: 80000000Firma digitalX509v3 ID de clave de asunto: 5CC36972 D07FE997 510E1A67 8A8ECC23 E40CFB68 X509v3 Restricciones básicas:CA: FALSEX Nombre alternativo del sujeto 509v3:smtp.gmail.com Dirección IP: OtherNames : X509v3 Authority Key ID: 8A747FAF 85CDEE95 CD3D9CD0 E24614F3 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 Usage:Server AuthCert install time: 03:10:41 UTC Mar 11 6 2023 Tiempo de instalación del certificado en nsec: 1678936241822955008Puntos de confianza asociados: CA-gmail-SMTP

Una forma más sencilla de encontrar los certificados

Alternativamente, puede intentar utilizar una llamada openssl de un servidor/laptop como una manera más fácil de obtener los certificados de un servidor SMTP sin tener que utilizar debugs y buscar en Google para rastrearlos:

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

También puede visitar use smtp.gmail.com:

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

Los resultados de esa llamada incluirán los certificados reales en sí mismos que se pueden utilizar para las configuraciones "crypto pki authenticate <trustpoint>".

Prueba de EEM con SMTP seguro de nuevo

Ahora que los certificados se aplican al dispositivo Cisco IOS XE, el script EEM enviará los mensajes SMTP seguros como se esperaba.

```
# event manager run SendSecureEmailEEM
```

Verifique el Spoiler para las salidas completas de debug de crypto y ssl:

Deflector (Destaque para leer)

```
# 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:
```

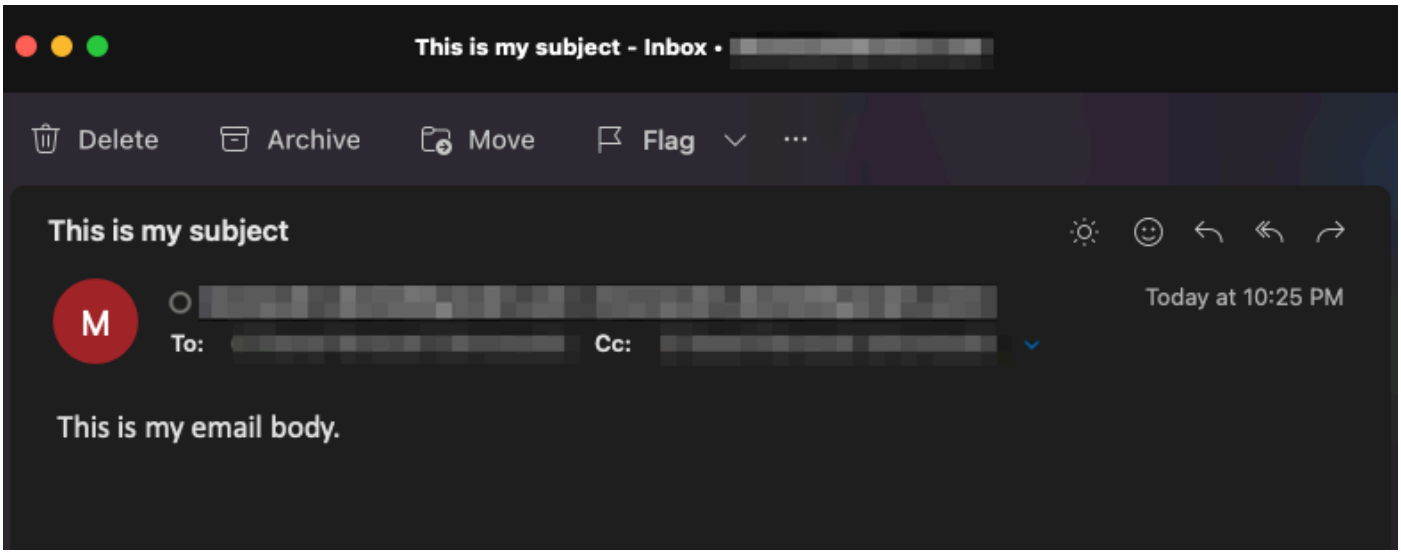
event manager run SendSecureEmailEEM*Mar 16 03:28:50.673: CRYPTO_OPSSL: Allocated the memory for OPSSLContext*Mar 16 03:28:50.673: CRYPTO_OPSSL: Set cipher specs to mask 0x02FC0000 for version 128*Mar 16 03:28:50.674: Set the Default Lista de curvas CE: 0x70Ajuste la lista de curvas CE: secp521r1:secp384r1:prime256v1*Mar 16 03:28:50.674: opssl_SetPKIInfo entry*Mar 16 03:28:50.674: CRYPTO_PKI: (A069B) Sesión iniciada - identidad seleccionada (TP-self-signed-486541296)x TP-self-signed-486541296:refcount after increment = 1*Mar 16 03:28:50.674: CRYPTO_PKI: Begin local cert chain recovery.*Mar 16 03:28:50.674: CRYPTO_PKI(Cert Lookup) issuer="cn=IOS-Self-Signed-Certificate-486541296" serial number= 01*Mar 16 03:28:50.674: CRYPTO_PKI: se está buscando cert en handle=7F41E523CE0, 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: Finalizado con captura de cadena de certificados local 0.*Mar 16 03:28:50.675: CRYPTO_PKI: Solicitud recibida para finalizar la sesión PKI A069B.*16 de marzo de 03:28:50.675: CRYPTO_PKI: la sesión PKI A069B ha finalizado. Liberando todos los recursos.TP-self-signed-486541296:unlocked trustpoint TP-self-signed-486541296, refcount is 0*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 Criteria mode capability in CiscoSSL on SSL CTX 0x7F41F28EAFF8*Mar 16 03:28:50.675: CRYPTO_OPSSL: ciphersuites ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-GCM-SHA384:DHE-RSA AES256-SHA256:AES256-GCM-SHA384:AES256-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:DHE RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:AES128-GCM-SHA256:AES128-SHA256*16 de marzo de 03:28:50.676: Apretón de manos: antes de la inicialización de SSL*16:03:28:50.676: SSL_connect:before SSL initialize*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 hello del cliente*16 de marzo 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 Handlength 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 0 3:28:50.692: 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 03:28:5 0,693: extensión de servidor TLS "desconocida" (id=23), len=0extensión de servidor TLS "renegociar" (id=65281), len=1*mar 16 03:28:50.693: 00*mar 16 03:28:50.693: extensión de servidor TLS "Formatos de punto EC" (id=11), len=2*mar 16 03:28:50.693: 01 0 0*Mar 16 03:28:50.693: extensión de servidor TLS

"ticket de sesión" (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 0length F9A], 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<snip >*16 de marzo de 2013 03:28:50.763: 82 35 CF 62 8B C9 24 8B A5 B7 39 0C BB 7E 2A 41*16 de marzo de 2013 03:28:50.763: BF 52 CF FC A2 96 B6 C2 82 3F*16 de marzo de 2013:28 50.765: CC_DEBUG: Introducción de la función de devolución de llamada de la aplicación de la capa de corrección de errores*Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) Sesión iniciada - identidad no especificada*Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) Adición de certificado de peer*16 Mar 03:28:5:5:55:50.755: CRY7 YPTO_PKI: Se ha añadido certificado de par x509 - (1162) bytes*Mar 16 03:28:50.767: CRYPTO_PKI: (A069C) Agregando certificado de par*Mar 16 03:28:50.768: CRYPTO_PKI: Se ha agregado certificado de par x509 - (1434) bytes*Mar 16:03:28:5 60.768: CRYPTO_PKI: (A069C) Adición de certificado de peer*Mar 16:03:28:50.770: CRYPTO_PKI: Agregado certificado de peer x509 - (1382) bytes*Mar 16:03:28:50.770: CRYPTO_OPSSL: Validar devolución de llamada de cadena de certificado*Mar 16:03:28:50.7 0: CRYPTO_PKI(Búsqueda de certificados) issuer="cn=GTS CA 1C3,o=Google Trust Services LLC,c=US" número de serie= 52 87 E0 40 A4 FE F7 07 12 68 B0 4F DD DD F0 F4*16 de marzo 03:28:50.770: CRYPTO_PKI: se está buscando el certificado en handle=7F41E523CE0, digest=A7 CC 4A7 B 0F 36 C3 AC D1 2F 77 DD 1D 9A 37 DC FC*Mar 16 03:28:50.770: CRYPTO_PKI(Búsqueda de certificados) emiser="cn=GTS Root R1,o=Google Trust Services LLC,c=US" número de serie= 02 03 BC 53 59 6B 34 C7 18 F5 01 50 66*Mar 16 03:28:50 771: CRYPTO_PKI: buscando cert en handle=7F41E523CE0, 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-sa,c=BE" número de serie = 77 BD 0D 6C DB 36 F9 1A EA 21 0F C4 F0 58 D3 0D*Mar 16 03:28:50.771: CRYPTO_PKI: buscando certificado en el identificador=7F41E523CE0, digest=94 40 D1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A*Mar 16 03:2 8:50.771: CRYPTO_PKI: No se ha encontrado el registro de certificado para la serie del emisor.*16 de marzo 03:28:50.772: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()*16 de marzo 03:28:50.772: CRYPTO_PKI: Se ha encontrado una coincidencia de asunto*16 de marzo de 03:#28:50.77772: CRYPTO_PKI: ip-ext-val: no es necesaria la validación de la extensión IP:Incremento del refcount para el contexto id-35 a 1*Mar 16 03:28:50.773: CRYPTO_PKI: crear nuevo ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 35*Mar 16 03:28:50.773: CRYPTO_PKI: (A069C)la ruta de validación tiene 1 certs*Mar 11 6:03:28:50.773: CRYPTO_PKI: (A069C) Comprobar certificados idénticos*Mar 16:03:28:50.773: CRYPTO_PKI(Búsqueda de certificados) emiser="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-sa,c=BE" número de serie= 77 BD 0D 6C DB 36 F9 1A EA 21 0F4 F0 55 8 D3 0D*Mar 16 03:28:50.774: CRYPTO_PKI: buscando certificado en identificador=7F41E523CE0, resumen=94 40 D1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A*Mar 16 03:28:50.774: CRYPTO_PKI: No se ha encontrado el registro de certificado para el emisor serie. *16 de marzo de 03:28:50.774: CRYPTO_PKI: (A069C) Validación de certificado no fiable*16 de marzo de 03:28:50.774: CRYPTO_PKI: (A069C) Crear una lista de puntos de confianza adecuados*16 de marzo de 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) Los puntos de confianza adecuados son: CA-GlobalSign-Root,*Mar 16 03:28:50.775: CRYPTO_PKI: (A069C) Intentando para validar el certificado mediante CA-GlobalSign-Root policy*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: Agregado 1 certificados a trusted * Mar 16 03:28:50.775: CRYPTO_PKI: Preparar proveedores de servicios de revocación de sesiones * 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 16 de marzo 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>*16 de marzo 03:28:50.780: CKA_PUBLIC_EXPONENT: 0 11 00 01*16 de marzo 03:28:50.780: CKA_VERIFY_RECOVER: 01*16 de marzo 03:28:50.780: CRYPTO_PKI: Eliminando la clave almacenada en caché con ID de clave 45*16 de marzo 03:28:50.781: CRYPTO_PKI: Intentando insertar la clave pública del par en la caché*16 03:2 8:50.781: CRYPTO_PKI: el público del par se ha insertado correctamente con la ID de clave 46*16 de marzo 03:28:50.781: P11:C_CreateObject: 131118*16 de marzo 03:28:50.781: P11:C_GetMechanismInfo slot 1 tipo 3 (mecanismo no válido)*16 03:28:50.781: P 1: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:se encontró pubkey en la caché usando index = 46*Mar 16:03:2 8:50.781: P11:clave pública encontrada: 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 0 3:28:50.788: P11:CEAL:CRYPTO_NO_ERR*Mar 16 03:28:50.788: P11:C_DestroyObject 2:2002E*Mar 16 03:28:50.788: CRYPTO_PKI: Caducidad de la clave almacenada en caché del par con ID de clave 46*Mar 16:03:28:5 60.788: CRYPTO_PKI: (A069C) El certificado está verificado*16 de marzo de 03:28:50.788: CRYPTO_PKI: Eliminar proveedores de servicios de revocación de sesiones*16 de marzo de 03:28:50.788: CRYPTO_PKI: Eliminar proveedores de servicios de revocación de sesionesCA-GlobalSign-Root:estado de validación - CRYPTO_VALID_CERT_WITH_WARNING*16 03 03:28:50.788: CRYPTO_PKI: (A069C) Certificado validado sin comprobación de revocación: recuento de certificados tras incremento = 1*Mar 16 03:28:50.790: CRYPTO_PKI: Rellenar datos de autenticación AAA*Mar 16 03:28:50.790: CRYPTO_PKI: No se puede obtener el atributo configurado para la autorización de lista AAA principal.*Mar 16 03:2 8:50.790: PKI: uso de clave de certificado: Firma digital , Firma de certificado , Firma de CRL*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C)el certificado de cadena se ancló al trustpoint CA-GlobalSign-Root, y el resultado de la validación de cadena fue: CRYPTO_VALID_CERT_WITH_WARNING*Mar. 16 03:28:50.790: CRYVALID. PTO_PKI: (A069C) Quitar contexto de verificación*Mar 16 03:28:50.790: CRYPTO_PKI: destruir ca_req_context type PKI_VERIFY_CHAIN_CONTEXT, ident 35, recuento de referencias 1:Reducir el recuento de contexto id-35 a 0*Mar 16 03:28:50.790: CRYPTO_PKI: ca_req_context liberado*Mar 1 6:03:28:50.790: CRYPTO_PKI: (A069C) Validación TP es CA-GlobalSign-Root*16 de marzo de 2013:28:50.790: CRYPTO_PKI: (A069C) Validación del certificado correcta*16 de marzo de 2013:28:50.790: CRYPTO_OPSSL: La verificación del certificado se ha realizado correctamente*16 16:03:28:28 0.790: CRYPTO_PKI: Solicitud recibida para finalizar la sesión PKI A069C.*16 de marzo 03:28:50.790: CRYPTO_PKI: La sesión PKI A069C ha finalizado. Liberando todos los recursos.:cert refcount tras decrement = 0*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 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 3:28:50.792: E0 D7 D5 9C 75 C0 7D 5B D6 B2 0A B5 CC EA E1 4B*16 de marzo 03:28:50.792: 4E5 72 7B 54 5D 9B2 95 91 E0 CC D6 A5 8E CE*16 de marzo 03:28:50.792: 8D 36 C9 83 4 2 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 2F 9 4E F0*16

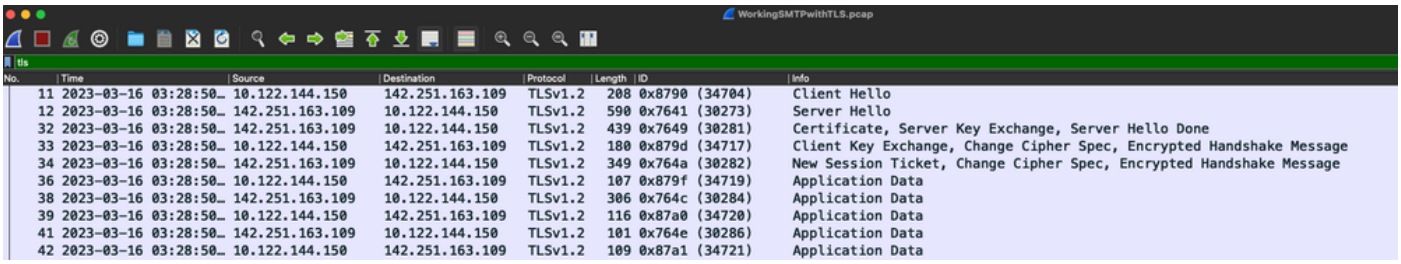
de marzo 03:28:50.793: A8 02 20 24 42 91 BE B7 10 1C D1 C0 12 28 FB*16 de marzo 03:28:50.793: E4 DE 81 0B AA 66 19 CD 28 5A0 30 7D 3C 4A 56*16 de marzo 03:28:5 0,793: 0D 94 E2*Mar 16 03:28:50.793: *Mar 16 03:28:50.794: P11:C_FindObjectsInit:*Mar 16 03:28:50.794: CKA_CLASS: PUBLIC KEY*Mar 16:03:28:50.794: CKA_KEY TIPO: 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> 16 03:28:50.796: P11:C_FindObjectsFinal*Mar 16 03:28:50.796: P11:C_VerifyInit - Sesión encontrada*Mar 16 03:28:50.796: P11:C_VerifyInit - id de clave = 131073*Mar 16 03:28:50.796: P1: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 [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 03:28:50.81 1: 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 9D1 6A 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 6 03:28:50.812: SSL_connect:SSLv3/TLS write client key exchange*16 de marzo de 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 ChangeCypherSpec [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:

Puede comprobar que el correo electrónico se ha recibido y que todos los campos (para, de, cc, asunto, cuerpo) se han rellenado correctamente:

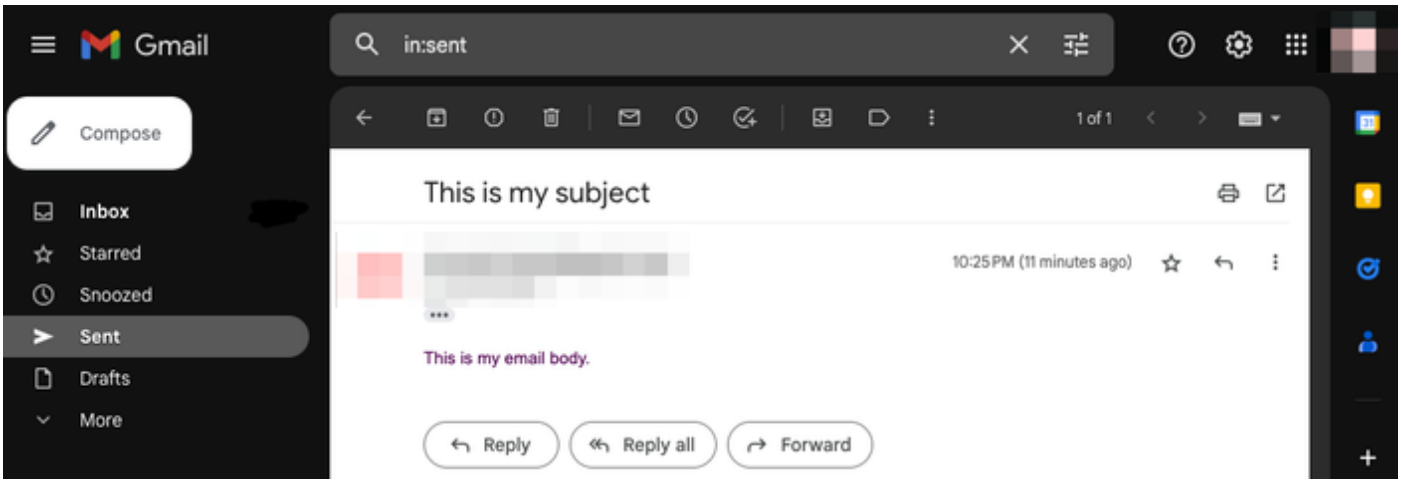


También puede verificar que el intercambio de señales de TLS y la sesión tuvieron lugar desde la

captura de paquetes en el dispositivo Cisco IOS XE (adjunto como "WorkingSMTPwithTLS.pcap"):



Incluso puede verificar que los correos electrónicos se reflejen en la carpeta "Enviados" de la cuenta de correo electrónico utilizada:



Otras advertencias y consideraciones

Nombres de usuario con símbolos @

Se pueden ver problemas al intentar utilizar un relay SMTP. Debido a la retransmisión SMTP, la cadena de servidor tiene este formato (un "@" en el nombre de usuario):

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

El código para analizar el nombre de usuario y la contraseña divide la cadena en la primera aparición del símbolo "@". Como resultado, el sistema piensa que el nombre de host del servidor comienza inmediatamente después del primer símbolo "@" a través del resto de la cadena, e interpreta todo lo anterior como el "nombre de usuario:contraseña".

La implementación TCL de SMTP utiliza una expresión regular (regex) que maneja esta información de nombre de usuario/contraseña/servidor de manera diferente. Debido a esa diferencia, TCL permite nombres de usuario con un símbolo "@"; sin embargo, Cisco IOS XE TCL no admite crypto, por lo que no hay opción para enviar correos electrónicos seguros a través de TLS.

Para resumir:

- Si el correo electrónico debe ser seguro, no podrá enviarlo con TCL.
- Si hay un "@" en su nombre de usuario, no puede enviarlo con un EEM.

El ID de bug de Cisco CSCwe75439 se registró para abordar esta oportunidad de mejorar la función de correo electrónico de EEM; sin embargo, actualmente no hay un mapa de ruta para esta solicitud de mejora.

Conclusión

Como se muestra aquí, es posible enviar correos electrónicos seguros a través de SMTP con TLS mediante el applet Embedded Event Manager (EEM). Requiere cierta configuración en el lado del servidor, así como la configuración de los certificados necesarios para permitir la confianza, pero es factible si desea generar notificaciones de correo electrónico automatizadas y seguras.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).