

Configure Secure SMTP server on ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configuration](#)

[SMTP Settings](#)

[Unsecure SMTP Communication Settings without Authentication or Encryption](#)

[Secure SMTP Communication Settings](#)

[Secure SMTP Communication with Encryption Enabled](#)

[Secure SMTP Communication with Authentication Settings Enabled](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to configure the Simple Mail Transfer Protocol (SMTP) Server on the Cisco Identity Services Engine (ISE) in order to support Email notifications for multiple services. ISE version 3.0 supports both secured and unsecured connections to SMTP Server.

Contributed by Poonam Garg, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have a basic knowledge of the Cisco ISE and SMTP Server functionality.

Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is live, ensure that you understand the potential impact of any command.

Configuration

This section describes the configuration of the ISE in order to support email notifications used to:

- Send email alarm notifications to any internal admin users with the Inclusion of system alarms in emails option enabled. The sender's email address to send alarm notifications is hardcoded as ise@<hostname>.
- Enable sponsors to send an email notification to guests with their log In credentials and password reset instructions.
- Enable guests to automatically receive their log In credentials after they successfully register themselves and with actions to take before their guest accounts expire.
- Send reminder emails to ISE admin users/Internal network users configured on the ISE prior to their password expiration date.

SMTP Settings

Before ISE can use any email services, it must have an SMTP relay server configured. In order to update the SMTP server details, navigate to **Administration > System > Settings > Proxy > SMTP server**.

This table shows which node in a distributed ISE environment sends an email.

Email Purpose	Node that sends the Email
Guest account expiration	Primary PAN
Alarms	Active MnT
Sponsor and Guest account notifications from respective portals	PSN
Password expirations	Primary PAN

Configure the SMTP server in order to have the ability to accept any Emails from the ISE with or without authentication or encryption based on your requirement.

Unsecure SMTP Communication Settings without Authentication or Encryption

1. Define the SMTP Server hostname (outbound SMTP server).
2. SMTP Port (this port must be open in the network to connect to the SMTP server).
3. Connection Timeout (Enter the maximum time Cisco ISE waits for a response from the SMTP server).
4. Click **Test Connection** and Save.

The screenshot shows the Cisco ISE Administration interface for the SMTP Server Settings. The left sidebar contains navigation options like Client Provisioning, FIPS Mode, Security Settings, Alarm Settings, Posture, Profiling, Protocols, Endpoint Scripts, Proxy, SMTP Server, SMS Gateway, System Time, ERS Settings, API Gateway Settings, and Network Success Diagnostics. The main content area is titled 'SMTP Server Settings' and includes a description: 'Configure a Simple Mail Transfer Protocol(SMTP) server to send email notifications for alarms, to enable sponsors to send email notification to guests with their login credentials and password reset instructions, and enable guests to automatically receive their login credentials after they successfully register themselves and with actions to take before their guest accounts expire.' Below this, there are input fields for 'SMTP Server' (mail.testlab.com), 'SMTP Port' (25), and 'Connection Timeout' (60 seconds). There are also sections for 'Encryption settings' with a checkbox for 'Use TLS/SSL Encryption' and 'Authentication Settings' with a checkbox for 'Use Password Authentication'. A 'Test Connection' button is located at the bottom right.

Packet capture shows the ISE communication with the SMTP Server without Authentication or Encryption:

The screenshot shows a network packet capture (PCAP) for an SMTP session. The top part shows a list of packets with their timestamps, source and destination IP addresses, and protocols. The bottom part shows the details of a selected packet (packet 2856), including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) information. The SMTP data is visible in the 'Simple Mail Transfer Protocol' section, showing a '220' response from the server and a '220' response code from the client. The response text is: '220 DC1.testlab.com Microsoft ESMTS MAIL Service, Version: 8.5.9600.16384 ready at Wed, 28 Oct 2020 12:23:03 +0000 \r\n' and 'Response code: <domain> Service ready (220)'. The response parameter is: 'DC1.testlab.com Microsoft ESMTS MAIL Service, Version: 8.5.9600.16384 ready at Wed, 28 Oct 2020 12:23:03 +0000'.

Secure SMTP Communication Settings

The secured connection can be made in two ways:

1. SSL Based
2. Username/Password-based

The SMTP Server used must support SSL and Credentials based authentication. Secured SMTP communication can be used with either of the options or both the options enabled simultaneously.

Secure SMTP Communication with Encryption Enabled

1. Import Root CA Certificate of the SMTP server certificate in the ISE Trusted Certificates with usage: **Trust for authentication within ISE** and **Trust for client authentication and Syslog**.
2. Configure the SMTP server, Port configured on the SMTP server for encrypted communication, and check the option **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

Test Connection shows a successful connection to the SMTP Server.

Administration · System

Certificates Logging Maintenance Upgr

SMTP Server Settings

Configure a Simple Mail Transfer Protocol(SMTP) server to allow network 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*

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](#)

Packet captures show that the Server has accepted the **STARTTLS** option as requested by the 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

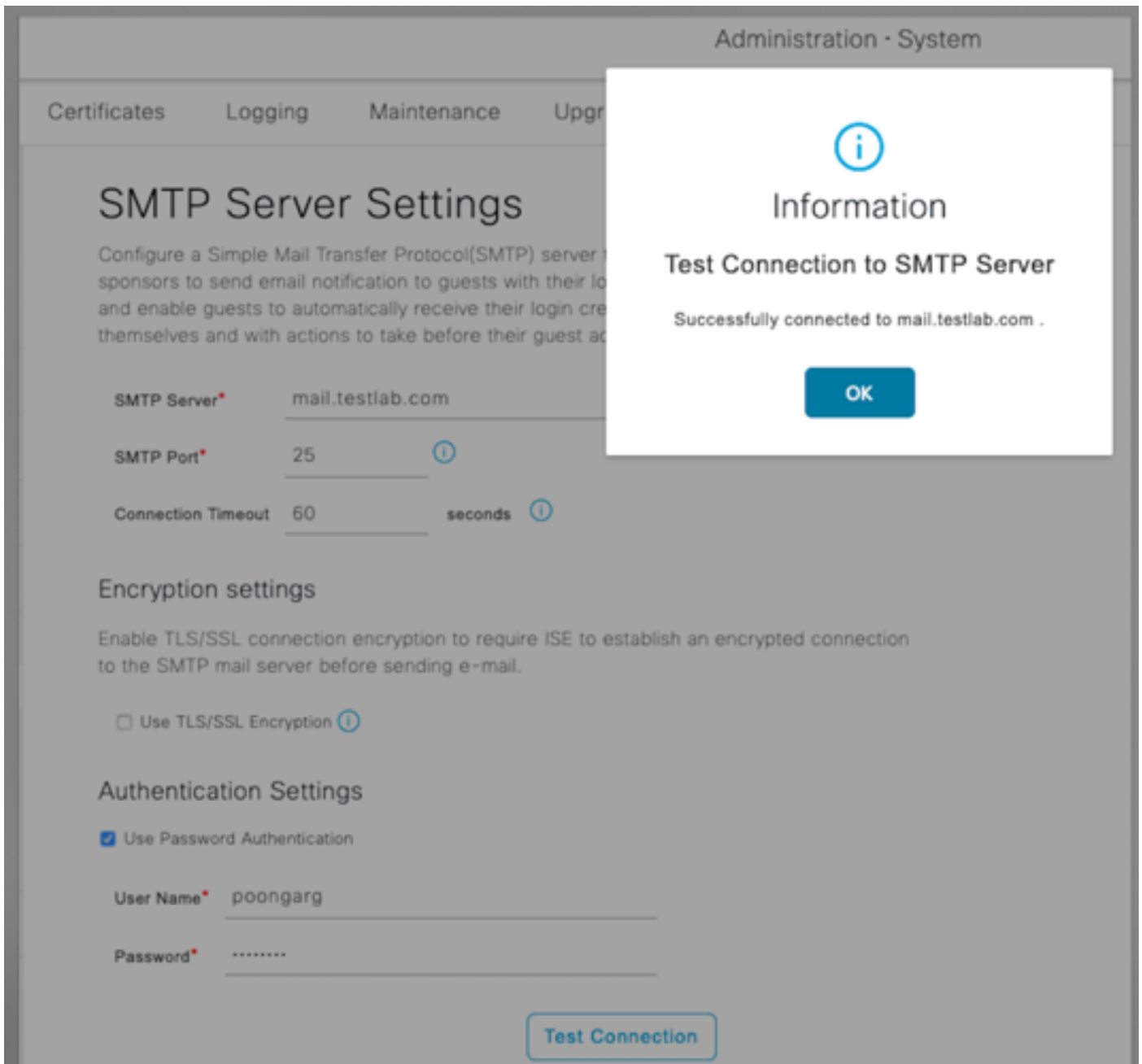
```

> Frame 835: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface
> 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
  
```

Secure SMTP Communication with Authentication Settings Enabled

1. Configure the SMTP Server and SMTP Port.
2. Under Authentication Settings, check the **Use Password Authentication** option and provide the username and password.

Successful **Test Connection** when password-based authentication works :



Sample packet capture that shows successful authentication with credentials:

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: 8.5.9600.16384 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 VXNlcnRhdnMhMjU=
1637	2020-10-28 18:43:13.672793	10.106.32.25	10.197.164.21	SMTP	80	C: User: cG9vaWdhcnRlcw=
1638	2020-10-28 18:43:13.673429	10.197.164.21	10.106.32.25	SMTP	84	S: 334 UGFzc3dvcmQ6
1639	2020-10-28 18:43:13.673474	10.106.32.25	10.197.164.21	SMTP	80	C: Pass: OyFzY2BxMjU=
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

Verify

Use this section to confirm that your configuration works properly.

1. Use the Test Connection option in order to verify the connectivity to the configured SMTP

server.

- Send a test email from Guest portal at **Work Centers > Guest Access > Portals & Components > Guest Portals > Self-Registered Guest Portal(default) > Portal Page Customization > Notifications > Email > Preview window Settings**, enter a valid email address and Send Test Email. The recipient must receive the Email from the configured email address under Guest Email Settings.

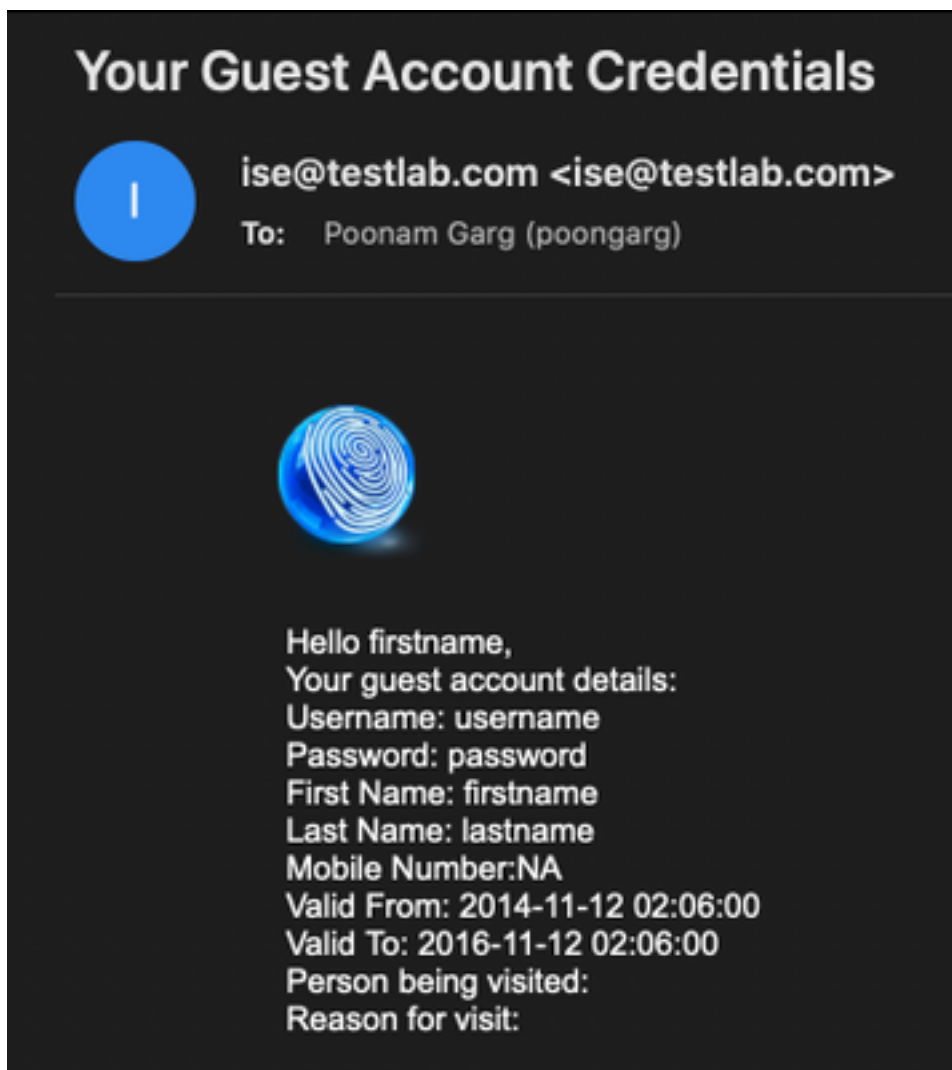
Sample email notification sent for Guest Account Credentials:

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 xch-rcd-001.cisco.com Microsoft ESMTPL 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: EHLO ISE3-1
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-xch-rcd-001.cisco.com Hello [18.186.32.25] 250-SIZE 37748736 250-PIPELINING 250-DSN 250-ENHANCED
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:<ise@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:poongarg@cisco.com
2522	2020-10-26 18:51:34.405811	173.37.182.6	SMTP	17	00:50:56:0b:76:f6, bc:16:65:01:81:bf	S: 250 2.1.0 Recipient OK
2523	2020-10-26 18:51:34.674506	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	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	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	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 18:51:34.952109	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 18:51:34.956436	18.186.32.25	SMTP	2714	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA Fragment, 2660 bytes
2548	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: <ise@testlab.com>, subject: Your Guest Account Credentials, (text/html) (image/png)
2583	2020-10-26 18:51:35.597364	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=XCH-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_8b: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
    
```

Sample email notification received by Email recipient:



Troubleshoot

This section provides the information you can use in order to troubleshoot your configuration:

Problem: Test connection shows: "Could not connect to SMTP Server, SSL Error. Please check the trusted certificates".



Packet capture shows that the certificate presented by the SMTP server is not trusted:

Time	Source	Destination	Protocol	Length	Info
1698	2020-10-28 17:50:22.639934	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 WS=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 17:50:22.686448	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
1716	2020-10-28 17:50:22.687636	10.106.32.25	10.197.164.21	TLSv1.2	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)

Solution: Import Root CA Certificate of the SMTP server in the ISE Trusted Certificates and if TLS support is configured on the port.

Problem: Test Connection shows: Authentication failure: Could not connect to SMTP Server, User Name or Password is incorrect.



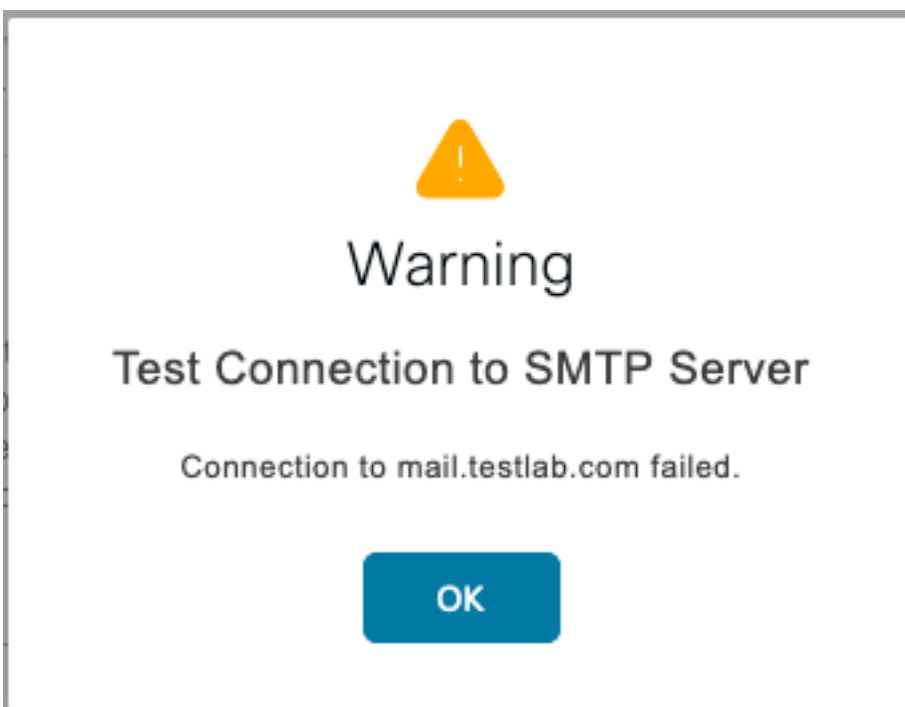
Sample packet capture here shows that the authentication was not successful.

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 ESMTS 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 VbWlce5hbw06
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

Solution: Validate Username or Password configured on the SMTP server.

Problem: Test Connection shows: Connection to SMTP server failed.



Solution: Verify the SMTP Server Port configuration, Check if the SMTP server name is resolvable by the configured DNS server on ISE.

The example here shows a reset is sent by the SMTP server on 587 port which is not configured for SMTP service.

```
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 WS=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)
  010) ... = 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...0... = Push: Not set
▶ ....0...1... = Reset: Set
  ....0...0... = Syn: Not set
  ....0...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]
```

Related Information

- 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
- [Technical Support & Documentation - Cisco Systems](#)