

# Configuración del servidor SMTP seguro en ISE

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuración](#)

[Configuración SMTP](#)

[Configuración de comunicación SMTP no segura sin autenticación o cifrado](#)

[Configuración de comunicación SMTP segura](#)

[Comunicación SMTP segura con cifrado habilitado](#)

[Comunicación SMTP segura con configuración de autenticación habilitada](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo configurar el servidor de protocolo simple de transferencia de correo (SMTP) en Cisco Identity Services Engine (ISE) para admitir notificaciones de correo electrónico para varios servicios. ISE versión 3.0 admite conexiones seguras y no seguras con el servidor SMTP.

Colaborado por Poonam Garg, ingeniero del TAC de Cisco.

## Prerequisites

### Requirements

Cisco recomienda que tenga un conocimiento básico de la funcionalidad de Cisco ISE y del servidor SMTP.

### Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configuración

Esta sección describe la configuración de ISE para soportar las notificaciones de correo electrónico utilizadas para:

- Enviar notificaciones de alarma por correo electrónico a cualquier usuario administrador interno con la opción Inclusión de alarmas del sistema en correos electrónicos activada. La dirección de correo electrónico del remitente para enviar notificaciones de alarma está codificada como ise@<hostname>.
- Habilite a los patrocinadores para que envíen una notificación por correo electrónico a los invitados con sus credenciales de inicio de sesión e instrucciones de restablecimiento de contraseña.
- Permite a los invitados recibir automáticamente sus credenciales de inicio de sesión después de registrarse correctamente y con las acciones que deben realizar antes de que caduquen sus cuentas de invitado.
- Envíe correos electrónicos recordatorios a los usuarios administradores de ISE/usuarios de red internos configurados en ISE antes de la fecha de vencimiento de la contraseña.

## Configuración SMTP

Antes de que ISE pueda utilizar cualquier servicio de correo electrónico, debe tener configurado un servidor de retransmisión SMTP. Para actualizar los detalles del servidor SMTP, navegue hasta **Administration > System > Settings > Proxy > SMTP server**.

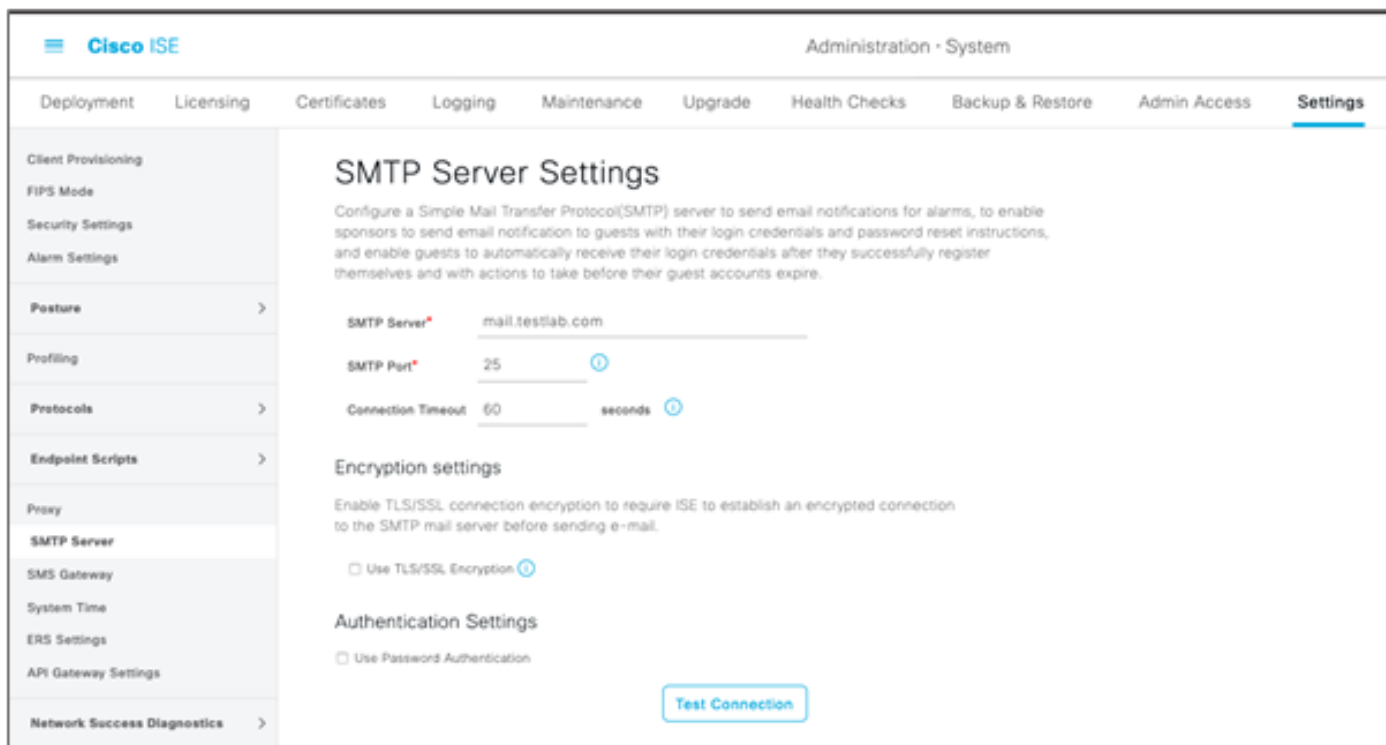
Esta tabla muestra qué nodo de un entorno ISE distribuido envía un correo electrónico.

Objetivo de correo electrónico	Nodo que envía el correo electrónico
Vencimiento de la cuenta de invitado	PAN principal
Alarmas	MnT activo
Notificaciones de cuentas de patrocinador y invitado de los portales respectivos	PSN
Vencimiento de contraseña	PAN principal

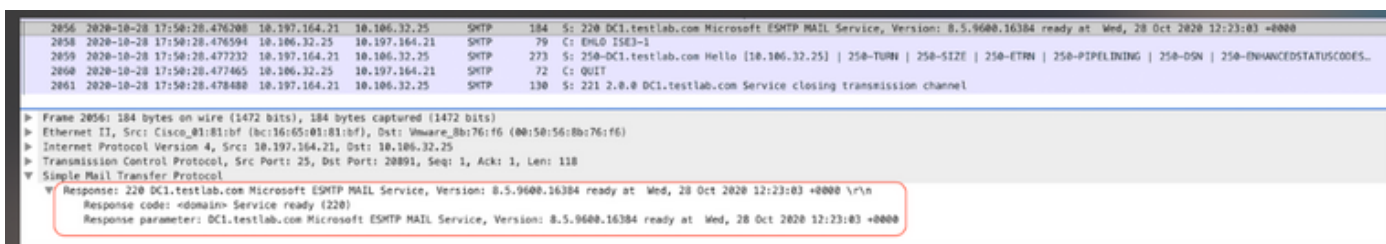
Configure el servidor SMTP para tener la capacidad de aceptar cualquier correo electrónico del ISE con o sin autenticación o cifrado según sus requerimientos.

### Configuración de comunicación SMTP no segura sin autenticación o cifrado

1. Defina el nombre de host del servidor SMTP (servidor SMTP saliente).
2. Puerto SMTP (este puerto debe estar abierto en la red para conectarse al servidor SMTP).
3. Tiempo de espera de conexión (introduzca el tiempo máximo que Cisco ISE espera una respuesta del servidor SMTP).
4. Haga clic en **Probar conexión** y Guardar.



La captura de paquetes muestra la comunicación de ISE con el servidor SMTP sin autenticación ni cifrado:



## Configuración de comunicación SMTP segura

La conexión segura se puede realizar de dos maneras:

1. Basado en SSL
2. Nombre de usuario/basado en contraseña

El servidor SMTP utilizado debe soportar la autenticación basada en SSL y Credentials. La comunicación SMTP segura se puede utilizar con cualquiera de las opciones o con ambas activadas simultáneamente.

### Comunicación SMTP segura con cifrado habilitado

1. Importar certificado de CA raíz del certificado del servidor SMTP en los certificados de confianza de ISE con uso: **Confiar en la autenticación dentro de ISE y Confiar en la autenticación del cliente y Syslog.**
2. Configure el servidor SMTP, el puerto configurado en el servidor SMTP para la comunicación cifrada, y verifique la opción **Use TLS/SSL encryption.**

- Certificate Management
- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Se...

Certificate Authority

Issuer

\* Friendly Name mail.cisco.com

Status  Enabled

Description

Subject CN=mail.cisco.com,O=Cisco Systems, Inc.,L=San Jose,ST=California,C=US

Issuer CN=HydrantID SSL ICA G2,D=HydrantID (Avalanche Cloud Corporation),C=US

Valid From Mon, 6 Apr 2020 12:48:24 UTC

Valid To (Expiration) Wed, 6 Apr 2022 12:58:00 UTC

Serial Number 08 20 2F 3A 96 C4 5F FB 22 52 1F 23 63 87 E6 48 6E 14 99 80

Signature Algorithm SHA256WITHRSA

Key Length 2048

Usage

- Trusted For: ⓘ
- Trust for authentication within ISE
  - Trust for client authentication and Syslog
  - Trust for certificate based admin authentication
  - Trust for authentication of Cisco Services

Probar conexión muestra una conexión correcta con el servidor SMTP.

Administration · System

Certificates Logging Maintenance Upgr

## SMTP Server Settings

Configure a Simple Mail Transfer Protocol(SMTP) server to allow system administrators to send email notification to guests with their login credentials and enable guests to automatically receive their login credentials themselves and with actions to take before their guest access.

SMTP Server\* mail.testlab.com

SMTP Port\* 25 ⓘ

Connection Timeout 60 seconds ⓘ

### Encryption settings

Enable TLS/SSL connection encryption to require ISE to establish an encrypted connection to the SMTP mail server before sending e-mail.

Use TLS/SSL Encryption ⓘ

### Authentication Settings

Use Password Authentication

Test Connection

**i**

**Information**

**Test Connection to SMTP Server**

Successfully connected to mail.testlab.com .

OK

Las capturas de paquetes muestran que el servidor ha aceptado la opción **STARTTLS** según lo solicitado por el ISE.

No.	Time	Source	Destination	Protocol	Len	Info
838	2020-10-28 18:49:25.415546	10.197.164.21	10.106.32.25	SMTP	184	S: 220 DC1.testlab.com Microsoft ESMTS MAIL Service, Version: 8.5.9600.16384 ready at Wed, 28 Oct 2020 13:22:00 +0000
832	2020-10-28 18:49:25.415868	10.106.32.25	10.197.164.21	SMTP	79	C: EHLO ISE3-1
833	2020-10-28 18:49:25.416551	10.197.164.21	10.106.32.25	SMTP	305	S: 250-DC1.testlab.com Hello [10.106.32.25]   250-AUTH=LOGIN   250-AUTH LOGIN   250-TURN   250-SIZE   250-ETRN   250-PIPELINING
834	2020-10-28 18:49:25.416650	10.106.32.25	10.197.164.21	SMTP	76	C: STARTTLS
835	2020-10-28 18:49:25.419256	10.197.164.21	10.106.32.25	SMTP	95	S: 220 2.0.0 SMTP server ready

```

> Frame 835: 95 bytes on wire (760 bits), 95 bytes captured (760 bits)
> Ethernet II, Src: Cisco_01:81:bf (bc:16:65:01:81:bf), Dst: Vmware_Bb:76:f6 (00:50:56:0b:76:f6)
> Internet Protocol Version 4, Src: 10.197.164.21, Dst: 10.106.32.25
> Transmission Control Protocol, Src Port: 25, Dst Port: 31529, Seq: 358, Ack: 24, Len: 29
> Simple Mail Transfer Protocol
  > Response: 220 2.0.0 SMTP server ready\r\n
    Response code: <domain> Service ready (220)
    Response parameter: 2.0.0 SMTP server ready
  
```

### Comunicación SMTP segura con configuración de autenticación habilitada

1. Configure el servidor SMTP y el puerto SMTP.
2. En Authentication Settings (Parámetros de autenticación), verifique la opción **Use Password Authentication (Usar autenticación de contraseña)** y proporcione el nombre de usuario y la contraseña.

Conexión de **prueba** correcta cuando funciona la autenticación basada en contraseña :

Administration · System

Certificates   Logging   Maintenance   Upgr

## SMTP Server Settings

Configure a Simple Mail Transfer Protocol(SMTP) server to allow sponsors to send email notification to guests with their login and enable guests to automatically receive their login credentials themselves and with actions to take before their guest activation.

SMTP Server\*

SMTP Port\*  ⓘ

Connection Timeout  seconds ⓘ

### Encryption settings

Enable TLS/SSL connection encryption to require ISE to establish an encrypted connection to the SMTP mail server before sending e-mail.

Use TLS/SSL Encryption ⓘ

### Authentication Settings

Use Password Authentication

User Name\*

Password\*

[Test Connection](#)

Information

**Test Connection to SMTP Server**

Successfully connected to mail.testlab.com .

[OK](#)

Ejemplo de captura de paquetes que muestra una autenticación exitosa con credenciales:

No.	Time	Source	Destination	Protocol	Leng	Info
1631	2020-10-28 18:43:13.671815	10.197.164.21	10.106.32.25	SMTP	184	S: 220 DC1.testlab.com Microsoft ESMTA MAIL Service, Version: 0.5.9000.10384 ready at Wed, 28 Oct 2020 13:15:48 +0000
1633	2020-10-28 18:43:13.671279	10.106.32.25	10.197.164.21	SMTP	79	C: EHLO ISE3-1
1634	2020-10-28 18:43:13.671925	10.197.164.21	10.106.32.25	SMTP	305	S: 250-DC1.testlab.com Hello [10.106.32.25]   250-AUTH=LOGIN   250-AUTH LOGIN   250-TURN   250-SIZE   250-ETRN   250-PIPELINING  ...
1635	2020-10-28 18:43:13.672058	10.106.32.25	10.197.164.21	SMTP	78	C: AUTH LOGIN
1636	2020-10-28 18:43:13.672652	10.197.164.21	10.106.32.25	SMTP	84	S: 334 VxNlcnShobMUG
1637	2020-10-28 18:43:13.672793	10.106.32.25	10.197.164.21	SMTP	80	C: User: cG9vbnRhdncnc=
1638	2020-10-28 18:43:13.673429	10.197.164.21	10.106.32.25	SMTP	84	S: 334 UGFzc3dvccnDQ6
1639	2020-10-28 18:43:13.673474	10.106.32.25	10.197.164.21	SMTP	80	C: Pass: DyFzY2BxMjM=
1640	2020-10-28 18:43:13.673862	10.197.164.21	10.106.32.25	SMTP	103	S: 235 2.7.0 Authentication successful
1641	2020-10-28 18:43:13.677271	10.106.32.25	10.197.164.21	SMTP	72	C: QUIT
1642	2020-10-28 18:43:13.677986	10.197.164.21	10.106.32.25	SMTP	138	S: 221 2.0.0 DC1.testlab.com Service closing transmission channel

▶ Frame 1640: 103 bytes on wire (824 bits), 103 bytes captured (824 bits)  
 ▶ Ethernet II, Src: Cisco\_81:81:bf (bc:16:65:01:81:bf), Dst: Vmware\_8b:76:f6 (00:50:56:8b:76:f6)  
 ▶ Internet Protocol Version 4, Src: 10.197.164.21, Dst: 10.106.32.25  
 ▶ Transmission Control Protocol, Src Port: 25, Dst Port: 30267, Seq: 394, Ack: 54, Len: 37  
 ▼ Simple Mail Transfer Protocol  
 Response: 235 2.7.0 Authentication successful\r\n  
 Response code: Authentication successful (235)  
 Response parameter: 2.7.0 Authentication successful

## Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

1. Utilice la opción Test Connection para verificar la conectividad con el servidor SMTP

configurado.

- Envíe un correo electrónico de prueba desde el portal de invitados en **Centros de trabajo > Acceso de invitado > Portales y componentes > Portales de invitados > Portal de invitado registrado automáticamente(predeterminado) > Personalización de la página del portal > Notificaciones > Correo electrónico > Configuración de la ventana de vista previa**, introduzca una dirección de correo electrónico válida y envíe correo electrónico de prueba. El destinatario debe recibir el correo electrónico de la dirección configurada en Configuración de correo electrónico de invitado.

Ejemplo de notificación de correo electrónico enviada para credenciales de cuenta de invitado:

Time	Source	Destination	Protocol	Len	Address	Info
2475	2020-10-26 18:51:33.867597	173.37.182.6	SMTP	151	00:50:56:0b:76:f6, bc:16:65:01:81:bf	S: 220 vch-rcd-001.cisco.com Microsoft ESMTS MAIL Service ready at Mon, 26 Oct 2020 08:24:07 -0500
2477	2020-10-26 18:51:33.867908	18.186.32.25	SMTP	67	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: ENCL ESE3-1
2494	2020-10-26 18:51:34.136372	173.37.182.6	SMTP	299	00:50:56:0b:76:f6, bc:16:65:01:81:bf	S: 250-SIZE 37748736   250-PIPELINING   250-DSN   250-ENHANC
2495	2020-10-26 18:51:34.136729	18.186.32.25	SMTP	83	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: MAIL FROM:<is@testlab.com>
2513	2020-10-26 18:51:34.405187	173.37.182.6	SMTP	75	00:50:56:0b:76:f6, bc:16:65:01:81:bf	S: 250 2.1.0 Sender OK
2514	2020-10-26 18:51:34.405472	18.186.32.25	SMTP	84	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: RCPT TO:<pongarg@cisco.com>
2522	2020-10-26 18:51:34.614367	173.37.182.6	SMTP	78	00:50:56:0b:76:f6, bc:16:65:01:81:bf	S: 250 2.1.5 Recipient OK
2523	2020-10-26 18:51:34.614586	18.186.32.25	SMTP	60	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA
2532	2020-10-26 18:51:34.943137	173.37.182.6	SMTP	180	00:50:56:0b:76:f6, bc:16:65:01:81:bf	S: 354 Start mail input; end with <CRLF>.<CRLF>
2533	2020-10-26 18:51:34.951891	18.186.32.25	SMTP	2714	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA Fragment, 2660 bytes
2534	2020-10-26 18:51:34.951932	18.186.32.25	SMTP	2714	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA Fragment, 2660 bytes
2535	2020-10-26 18:51:34.951932	18.186.32.25	SMTP	2714	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA Fragment, 2660 bytes
2536	2020-10-26 18:51:34.952189	18.186.32.25	SMTP	199	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA Fragment, 145 bytes
2537	2020-10-26 18:51:34.958436	18.186.32.25	SMTP	2714	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA Fragment, 2660 bytes
2560	2020-10-26 18:51:35.220463	18.186.32.25	SMTP	2714	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA Fragment, 2660 bytes
2561	2020-10-26 18:51:35.220480	18.186.32.25	SMTP	2714	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA Fragment, 2660 bytes
2563	2020-10-26 18:51:35.220783	18.186.32.25	SMTP	2714	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA Fragment, 2660 bytes
2564	2020-10-26 18:51:35.220793	18.186.32.25	SMTP	2714	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA Fragment, 2660 bytes
2566	2020-10-26 18:51:35.220878	18.186.32.25	SMTP	784	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	From: <is@testlab.com>, subject: Your Guest Account Credentials, (text/html) (image/png)
2583	2020-10-26 18:51:35.597164	173.37.182.6	SMTP	186	00:50:56:0b:76:f6, bc:16:65:01:81:bf	S: 250 2.6.0 <366327480.7.1603718485230@ISE3-1> [InternalId=201137613468157, Hostname=ECN-ALN-001.cisco.com]
2584	2020-10-26 18:51:35.597441	18.186.32.25	SMTP	60	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: QUIT
2595	2020-10-26 18:51:35.865758	173.37.182.6	SMTP	102	00:50:56:0b:76:f6, bc:16:65:01:81:bf	S: 221 2.0.0 Service closing transmission channel

```

Frame 2522: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: Cisco_01:81:bf (bc:16:65:01:81:bf), Dst: Vmware_0b:76:f6 (00:50:56:0b:76:f6)
Internet Protocol Version 4, Src: 173.37.182.6, Dst: 18.186.32.25
Transmission Control Protocol, Src Port: 25, Dst Port: 22003, Seq: 364, Ack: 73, Len: 24
Sample Mail Transfer Protocol
Response: 250 2.1.5 Recipient OK\r\n
Response code: Requested mail action okay, completed (250)
Response parameter: 2.1.5 Recipient OK
    
```

Ejemplo de notificación por correo electrónico recibida por destinatario de correo electrónico:

# Your Guest Account Credentials



ise@testlab.com <ise@testlab.com>

To: Poonam Garg (poongarg)



Hello firstname,  
Your guest account details:  
Username: username  
Password: password  
First Name: firstname  
Last Name: lastname  
Mobile Number:NA  
Valid From: 2014-11-12 02:06:00  
Valid To: 2016-11-12 02:06:00  
Person being visited:  
Reason for visit:

## Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración:

Problema: La conexión de prueba muestra: "No se pudo conectar con el servidor SMTP, Error SSL. Compruebe los certificados de confianza".





La captura de paquetes muestra que el certificado presentado por el servidor SMTP no es de confianza:

The image shows a network traffic capture with several rows of data. The row for frame 1710 is highlighted in blue. Below the table, there is a detailed view of the TLS alert message, with the description 'Certificate Unknown (46)' circled in red.

No.	Time	Source	Destination	Protocol	Length	Info
1698	2020-10-28 17:50:22.659934	10.106.32.25	10.197.164.21	TCP	74	20881 -> 25 [SYN] Seq=8 Min=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=462914246 TSecr=0 MS=128
1700	2020-10-28 17:50:22.661340	10.106.32.25	10.197.164.21	TCP	66	20881 -> 25 [ACK] Seq=1 Ack=1 Min=29312 Len=0 TSval=462914248 TSecr=919415203
1702	2020-10-28 17:50:22.662379	10.106.32.25	10.197.164.21	TCP	66	20881 -> 25 [ACK] Seq=1 Ack=119 Min=29312 Len=0 TSval=462914249 TSecr=919415203
1703	2020-10-28 17:50:22.662672	10.106.32.25	10.197.164.21	SMTP	79	C: EHLO ISE3-1
1705	2020-10-28 17:50:22.665865	10.106.32.25	10.197.164.21	SMTP	76	C: STARTTLS
1707	2020-10-28 17:50:22.667148	10.106.32.25	10.197.164.21	TLSv1.2	238	Client Hello
1709	2020-10-28 17:50:22.680617	10.106.32.25	10.197.164.21	TCP	66	20881 -> 25 [ACK] Seq=196 Ack=2295 Win=34176 Len=0 TSval=462914267 TSecr=919415205
1710	2020-10-28 17:50:22.688448	10.106.32.25	10.197.164.21	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)
1711	2020-10-28 17:50:22.686528	10.106.32.25	10.197.164.21	TCP	66	20881 -> 25 [FIN, ACK] Seq=203 Ack=2295 Win=34176 Len=0 TSval=462914273 TSecr=919415205
1714	2020-10-28 17:50:22.687552	10.106.32.25	10.197.164.21	TCP	66	20881 -> 25 [ACK] Seq=204 Ack=2296 Win=34176 Len=0 TSval=462914274 TSecr=919415206

▼ Frame 1710: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)  
▶ Ethernet II, Src: Vmware\_8b:76:f6 (00:50:56:8b:76:f6), Dst: Cisco\_01:81:bf (bc:16:65:01:81:bf)  
▶ Internet Protocol Version 4, Src: 10.106.32.25, Dst: 10.197.164.21  
▶ Transmission Control Protocol, Src Port: 20881, Dst Port: 25, Seq: 196, Ack: 2295, Len: 7  
▼ Secure Sockets Layer  
▼ TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Certificate Unknown)  
Content Type: Alert (21)  
Version: TLS 1.2 (0x0303)  
Length: 2  
▼ Alert Message  
Level: Fatal (2)  
Description: Certificate Unknown (46)

Solución: Importe el certificado de CA raíz del servidor SMTP en los certificados de confianza de ISE y si el soporte de TLS está configurado en el puerto.

Problema: Test Connection muestra: Falta de autenticación: No se pudo conectar al servidor SMTP, el nombre de usuario o la contraseña son incorrectos.



La captura de paquetes de muestra aquí muestra que la autenticación no fue exitosa.

The image shows a network traffic capture with several rows of data. The row for frame 952 is highlighted in blue. Below the table, there is a detailed view of the SMTP response, with the error message '535 5.7.3 Authentication unsuccessful' circled in red.

No.	Time	Source	Destination	Protocol	Length	Info
938	2020-10-28 18:11:40.722253	10.197.164.21	10.186.32.25	SMTP	184	S: 229 DC1.testlab.com Microsoft ESMTP MAIL Service, Version: 6.5.9600.16384 ready at Wed, 28 Oct 2020 12:44:15 +0800
940	2020-10-28 18:11:40.722653	10.186.32.25	10.197.164.21	SMTP	79	C: EHLO ISE3-1
941	2020-10-28 18:11:40.723363	10.197.164.21	10.186.32.25	SMTP	305	S: 250-DC1.testlab.com Hello [10.186.32.25]   250-AUTH=LOGIN   250-AUTH LOGIN   250-TURN   250-SIZE   250-ETRN   250-PIPELINING
942	2020-10-28 18:11:40.723531	10.186.32.25	10.197.164.21	SMTP	78	C: AUTH LOGIN
946	2020-10-28 18:11:40.729063	10.197.164.21	10.186.32.25	SMTP	84	S: 334 VbWlce5h0w06
949	2020-10-28 18:11:40.729172	10.186.32.25	10.197.164.21	SMTP	76	C: User: dGVzZDQ0=
950	2020-10-28 18:11:40.730056	10.197.164.21	10.186.32.25	SMTP	84	S: 334 UGfzc3dvcnQ6
951	2020-10-28 18:11:40.730151	10.186.32.25	10.197.164.21	SMTP	80	C: Pass: QyFzY28xRjM=
952	2020-10-28 18:11:40.748181	10.197.164.21	10.186.32.25	SMTP	205	S: 535 5.7.3 Authentication unsuccessful

▼ Frame 952: 105 bytes on wire (840 bits), 105 bytes captured (840 bits)  
▶ Ethernet II, Src: Cisco\_01:81:bf (bc:16:65:01:81:bf), Dst: Vmware\_8b:76:f6 (00:50:56:8b:76:f6)  
▶ Internet Protocol Version 4, Src: 10.197.164.21, Dst: 10.186.32.25  
▶ Transmission Control Protocol, Src Port: 25, Dst Port: 24553, Seq: 394, Ack: 58, Len: 39  
▼ Simple Mail Transfer Protocol  
▼ Response: 535 5.7.3 Authentication unsuccessful\r\nResponse code: Authentication credentials invalid (535)  
Response parameter: 5.7.3 Authentication unsuccessful

Solución: Valide el nombre de usuario o la contraseña configurados en el servidor SMTP.

Problema: Test Connection muestra: Error en la conexión al servidor SMTP.



Solución: Verifique la configuración del puerto del servidor SMTP, verifique si el nombre del servidor SMTP puede ser resuelto por el servidor DNS configurado en ISE.

El ejemplo aquí muestra que el servidor SMTP envía un reinicio en el puerto 587 que no está configurado para el servicio SMTP.

```
1103 2020-10-28 18:24:18.330613 10.106.32.25 10.197.164.21 DNS 76 Standard query 0x2a06 A mail.testlab.com
1104 2020-10-28 18:24:18.330643 10.106.32.25 10.197.164.21 DNS 76 Standard query 0xde13 AAAA mail.testlab.com
1105 2020-10-28 18:24:18.331978 10.197.164.21 10.106.32.25 DNS 92 Standard query response 0x2a06 A mail.testlab.com A 10.197.164.21
1106 2020-10-28 18:24:18.332020 10.197.164.21 10.106.32.25 DNS 127 Standard query response 0xde13 AAAA mail.testlab.com SOA dcl.testlab.com
1107 2020-10-28 18:24:18.332281 10.106.32.25 10.197.164.21 TCP 74 21243 -> 587 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=464949919 TSecr=0 MS=128
1108 2020-10-28 18:24:18.335520 10.197.164.21 10.106.32.25 TCP 60 587 -> 21243 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1109 2020-10-28 18:24:18.336787 10.106.32.25 10.65.91.198 TLSv1.2 929 Application Data
1110 2020-10-28 18:24:18.362481 Vmware_8b:6e... Broadcast ARP 60 Who has 10.106.32.5? Tell 10.106.32.15

> Frame 1108: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Cisco_01:01:bf (bc:16:65:01:01:bf), Dst: Vmware_8b:76:f6 (08:50:56:8b:76:f6)
> Internet Protocol Version 4, Src: 10.197.164.21, Dst: 10.106.32.25
> Transmission Control Protocol, Src Port: 587, Dst Port: 21243, Seq: 1, Ack: 1, Len: 0
  Source Port: 587
  Destination Port: 21243
  [Stream index: 34]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x014 (RST, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ....0... = Congestion Window Reduced (CWR): Not set
    ....0... = EDN-Echo: Not set
    ....00.. = Urgent: Not set
    ....01... = Acknowledgment: Set
    ....0... = Push: Not set
  > ....0... = Reset: Set
    ....00.. = Syn: Not set
    ....0... = Fin: Not set
  [TCP Flags: .....A-R..]
  Window size value: 0
  [Calculated window size: 0]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0xe949 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
```

## Información Relacionada

- [https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin\\_guide/b\\_ISE\\_admin\\_3\\_0/b\\_ISE\\_admin\\_30\\_basic\\_setup.html#id\\_121735](https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0/b_ISE_admin_30_basic_setup.html#id_121735)
- [Soporte Técnico y Documentación - Cisco Systems](#)