

在ISE上配置安全SMTP服务器

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[SMTP设置](#)

[不使用身份验证或加密的不安全SMTP通信设置](#)

[安全SMTP通信设置](#)

[启用加密的安全SMTP通信](#)

[启用身份验证设置的安全SMTP通信](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何在思科身份服务引擎(ISE)上配置简单邮件传输协议(SMTP)服务器，以支持多个服务的邮件通知。ISE版本3.0支持与SMTP服务器的安全连接和不安全连接。

作者：思科TAC工程师Poonam Garg。

先决条件

要求

思科建议您对思科ISE和SMTP服务器功能有基本的了解。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

本节介绍ISE的配置，以支持用于以下目的的电子邮件通知：

- 在启用“在邮件中包含系统警报”选项的情况下，向任何内部管理员用户发送电子邮件警报通知。发送警报通知的发件人的电子邮件地址硬编码为ise@<hostname>。
- 使发起人能够向访客发送电子邮件通知及其登录凭证和密码重置说明。

- 使访客能够在成功注册自己并在访客帐户到期之前采取操作后自动接收其登录凭证。
- 在密码到期日期之前，向ISE上配置的ISE管理员用户/内部网络用户发送提醒电子邮件。

SMTP设置

ISE必须配置SMTP中继服务器，才能使用任何电子邮件服务。要更新SMTP服务器详细信息，请导航至Administration > System > Settings > Proxy > SMTP server。

此表显示分布式ISE环境中哪个节点发送电子邮件。

电子邮件用途	发送电子邮件的节点
访客帐户过期	主PAN
警报	活动MnT
来自各个门户的发起人和访客帐户通知	PSN
密码到期	主PAN

配置SMTP服务器，以便能够根据您的要求接受来自ISE的任何具有或不具有身份验证或加密的邮件。

不使用身份验证或加密的不安全SMTP通信设置

1. 定义SMTP服务器主机名（出站SMTP服务器）。
2. SMTP端口（此端口必须在网络中打开才能连接到SMTP服务器）。
3. 连接超时（输入Cisco ISE等待SMTP服务器响应的最长时间）。
4. 单击Test Connection并保存。

The screenshot shows the 'SMTP Server Settings' page in the Cisco ISE Administration console. The page includes a navigation menu on the left with 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 contains the following configuration options:

- 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

A 'Test Connection' button is located at the bottom right of the configuration area.

数据包捕获显示与SMTP服务器的ISE通信（无身份验证或加密）：

```

2056 2020-10-28 17:50:28.476200 10.197.164.21 10.106.32.25 SMTP 184 S: 220 DC1.testlab.com Microsoft ESMTMP MAIL Service, Version: 8.5.9600.16384 ready at Wed, 28 Oct 2020 12:23:03 +0000
2058 2020-10-28 17:50:28.476594 10.106.32.25 10.197.164.21 SMTP 79 C: EHLO ISE3-1
2059 2020-10-28 17:50:28.477232 10.197.164.21 10.106.32.25 SMTP 273 S: 250-DC1.testlab.com Hello [10.106.32.25] | 250-TURN | 250-SIZE | 250-ETRN | 250-PIPELINING | 250-DSN | 250-ENHANCEDSTATUSCODES.
2060 2020-10-28 17:50:28.477465 10.106.32.25 10.197.164.21 SMTP 72 C: QUIT
2061 2020-10-28 17:50:28.478480 10.197.164.21 10.106.32.25 SMTP 130 S: 221 2.0.0 DC1.testlab.com Service closing transmission channel

> Frame 2056: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits)
> Ethernet II, Src: Cisco_01:81:b1:f (bc:16:05:01:81:b1:f), 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: 20891, Seq: 1, Ack: 1, Len: 118
v Simple Mail Transfer Protocol
v Response: 220 DC1.testlab.com Microsoft ESMTMP MAIL Service, Version: 8.5.9600.16384 ready at Wed, 28 Oct 2020 12:23:03 +0000 \r\n
Response code: <domain> Service ready (220)
Response parameter: DC1.testlab.com Microsoft ESMTMP MAIL Service, Version: 8.5.9600.16384 ready at Wed, 28 Oct 2020 12:23:03 +0000

```

安全SMTP通信设置

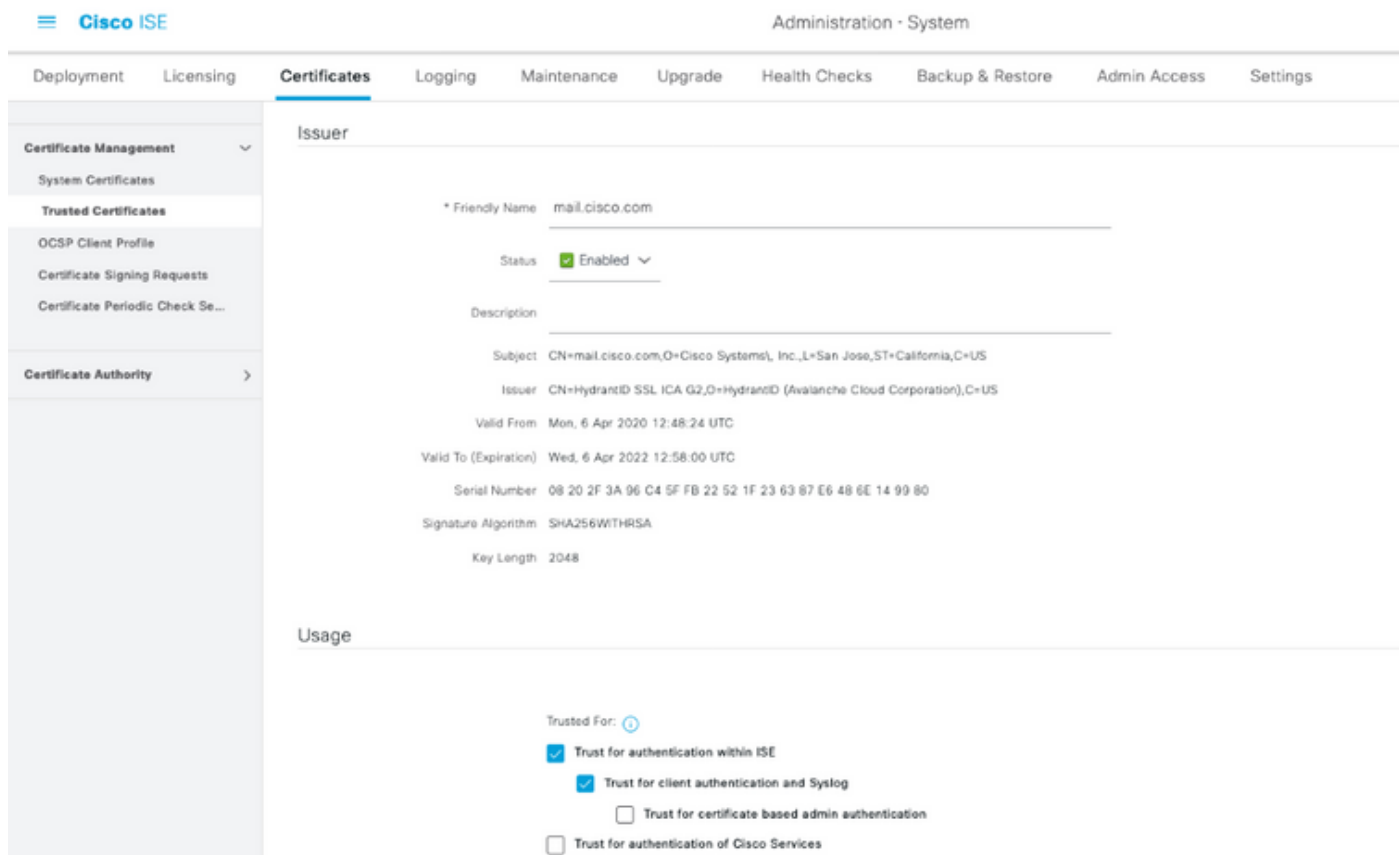
安全连接可通过两种方式建立：

1. 基于SSL
2. 基于用户名/密码

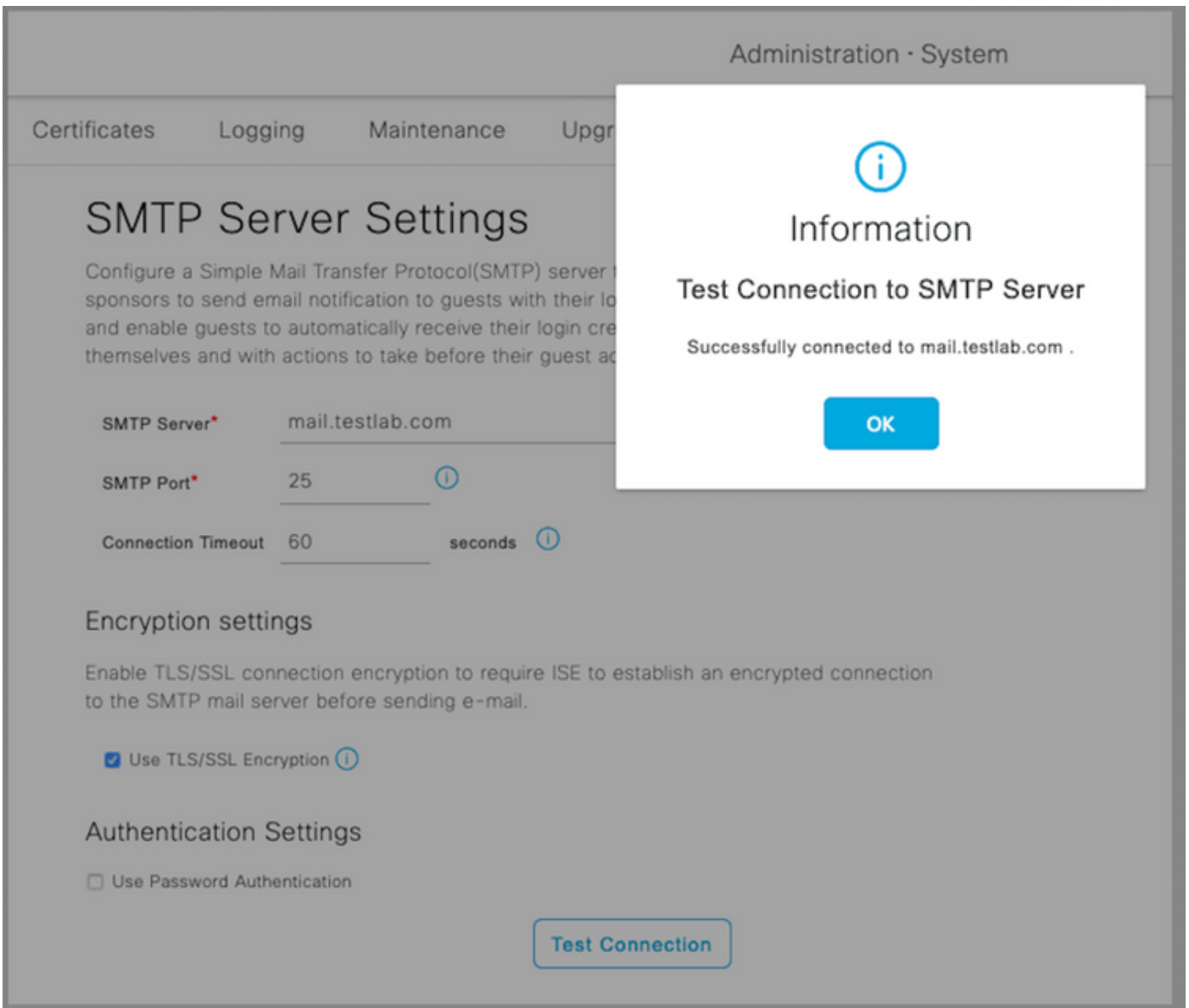
使用的SMTP服务器必须支持基于SSL和凭证的身份验证。安全SMTP通信可与同时启用的选项之一或两个选项一起使用。

启用加密的安全SMTP通信

1. 在ISE受信任证书中导入SMTP服务器证书的根CA证书（使用）：在ISE中信任身份验证，在客户端身份验证和系统日志中信任。
2. 配置SMTP服务器、在SMTP服务器上配置的用于加密通信的端口，并选中选项使用TLS/SSL加密。



测试连接显示与SMTP服务器的连接成功。



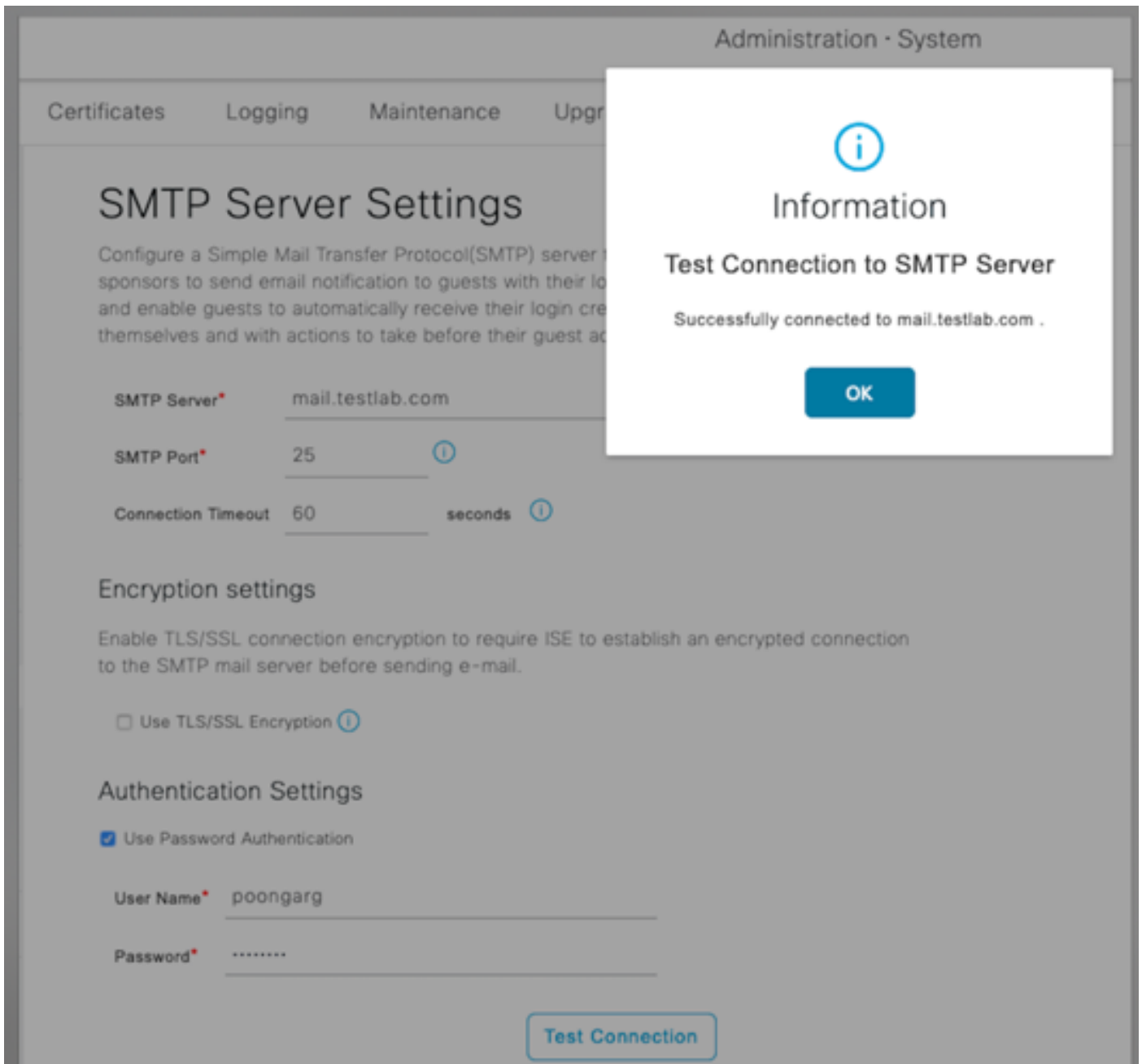
数据包捕获显示服务器已接受ISE请求的STARTTLS选项。

No.	Time	Source	Destination	Protocol	Len	Info
830	2020-10-28 18:49:25.415546	10.197.164.21	10.106.32.25	SMTP	184	S: 220 DC1.testlab.com Microsoft ESMTPL MAIL Service, Version: 8.5.9600.16384 ready at Wed, 28 Oct 2020 13:22:00 +0800
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 18:49:25.416658	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_01:03:bf (bc:16:65:01:03:bf), Dst: Vmware_08:76:f6 (00:50:56:08:76: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

启用身份验证设置的安全SMTP通信

1. 配置SMTP服务器和SMTP端口。
 2. 在Authentication Settings下，选中Use Password Authentication选项并提供用户名和密码。
- 基于密码的身份验证工作时测试连接成功：



数据包捕获示例，显示使用凭证成功进行身份验证：

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 VxMlcnShobMUG
1637	2020-10-28 18:43:13.672783	10.106.32.25	10.197.164.21	SMTP	80	C: User: cG9vbnRhdnc=
1638	2020-10-28 18:43:13.673429	10.197.164.21	10.106.32.25	SMTP	84	S: 334 UGFzc3dvccDQ6
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

验证

使用本部分可确认配置能否正常运行。

1. 使用Test Connection (测试连接) 选项验证与已配置SMTP服务器的连接。

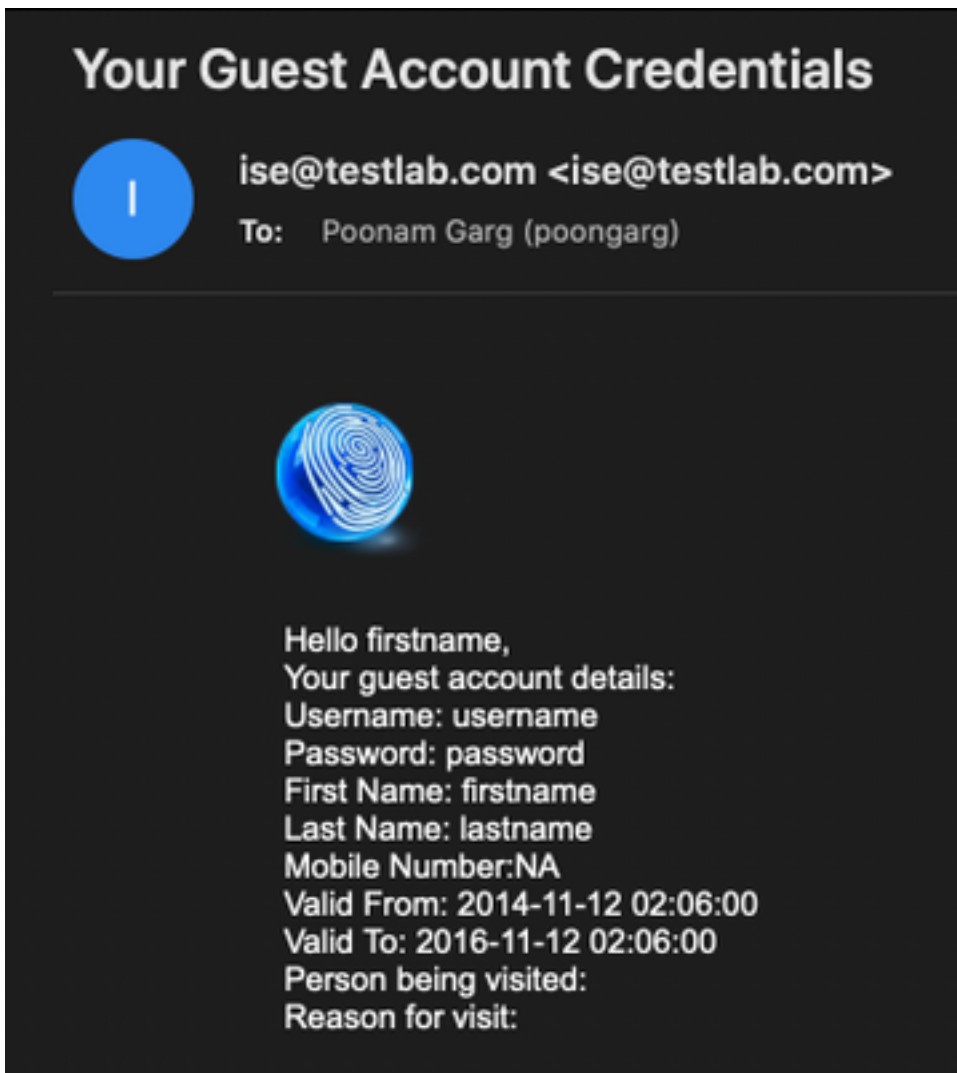
2. 从访客门户发送测试电子邮件，从**工作中心>访客接入>门户和组件>访客门户>自注册访客门户 (默认)>门户页面自定义>通知>邮件>预览窗口设置**，输入有效的电子邮件地址并发送测试电子邮件。收件人必须从“访客电子邮件设置”下配置的电子邮件地址接收电子邮件。

为访客帐户凭证发送的电子邮件通知示例：

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 18:51:35.031511	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 18:51:34.674506	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 <CR LF>.<CR LF>
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 18:51:34.956426	18.186.32.25	SMTP	2714	bc:16:65:01:81:bf, 00:50:56:0b:76:f6	C: DATA Fragment, 2660 bytes
2568	2020-10-26 18:51:35.228463	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 18:51:35.228480	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 18:51:35.228783	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 18:51:35.228793	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 18:51:35.228878	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 18:51:35.597164	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=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) on interface 0/24
 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

电子邮件收件人收到的电子邮件通知示例：



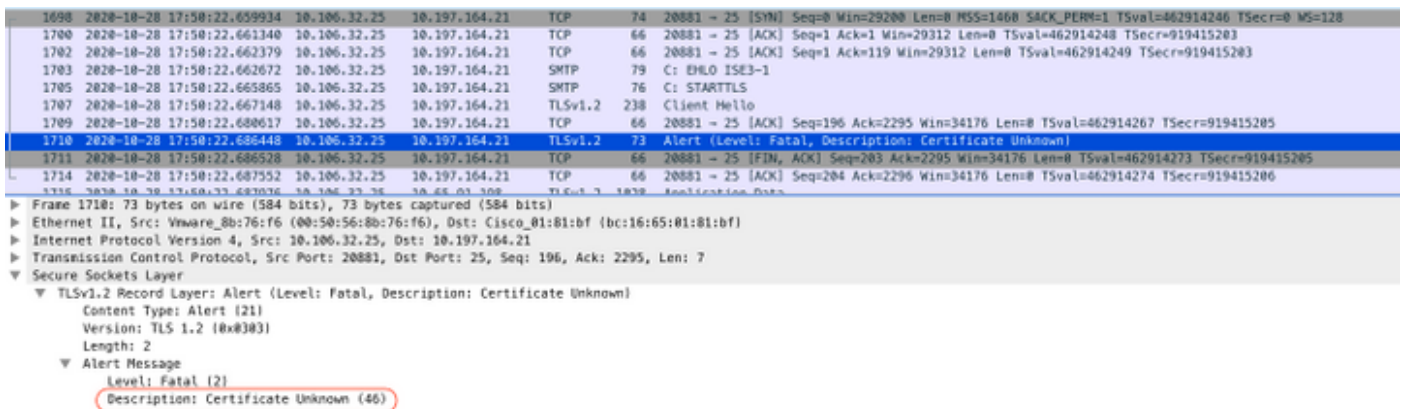
故障排除

本节提供可用于排除配置故障的信息：

问题：测试连接显示：“无法连接到SMTP服务器，SSL错误。请检查受信任证书”。



数据包捕获显示SMTP服务器提供的证书不受信任：



解决方案：导入ISE受信任证书中SMTP服务器的根CA证书（如果端口上配置了TLS支持）。

问题：测试连接显示：身份验证失败：无法连接到SMTP服务器，用户名或密码不正确。



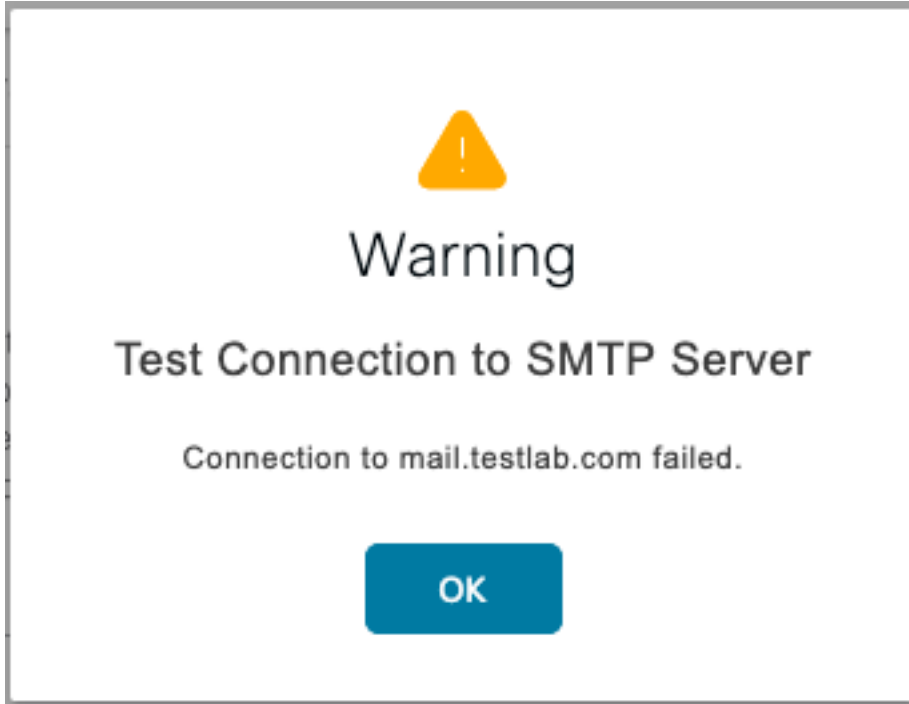
此处的数据包捕获示例显示身份验证失败。

No.	Time	Source	Destination	Protocol	Len	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 ESMT 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 V0Wlca5hbW06
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 UGfzc3dvcm06
951	2020-10-28 18:11:40.730151	10.186.32.25	10.197.164.21	SMTP	80	C: Pass: QyFzrz2BxMjM=
952	2020-10-28 18:11:40.748181	10.197.164.21	10.186.32.25	SMTP	305	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:16:65:81:81: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

解决方案：验证在SMTP服务器上配置的用户名或密码。

问题：测试连接显示：连接SMTP服务器失败。



解决方案：验证SMTP服务器端口配置，检查SMTP服务器名称是否可由ISE上配置的DNS服务器解析。

此示例显示SMTP服务器在587端口上发送重置，该端口未配置SMTP服务。


```

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 WS=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_0b: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_01:81:bf (bc:16:65:01:81:bf), Dst: Vmware_0b: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
... ...1 = Acknowledgment: Set
...0... = Push: Not set
▶1.. = 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]

相关信息

- 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
- [技术支持和文档 - Cisco Systems](#)