

Configurar o servidor SMTP seguro no ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuração](#)

[Configurações SMTP](#)

[Configurações de comunicação SMTP não seguras sem autenticação ou criptografia](#)

[Configurações de comunicação SMTP segura](#)

[Comunicação SMTP segura com criptografia habilitada](#)

[Comunicação SMTP segura com configurações de autenticação habilitadas](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar o Servidor SMTP (Simple Mail Transfer Protocol) no Cisco Identity Services Engine (ISE) para oferecer suporte a notificações por e-mail para vários serviços. O ISE versão 3.0 suporta conexões seguras e não seguras para o Servidor SMTP.

Contribuído por Poonam Garg, engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha um conhecimento básico da funcionalidade do Cisco ISE e do Servidor SMTP.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configuração

Esta seção descreve a configuração do ISE para oferecer suporte às notificações por e-mail usadas para:

- Envie notificações de alarme por e-mail para qualquer usuário administrador interno com a opção Inclusão de alarmes de sistema em e-mails ativada. O endereço de e-mail do remetente para enviar notificações de alarme está codificado como ise@<hostname>.
- Permite que os patrocinadores enviem uma notificação por e-mail aos convidados com suas credenciais de login e instruções de redefinição de senha.
- Permitir que os convidados recebam automaticamente suas credenciais de login depois que se registrarem com êxito e com ações a serem tomadas antes que suas contas de convidado expirem.
- Enviar e-mails de lembrete para usuários de administrador ISE/usuários de rede interna configurados no ISE antes da data de expiração da senha.

Configurações SMTP

Antes que o ISE possa usar qualquer serviço de e-mail, ele deve ter um servidor de retransmissão SMTP configurado. Para atualizar os detalhes do servidor SMTP, navegue para **Administration > System > Settings > Proxy > SMTP server**.

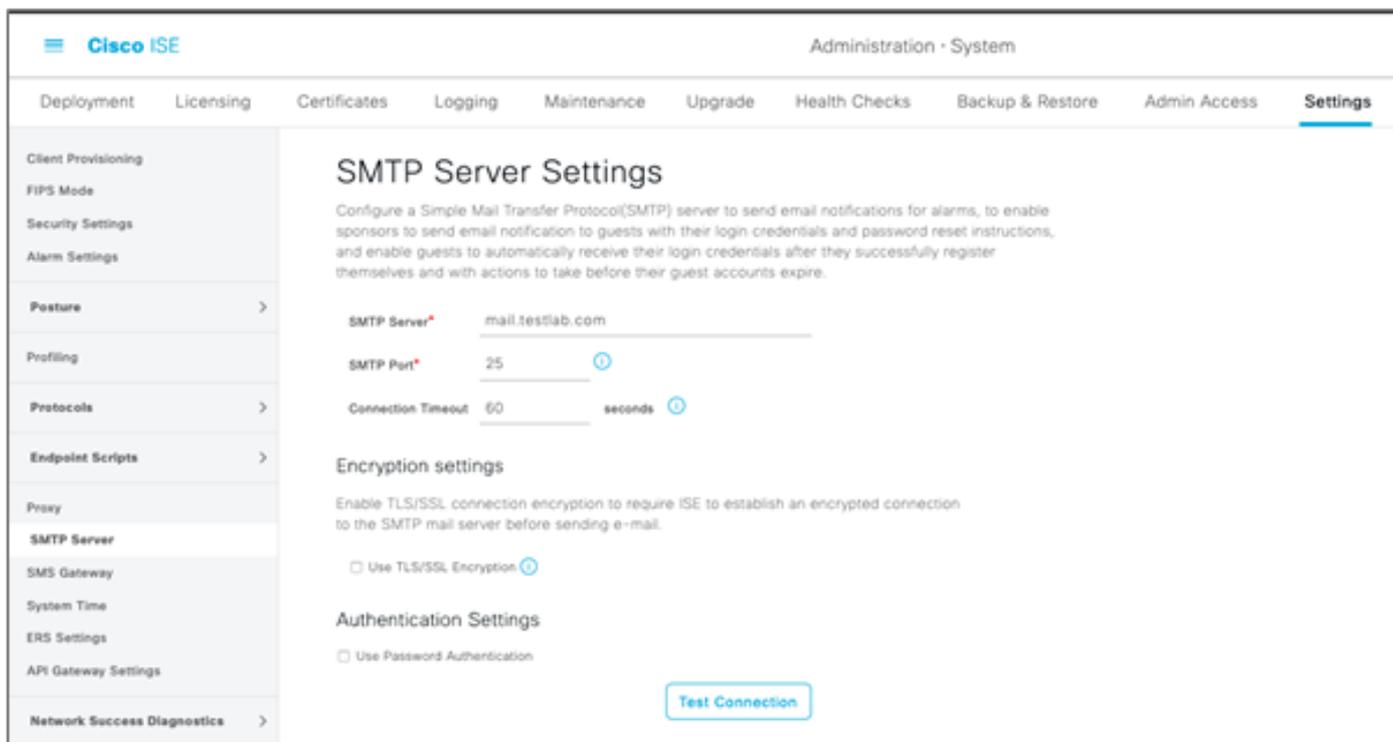
Esta tabela mostra qual nó em um ambiente ISE distribuído envia um e-mail.

Finalidade do e-mail	Nó que envia o e-mail
Expiração da conta de convidado	PAN principal
Alarmes	MnT ativo
Notificações de conta de patrocinador e convidado dos respectivos portais	PSN
Expirações de senha	PAN principal

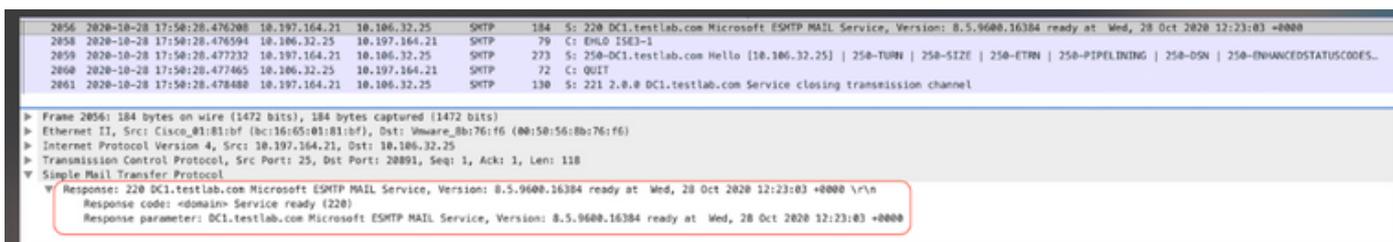
Configure o servidor SMTP para ter a capacidade de aceitar todos os e-mails do ISE com ou sem autenticação ou criptografia com base em seu requisito.

Configurações de comunicação SMTP não seguras sem autenticação ou criptografia

1. Defina o nome de host do Servidor SMTP (servidor SMTP de saída).
2. Porta SMTP (esta porta deve estar aberta na rede para se conectar ao servidor SMTP).
3. Tempo limite da conexão (insira o tempo máximo que o Cisco ISE espera por uma resposta do servidor SMTP).
4. Clique em **Testar conexão** e salvar.



A captura de pacotes mostra a comunicação do ISE com o Servidor SMTP sem autenticação ou criptografia:



Configurações de comunicação SMTP segura

A conexão segura pode ser feita de duas maneiras:

1. Baseado em SSL
2. Baseado em nome de usuário/senha

O Servidor SMTP usado deve suportar autenticação baseada em SSL e Credenciais. A comunicação SMTP segura pode ser usada com uma das opções ou ambas as opções habilitadas simultaneamente.

Comunicação SMTP segura com criptografia habilitada

1. Importar certificado CA raiz do certificado do servidor SMTP nos certificados confiáveis ISE com uso: **Confiança para autenticação no ISE e Trust para autenticação de cliente e Syslog**.
2. Configure o servidor SMTP, a porta configurada no servidor SMTP para comunicação criptografada e marque a opção **Usar criptografia TLS/SSL**.

- 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

Test Connection (Testar conexão) mostra uma conexão bem-sucedida com o Servidor SMTP.

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 credentials and enable guests to automatically receive their login credentials themselves and with actions to take before their guest access.

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

[Test Connection](#)

ⓘ

Information

Test Connection to SMTP Server

Successfully connected to mail.testlab.com .

[OK](#)

As capturas de pacotes mostram que o servidor aceitou a opção **STARTTLS** conforme solicitado pelo 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 ESMT 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
  
```

Comunicação SMTP segura com configurações de autenticação habilitadas

1. Configure o Servidor SMTP e a Porta SMTP.
2. Em Configurações de autenticação, marque a opção **Usar autenticação de senha** e forneça o nome de usuário e a senha.

Êxito ao **Testar Conexão** quando a autenticação baseada em senha funciona:

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 actions.

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](#)

i

Information

Test Connection to SMTP Server

Successfully connected to mail.testlab.com .

[OK](#)

Exemplo de captura de pacote que mostra autenticação bem-sucedida com credenciais:

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 ESMTP MAIL Service, Version: 8.5.9080.10384 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 VVNIcndh0mAG
1637	2020-10-28 18:43:13.672783	10.106.32.25	10.197.164.21	SMTP	80	C: User: c0p@vshdncx=
1638	2020-10-28 18:43:13.673429	10.197.164.21	10.106.32.25	SMTP	84	S: 334 UGFrc3dvccD6
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 18:43:13.677862	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

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

1. Use a opção Testar conexão para verificar a conectividade com o servidor SMTP

configurado.

- Envie um e-mail de teste do portal de convidados em **Centros de Trabalho > Acesso de Convidado > Portais e Componentes > Portais de Convidados > Portal de Convidado Autorregistrado(padrao) > Personalização da página do portal > Notificações > E-mail > Visualizar configurações da janela**, insira um endereço de e-mail válido e envie e e-mail de teste. O destinatário deve receber o e-mail do endereço de e-mail configurado em Configurações de e-mail de convidado.

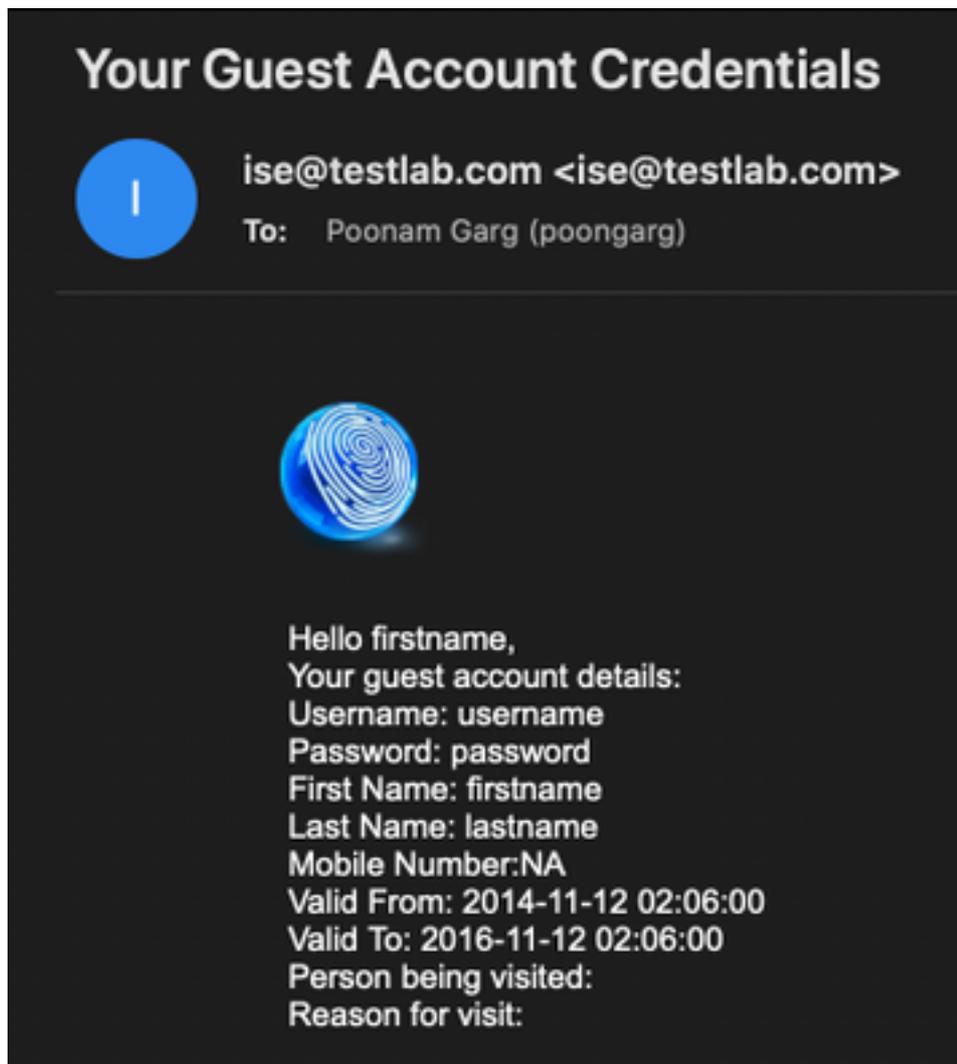
Exemplo de notificação por e-mail enviada para Credenciais de Conta de Convidado:

Time	Source	Destination	Protocol	Len	Address	Info	
2475	2020-10-26 18:51:33.867597	173.37.182.6	18.186.32.25	SMTP	151	00:50:56:0b:76:f6, bc:16:65:01:81:bf	S: 220 xch-rcd-001.cisco.com Microsoft ESMTMP MAIL Service ready at Mon, 26 Oct 2020 00:24:07 -0500
2477	2020-10-26 18:51:33.867980	18.186.32.25	173.37.182.6	SMTP	67	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: EHLO ISE3-1
2494	2020-10-26 18:51:34.136372	173.37.182.6	18.186.32.25	SMTP	299	00:50:56:0b:76:f6, bc:16:65:01:81:bf	S: 250-xch-rcd-001.cisco.com Hello [10.106.32.25] 250-SIZE 37748736 250-PIPELINING 250-DSN 250-ENHANCED MAIL FROM: ise@testlab.com
2495	2020-10-26 18:51:34.136729	18.186.32.25	173.37.182.6	SMTP	83	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: MAIL FROM: ise@testlab.com
2513	2020-10-26 18:51:34.405187	173.37.182.6	18.186.32.25	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	173.37.182.6	SMTP	84	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: RCPT TO: poongarg@cisco.com
2522	2020-10-26 18:51:34.674387	173.37.182.6	18.186.32.25	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 18:51:34.674586	18.186.32.25	173.37.182.6	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	18.186.32.25	SMTP	100	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	173.37.182.6	SMTP	2714	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA Fragment, 2660 bytes
2534	2020-10-26 18:51:34.951927	18.186.32.25	173.37.182.6	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	173.37.182.6	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	173.37.182.6	SMTP	199	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA Fragment, 145 bytes
2537	2020-10-26 18:51:34.950436	18.186.32.25	173.37.182.6	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	173.37.182.6	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	173.37.182.6	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	173.37.182.6	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	173.37.182.6	SMTP	2714	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA Fragment, 2660 bytes
2566	2020-10-26 18:51:35.220870	18.186.32.25	173.37.182.6	SMTP	764	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	From: ise@testlab.com, subject: Your Guest Account Credentials, (text/html) (image/png)
2583	2020-10-26 18:51:35.597144	173.37.182.6	18.186.32.25	SMTP	186	00:50:56:0b:76:f6, bc:16:65:01:81:bf	S: 250 2.6.0 <366327480.7.160371848320q[ISE3-1]@internal09-201137613468157.Hostname=KCH-ALN-001.cisco.com>
2584	2020-10-26 18:51:35.597441	18.186.32.25	173.37.182.6	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	18.186.32.25	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: Vwarc_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: 22083, Seq: 364, Ack: 73, Len: 24
Simple 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
    
```

Exemplo de notificação por e-mail recebida pelo destinatário do e-mail:



Troubleshoot

Esta seção fornece as informações que você pode usar para solucionar problemas de sua configuração:

Problema: A conexão de teste mostra: "Não foi possível conectar ao Servidor SMTP, Erro SSL. Verifique os certificados confiáveis".



A captura de pacote mostra que o certificado apresentado pelo servidor SMTP não é confiável:

```
1698 2020-10-28 17:50:22.659934 10.106.32.25 10.197.164.21 TCP 74 20881 - 25 [SYN] Seq=0 Win=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 Win=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 Win=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 17:50:22.688617 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
1718 2020-10-28 17:50:22.688076 10.106.32.25 10.197.164.21 TLSv1.2 1038 Application Data
▶ 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)
```

Solução: Importar certificado CA raiz do servidor SMTP nos certificados confiáveis ISE e se o suporte TLS estiver configurado na porta.

Problema: Test Connection mostra: Falha de autenticação: Não foi possível conectar ao servidor SMTP, o nome de usuário ou a senha estão incorretos.



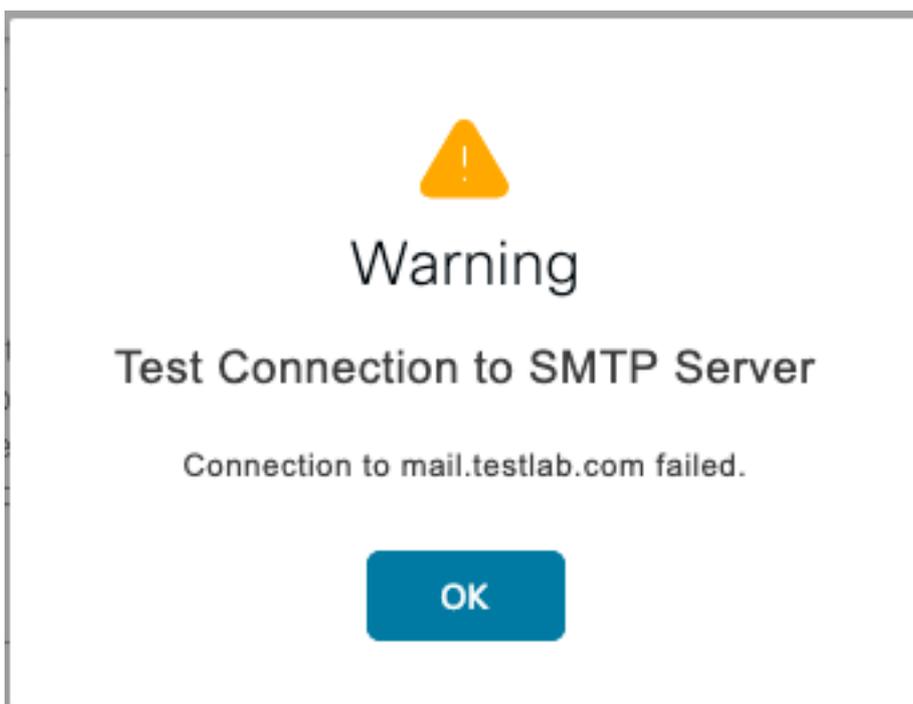
A captura de pacote de exemplo aqui mostra que a autenticação não foi bem-sucedida.

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: 220 DC1.testlab.com Microsoft ESMTPL MAIL Service, Version: 8.5.9600.16384 ready at Wed, 28 Oct 2020 12:44:15 +0000
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 VbVlce5hbw06
949	2020-10-28 18:11:40.729172	10.186.32.25	10.197.164.21	SMTP	76	C: User: dGVzdBQ=
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: QyFzY2BwMjM=
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:b1:bf (bc:16:65:81:b1:bf), Dst: Vmware_00:76:f6 (00:50:56:0b: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: 50, Len: 39
▼ Simple Mail Transfer Protocol
▼ Response: 535 5.7.3 Authentication unsuccessful\r\n
Response code: Authentication credentials invalid (535)
Response parameter: 5.7.3 Authentication unsuccessful

Solução: Valide o nome de usuário ou a senha configurados no servidor SMTP.

Problema: Test Connection mostra: Falha na conexão com o servidor SMTP.



Solução: Verifique a configuração da porta do servidor SMTP. Verifique se o nome do servidor SMTP pode ser resolvido pelo servidor DNS configurado no ISE.

O exemplo aqui mostra que uma redefinição é enviada pelo servidor SMTP na porta 587 que não está configurada para o serviço 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 50A dcl.testlab.com
1107 2020-10-28 18:24:18.332281 10.106.32.25 10.197.164.21 TCP 74 21243 - 587 [STN] Seq= Min=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 68 587 - 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 68 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_01:81:bf (bc:16:65:01:81:bf), Dst: Vmware_8b: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: 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... = ECN-Echo: Not set
  ....0... = Urgent: Not set
  ....01... = Acknowledgment: Set
  ....0... = Push: Not set
▶ ....0... = Reset: Set
  ....0... = 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]
```

Informações Relacionadas

- 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
- [Suporte Técnico e Documentação - Cisco Systems](#)