# Guía completa de la configuración para TLS en el ESA

## Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Descripción general funcional y requisitos](#)
[Traiga su propio certificado](#)
[Ponga al día un certificado actual](#)
[Despliegue los certificados autofirmados](#)
[Genere un certificado autofirmado y un CSR](#)
[Proporcione el certificado autofirmado a CA](#)
[Cargue el certificado firmado al ESA](#)
[Especifique el certificado para el uso con los servicios ESA](#)
[TLS entrante](#)
[TLS saliente](#)
[HTTPS](#)
[LDAP](#)
[Filtrado de URL](#)
[Sostenga la configuración del aparato y los certificados](#)
[Active TLS entrante](#)
[Active TLS saliente](#)
[Troubleshooting](#)
[Certificados intermedios](#)
[Notificaciones del permiso para los errores requeridos de la conexión TLS](#)
[Localice a las sesiones de comunicación acertadas de TLS en los registros del correo](#)
[Información Relacionada](#)

## Introducción

Este documento describe cómo crear un certificado para el uso con Transport Layer Security (TLS), activar TLS entrante y saliente, y resolver problemas los problemas básicos de TLS en Cisco envíe por correo electrónico el dispositivo de seguridad (ESA).

## Prerequisites

### Requisitos

No hay requisitos específicos para este documento.

### Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Antecedentes

La implementación de TLS en el ESA proporciona la aislamiento para la transmisión de punto a punto de los correos electrónicos con el cifrado. Permite que un administrador importe un certificado y una clave privada de un servicio del Certificate Authority (CA), o utiliza un certificado autofirmado.

Cisco AsyncOS para la Seguridad del correo electrónico soporta la extensión *STARTTLS al* Simple Mail Transfer Protocol (SMTP) (*S TP seguro sobre TLS*).

> **Tip**: Para más información sobre TLS, refiera al RFC 3207.

> **Note**: Este documento describe cómo instalar los Certificados en el cluster llano con el uso de la característica de la *administración centralizada* en el ESA. Los Certificados pueden ser aplicados en el nivel de equipo también; sin embargo, si la máquina se quita del cluster y después se agrega nunca detrás, los Certificados del nivel de equipo serán perdidos.

### Descripción general funcional y requisitos

Un administrador pudo desear de crear un certificado autofirmado en el dispositivo por ninguno de estos razones:

- Para cifrar las conversaciones SMTP con el otro MTAs que utilizan TLS (conversaciones entrantes y salientes)
- Para habilitar el servicio HTTPS en el dispositivo para el acceso al GUI vía el HTTPS
- Para el uso como certificado del cliente para los protocolos lightweight directory access (LDAP), si el servidor LDAP requiere un certificado del cliente
- Para permitir la comunicación segura entre el dispositivo y el administrador de empresa del Rivest-Shamir-Addleman (RSA) para la protección de la pérdida de datos (DLP)
- Para permitir la comunicación segura entre el dispositivo y un dispositivo avanzado de la rejilla de la amenaza de la protección de Cisco Malware (AMP)

El ESA viene preconfigurado con un certificado de la demostración que se pueda utilizar para establecer las conexiones TLS.

> **Caution**: Mientras que el certificado de la demostración es suficiente para el establecimiento de una conexión TLS segura, sea consciente que no puede ofrecer una conexión comprobable.

Cisco recomienda que usted obtiene un X.509, o certificado aumentado aislamiento del correo electrónico (PEM) de CA. Esto se pudo también referir como certificado de *Apache*. El certificado de CA es deseable sobre el certificado autofirmado porque un certificado autofirmado es similar al certificado previamente mencionado de la demostración, que no puede ofrecer una conexión comprobable.

> **Note**: El formato del certificado PEM se define más a fondo en el RFC 1421 con el RFC 1424. El PEM es un formato del envase que puede incluir solamente el certificado público (por ejemplo con Apache instala y los archivos */etc/ssl/certs del* certificado de CA) o una Cadena de certificados entera, para incluir la clave pública, la clave privada, y los certificados raíz. El nombre *PEM* es de un método fallado para el correo electrónico seguro, pero el formato del envase que utilizó sigue siendo active y es una traducción del base 64 de las claves X.509 ASN.1.

#### Traiga su propio certificado

La opción para importar su propio certificado está disponible en el ESA; sin embargo, el requisito es que el certificado esté en el formato del *PKCS-12*. Este formato incluye la clave privada. Los administradores no tienen a menudo Certificados que estén disponibles en este formato. Por este motivo, Cisco recomienda que usted genera el certificado en el ESA y lo hace firmar correctamente por CA.

#### Ponga al día un certificado actual

Si ha expirado un certificado que existe ya, salte la sección de los *certificados autofirmados que despliega de* este documento y re-muestra el certificado que existe.

> **Tip**: Refiera a la renovación un certificado en un documento de Cisco del dispositivo de seguridad del correo electrónico para más detalles.

# Despliegue los certificados autofirmados

Esta sección describe cómo generar un certificado autofirmado y un pedido de firma de certificado (CSR), proporcionar el certificado autofirmado a CA para firmar, cargar el certificado firmado al ESA, especificar el certificado para el uso con los servicios ESA, y sostener la configuración del aparato y los certificados.

## Genere un certificado autofirmado y un CSR

Para crear un certificado autofirmado vía el CLI, ingrese el comando del **certconfig**.

Complete estos pasos para crear un certificado autofirmado del GUI:

1. Navegue al **certificado de la red > de los Certificados > Add del** dispositivo GUI.

2. Haga clic el menú desplegable del **certificado autofirmado del crear**.

   Cuando usted crea el certificado, asegúrese de que el *Common Name* haga juego el nombre de host de la interfaz que escucha, o de que hace juego el nombre de host de la interfaz de la salida.

   La interfaz *que escucha* es la interfaz que se conecta al módulo de escucha que se configura bajo la **red > los módulos de escucha**.

   La interfaz de la *salida* se selecciona automáticamente, a menos que esté configurada explícitamente del CLI con el comando del **deliveryconfig**.
3. Para una conexión hacia adentro comprobable, valide que estos tres elementos hacen juego:

   Registro MX (nombre de host del Domain Name System (DNS))

   Common Name

   Nombre de host de la interfaz

   **Note**: El nombre de host del sistema no afecta a las conexiones TLS con respecto a ser comprobable. El nombre de host del sistema se muestra en la esquina superior derecha del dispositivo GUI, o de la salida de comando del **sethostname** CLI.

   **Caution**: Recuerde **someter** y **confiar** sus cambios antes de que usted exporte el CSR. Si estos pasos no se completan, el nuevo certificado no será confiado a la configuración del aparato, y el certificado firmado de CA no puede firmar, ni se aplique a, un certificado que exista ya.

## Proporcione el certificado autofirmado a CA

Complete estos pasos para presentar el certificado autofirmado a CA para firmar:

1. Salve el CSR a una computadora local en el formato PEM (la **red > certifica > *pedido de firma de certificado de la descarga del* name> del certificado**).

2. Envíe el certificado generado a CA reconocido para firmar.

3. Pida X.509/PEM/Apache un certificado formatado el certificado intermedio, así como.

CA entonces genera un certificado en el formato PEM.

**Note**: Para una lista de proveedores de CA, refiera al artículo de Wikipedia del Certificate Authority.

## Cargue el certificado firmado al ESA

Después de que CA devuelva el certificado público de confianza que es firmado por una clave privada, usted debe cargar el certificado firmado al ESA. El certificado se puede entonces utilizar con un módulo de escucha público o privado, un servicio de la interfaz IP HTTPS, la interfaz LDAP, o todas las conexiones TLS salientes a los dominios del destino.

Complete estos pasos para cargar el certificado firmado al ESA:

1. Asegúrese de que el certificado público de confianza que es formato recibido de las aplicaciones PEM, o un formato que se pueda convertir al PEM antes de que usted lo cargue al dispositivo. **Tip**: Usted puede utilizar el OpenSSLtoolkit, un programa del software gratuito, para convertir el formato.
2. Cargue el certificado firmado:

   Navegue a la **red > a los Certificados**.

   Haga clic el nombre del certificado que fue enviado a CA para firmar.

   Ingrese la trayectoria al archivo en el volumen de la máquina local o de la red.

   **Note**: Cuando usted carga el nuevo certificado, sobregraba el certificado actual. Un certificado intermedio que se relaciona con el certificado autofirmado puede también ser cargado.

   **Caution**: Recuerde **someter** y **confiar los** cambios después de que usted cargue el certificado firmado.

## Especifique el certificado para el uso con los servicios ESA

Ahora que el certificado se crea, se firma, y está cargado al ESA, puede ser utilizado para los servicios que requieren el uso del certificado.

### TLS entrante

Complete estos pasos para utilizar el certificado para los servicios entrantes de TLS:

1. Navegue a la **red > a los módulos de escucha**.
2. Haga clic el nombre del módulo de escucha.
3. Seleccione el nombre del certificado del menú desplegable del *certificado*.
4. Haga clic en Submit (Enviar).
5. Relance los pasos 1 a 4 según las necesidades para cualquier módulo de escucha adicional.
6. **Confíe los** cambios.

### TLS saliente

Complete estos pasos para utilizar el certificado para los servicios salientes de TLS:

1. Navegue **para enviar las directivas > los controles del destino**.
2. El tecleo **edita las configuraciones globales…** en la sección de las *configuraciones globales*.
3. Seleccione el nombre del certificado del menú desplegable del *certificado*.
4. Haga clic en Submit (Enviar).
5. **Confíe los** cambios.

### HTTPS

Complete estos pasos para utilizar el certificado para los servicios HTTPS:

1. Navegue a la **red > a las interfaces IP**.
2. Haga clic el nombre de la interfaz.
3. Seleccione el nombre del certificado del menú desplegable del *certificado HTTPS*.
4. Haga clic en Submit (Enviar).
5. Relance los pasos 1 a 4 según las necesidades para cualquier interfaz adicional.
6. **Confíe los** cambios.

### LDAP

Complete estos pasos para utilizar el certificado para los LDAP:

1. Navegue a la **administración del sistema > al LDAP**.
2. El tecleo **edita las configuraciones…** en la sección de las *configuraciones globales LDAP*.
3. Seleccione el nombre del certificado del menú desplegable del *certificado*.
4. Haga clic en Submit (Enviar).
5. **Confíe los** cambios.

### Filtrado de URL

Complete estos pasos para utilizar el certificado para el Filtrado de URL:

1. Ingrese el comando del **websecurityconfig** en el CLI.

2. Proceda con los prompts de comando. Asegúrese de que usted seleccione **Y** cuando usted alcanza este prompt:

```
Do you want to set client certificate for Cisco Web Security Services Authentication?
```

3. Seleccione el número que se asocia al certificado.

4. Ingrese el **comando commit** para confiar los cambios de configuración.

### Sostenga la configuración del aparato y los certificados

Asegúrese de que la configuración del aparato esté guardada ahora. La configuración del aparato contiene el trabajo completado del certificado que se ha aplicado vía los procesos previamente descritos.

Complete estos pasos para salvar el archivo de configuración del aparato:

1. Navegue al **archivo de la administración del sistema > del archivo de configuración > de la descarga a la computadora local a ver o a salvar**.

2. Exporte el certificado:

   Navegue a la **red > a los Certificados**.

   Haga clic el **certificado de exportación**.

   Seleccione el certificado para exportar.

   Ingrese el nombre del archivo del certificado.

   Ingrese una contraseña para el archivo de certificado.

   Haga clic la **exportación**.

   Salve el archivo a un local o a una máquina de la red.

   Los Certificados adicionales se pueden exportar ahora, o la **cancelación del** tecleo para volver a la **red > certifica la** ubicación.

   **Note**: Este proceso guarda el certificado en el formato del PKCS-12, que crea y salva el archivo con la protección de la contraseña.

## Active TLS entrante

Para activar TLS para todas las sesiones entrantes, conecte con la red GUI, elija las **directivas del correo > las directivas del flujo de correo** para el módulo de escucha entrante configurado, y después complete estos pasos:

1. Elija a un módulo de escucha para quien las directivas deban ser modificadas.

2. Haga clic el link para el nombre de la directiva para editarla.

3. En las *funciones de seguridad* seccione, elija uno de estos *cifrado y las opciones de autenticación* para fijar el nivel de TLS que se requiere para ese módulo de escucha y directiva del flujo de correo:

   **De** – Cuando se elige esta opción, TLS no se utiliza.

   **Preferido** – Cuando se elige esta opción, TLS puede negociar del MTA del telecontrol al ESA. Sin embargo, si el MTA del telecontrol no negocia (antes de la recepción de una respuesta *220*), la transacción SMTP continúa *en el claro* (no cifrado). No se hace ninguna tentativa para verificar si el certificado origina de un Certificate Authority de confianza. Si ocurre un error después de que se reciba la respuesta 220, después la transacción SMTP no recurre al texto claro.

   **Requerido** – Cuando se elige esta opción, TLS se puede negociar del MTA del telecontrol al ESA. No se hace ninguna tentativa para verificar el certificado del dominio. Si la negociación falla, no se envía ningún correo electrónico a través de la conexión. Si la negociación tiene éxito, después el correo se entrega vía una sesión encriptada.
4. Haga clic en Submit (Enviar).

5. Haga clic el botón de los **cambios del cometer**. Usted puede agregar un comentario opcional ahora, si está deseado.

6. **Cambios del cometer del** tecleo para salvar los cambios.

La directiva del flujo de correo para el módulo de escucha ahora se pone al día con las configuraciones de TLS que usted ha elegido.

Complete estos pasos para activar TLS para las sesiones entrantes que llegan de un conjunto selecto de los dominios:

1. Conecte con la red GUI y elija las **directivas del correo > la descripción del SOMBRERO**.

2. Agregue los remitentes al grupo apropiado del remitente.

3. Edite las configuraciones de TLS de la directiva del flujo de correo que se asocia al grupo del remitente que usted modificó en el paso anterior.

4. Haga clic en Submit (Enviar).

5. Haga clic el botón de los **cambios del cometer**. Usted puede agregar un comentario opcional ahora, si está deseado.

6. **Cambios del cometer del** tecleo para salvar los cambios.

La directiva del flujo de correo para el grupo del remitente ahora se pone al día con las configuraciones de TLS que usted ha elegido.

**Tip**: Refiera al artículo siguiente para más información sobre cómo el ESA maneja la verificación de TLS: ¿Cuál es el algoritmo para la verificación del certificado en el ESA?

# Active TLS saliente

Para activar TLS para las sesiones de salida, conecte con la red GUI, elija las **directivas del correo > los controles del destino**, y después complete estos pasos:

1. El tecleo **agrega el destino….**

2. Agregue el dominio del destino (tal como *domain.com*).

3. En la *sección de soporte de TLS*, haga clic el menú desplegable y elija una de estas opciones para habilitar el tipo de TLS que debe ser configurado:

   **Ninguno** – Cuando se elige esta opción, TLS no se negocia para las conexiones salientes de la interfaz al MTA para el dominio.

   **Preferido** – Cuando se elige esta opción, TLS se negocia de la interfaz ESA al MTA para el dominio. Sin embargo, si la negociación de TLS falla (antes de la recepción de una respuesta 220), la transacción SMTP continúa *en el claro* (no cifrado). No se hace ninguna tentativa para verificar si el certificado origina de CA de confianza. Si ocurre un error después de que se reciba la respuesta 220, después la transacción SMTP no recurre al texto claro.

   **Requerido** – Cuando se elige esta opción, TLS se negocia de la interfaz ESA al MTA para el dominio. No se hace ninguna tentativa para verificar el certificado del dominio. Si la negociación falla, no se envía ningún correo electrónico a través de la conexión. Si la negociación tiene éxito, después el correo se entrega vía una sesión encriptada.

   **Preferir-verifique** – Cuando se elige esta opción, TLS se negocia del ESA al MTA para el dominio, y de las tentativas del dispositivo de verificar el certificado del dominio. En este caso, estos tres resultados son posibles:

   Se negocia TLS y se verifica el certificado. El correo se entrega vía una sesión encriptada.

   Se negocia TLS, pero el certificado no se verifica. El correo se entrega vía una sesión encriptada.

   No se hace ninguna conexión TLS, y el certificado no se verifica. El correo electrónico se entrega en el sólo texto.**Requerir-verifique** – Cuando se elige esta opción, TLS se negocia del ESA al MTA para el dominio, y la verificación del certificado del dominio se requiere. En este caso, estos tres resultados son posibles:

   Se negocia una conexión TLS, y se verifica el certificado. El correo electrónico se entrega vía una sesión encriptada.

Se negocia una conexión TLS, pero el certificado no es verificado por CA de confianza. El correo no se entrega.

Una conexión TLS no se negocia, pero el correo no se entrega.

4. Realice más lejos los cambios que son necesarios los *controles del destino* para el dominio del destino.

5. Haga clic en Submit (Enviar).

6. Haga clic el botón de los **cambios del cometer**. Usted puede agregar un comentario opcional ahora, si está deseado.

7. **Cambios del cometer del** tecleo para salvar los cambios.

# Troubleshooting

Esta sección describe cómo resolver problemas los problemas básicos de TLS en el ESA.

## Certificados intermedios

Usted debe buscar los Certificados intermedios duplicados, especialmente cuando los Certificados actuales son actualizados en vez de una nueva creación del certificado. Los certificados intermedios pudieron haber cambiado, o pudieron haber sido encadenados incorrectamente, y el certificado pudo haber cargado los Certificados intermedios múltiples. Esto puede introducir los problemas del encadenamiento y de la verificación del certificado.

## Notificaciones del permiso para los errores requeridos de la conexión TLS

Usted puede configurar el ESA para enviar una alerta si la negociación de TLS falla cuando los mensajes se entregan a un dominio que requiera una conexión TLS. El mensaje de alerta contiene el nombre del dominio del destino para la negociación fallada de TLS. El ESA envía el mensaje de alerta a todos los beneficiarios que se fijen para recibir las alertas amonestadoras del nivel de gravedad para los tipos de la alerta del *sistema*.

**Note**: Esto es una configuración global, así que no puede ser fijada sobre una base del por-dominio.

Complete estos pasos para habilitar las alertas de la conexión TLS:

1. Navegue **para enviar las directivas > los controles del destino**.

2. El tecleo **edita las configuraciones globales**.

3. Marque el **envío una alerta cuando una conexión TLS requerida falla la** casilla de verificación.

**Tip**: Usted puede también configurar esta configuración con el **destconfig >** comando CLI **puesto**.

El ESA también registra los casos para los cuales TLS se requiere para un dominio pero no se podría utilizar en los registros del correo del dispositivo. Esto ocurre cuando se cumplen ninguno de estos condiciones:

- El MTA del telecontrol no soporta el ESMTP (por ejemplo, no entendía el *comando EHLO del* ESA).
- El MTA del telecontrol soporta el ESMTP, pero el comando *STARTTLS* no estaba en la lista de Extensiones de que hizo publicidad en su *EHLO* respuesta.
- El MTA del telecontrol hizo publicidad de la extensión *STARTTLS* pero respondió con un error cuando el ESA envió el comando *STARTTLS*.

## Localice a las sesiones de comunicación acertadas de TLS en los registros del correo

Las conexiones TLS se registran en los registros del correo, junto con otras acciones significativas que se relacionen con los mensajes, tales como acciones del filtro, contra virus y veredictos del anti-Spam, y las tentativas de la salida. Si hay una conexión TLS acertada, habrá una entrada del *éxito de* TLS en los registros del correo. Asimismo, una conexión TLS fallada produce una entrada *fallada* TLS. Si un mensaje no tiene una entrada asociada de TLS en el archivo del registro, ese mensaje no fue entregado sobre una conexión TLS.

> **Tip**: Para entender los registros del correo, refiera al documento de Cisco de la determinación de la disposición del mensaje ESA.

Aquí está un ejemplo de una conexión TLS acertada del host remoto (recepción):

```
Wed Jul 20 19:47:40 2005 Info: New smtp ICID 282204970 interface mail.example.com
(10.2.3.4) address 10.3.4.5 reverse dns host unknown verified no
Wed Jul 20 19:47:40 2005 Info: ICID 282204970 ACCEPT SG None match SBRS None
Wed Jul 20 19:47:40 2005 Info: ICID 282204970 TLS success
Wed Jul 20 19:47:40 2005 Info: Start MID 200257070 ICID 282204970
```

Aquí está un ejemplo de una conexión TLS fallada del host remoto (recepción):

```
Tue Jun 28 19:08:49 2005 Info: New SMTP ICID 282204971 interface Management
(10.2.3.4) address 10.3.4.5 reverse dns host unknown verified no
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 ACCEPT SG None match SBRS None
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 TLS failed
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 lost
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 TLS was required but remote host did
not initiate it
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 close
```

Aquí está un ejemplo de una conexión TLS acertada al host remoto (salida):

```
Tue Jun 28 19:28:31 2005 Info: New SMTP DCID 834 interface 10.10.10.100 address
192.168.1.25 port 25
Tue Jun 28 19:28:31 2005 Info: DCID 834 TLS success protocol TLSv1 cipher
DHE-RSA-AES256-SHA
Tue Jun 28 19:28:31 2005 Info: Delivery start DCID 834 MID 1074 to RID [0]
```

Aquí está un ejemplo de una conexión TLS fallada al host remoto (salida):

```
Fri Jul 22 22:00:05 2005 Info: DCID 2386070 IP 10.3.4.5 TLS failed: STARTTLS
unexpected response
```

# Información Relacionada

- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Dispositivo de la Administración de seguridad del contenido de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems