

ISE에서 보안 SMTP 서버 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[SMTP 설정](#)

[인증 또는 암호화 없이 SMTP 통신 설정 비보안](#)

[보안 SMTP 통신 설정](#)

[암호화를 사용하는 보안 SMTP 통신](#)

[인증 설정과의 보안 SMTP 통신 사용](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 여러 서비스에 대한 이메일 알림을 지원하기 위해 Cisco ISE(Identity Services Engine)에서 SMTP(Simple Mail Transfer Protocol) 서버를 구성하는 방법에 대해 설명합니다. ISE 버전 3.0은 SMTP 서버에 대한 보안 및 비보안 연결을 모두 지원합니다.

기고자: Poonam Garg, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

Cisco는 Cisco ISE 및 SMTP 서버 기능에 대한 기본 지식을 가지고 있는 것을 권장합니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

이 섹션에서는 다음에 사용되는 이메일 알림을 지원하기 위해 ISE의 컨피그레이션에 대해 설명합니다.

- Include of system alarms in emails(이메일에 시스템 경보 포함) 옵션이 활성화된 내부 관리자 사용자에게 이메일 경보 알림을 보냅니다.경보 알림을 보낼 발신자의 이메일 주소는 ise@<hostname>으로 하드코딩됩니다.
- 스폰서가 게스트에게 로그인 자격 증명 및 비밀번호 재설정 지침을 사용하여 이메일 알림을 보낼 수 있도록 합니다.
- 게스트가 성공적으로 등록한 후 자동으로 로그인 자격 증명을 수신하고 게스트 계정이 만료되기 전에 취해야 할 조치를 취할 수 있습니다.
- 암호 만료 날짜 전에 ISE에 구성된 ISE 관리자 사용자/내부 네트워크 사용자에게 알림 이메일을 보냅니다.

SMTP 설정

ISE에서 이메일 서비스를 사용하려면 먼저 SMTP 릴레이 서버를 구성해야 합니다.SMTP 서버 세부 정보를 업데이트하려면 Administration(관리) > System(시스템) > Settings(설정) > Proxy(프록시) > SMTP server(SMTP 서버)로 이동합니다.

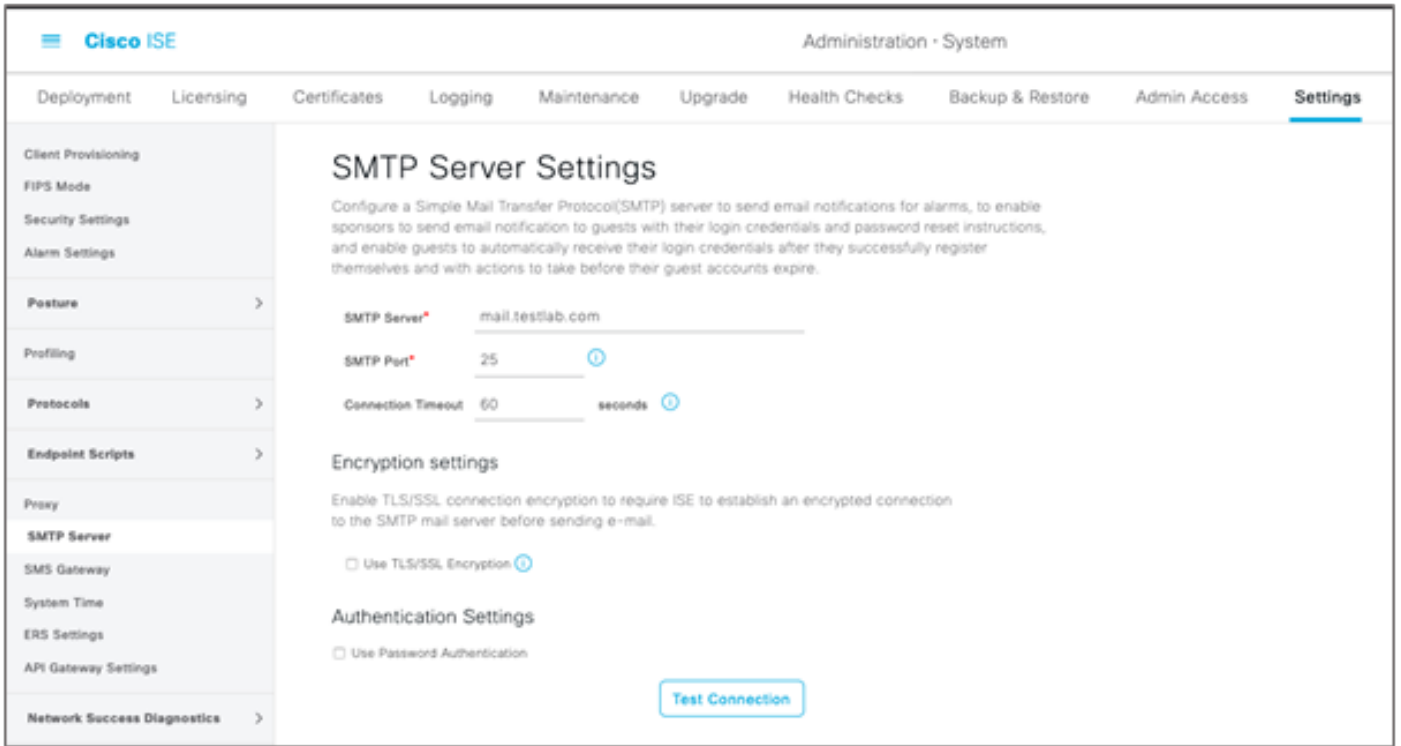
이 표에서는 분산 ISE 환경의 어떤 노드가 이메일을 전송하는지 보여줍니다.

이메일 용도	이메일을 보내는 노드
게스트 계정 만료	기본 PAN
경보	활성 MnT
각 포털의 스폰서 및 게스트 계정 알림	PSN
비밀번호 만료	기본 PAN

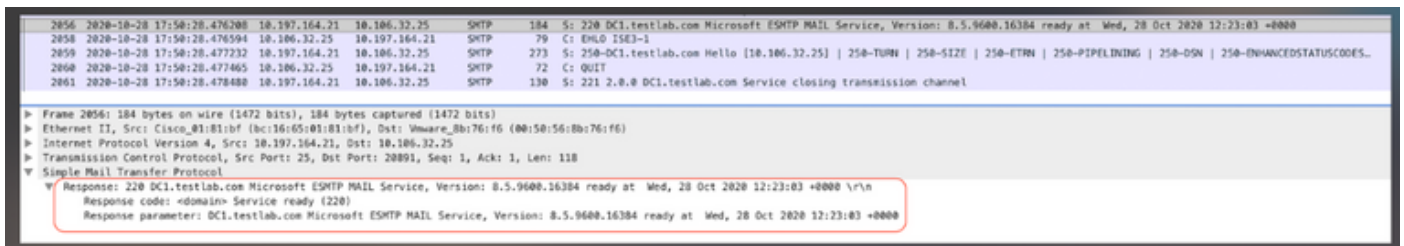
요구 사항에 따라 인증 또는 암호화를 사용하거나 사용하지 않고 ISE의 이메일을 수락할 수 있도록 SMTP 서버를 구성합니다.

인증 또는 암호화 없이 SMTP 통신 설정 비보안

1. SMTP 서버 호스트 이름(아웃바운드 SMTP 서버)을 정의합니다.
2. SMTP 포트(SMTP 서버에 연결하려면 네트워크에서 이 포트가 열려 있어야 함).
3. Connection Timeout(연결 시간 제한) (Cisco ISE가 SMTP 서버의 응답을 기다리는 최대 시간 입력).
4. 연결 테스트 및 저장을 클릭합니다.



패킷 캡처는 인증 또는 암호화 없이 SMTP 서버와의 ISE 통신을 표시합니다.



보안 SMTP 통신 설정

보안 연결은 두 가지 방법으로 만들 수 있습니다.

1. SSL 기반
2. 사용자 이름/비밀번호 기반

사용된 SMTP 서버는 SSL 및 자격 증명 기반 인증을 지원해야 합니다. 보안 SMTP 통신은 두 옵션 중 하나 또는 두 옵션 모두 동시에 활성화된 옵션과 함께 사용할 수 있습니다.

암호화를 사용하는 보안 SMTP 통신

1. ISE의 신뢰할 수 있는 인증서 사용 시 SMTP 서버 인증서의 루트 CA 인증서 가져오기: ISE 내에서 인증을 위한 신뢰 및 클라이언트 인증 및 Syslog를 위한 신뢰.
2. SMTP 서버를 구성하고, 암호화된 통신을 위해 SMTP 서버에 구성된 포트를 구성하고, Use TLS/SSL encryption(TLS/SSL 암호화 사용) 옵션을 선택합니다.

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(연결 테스트)은 SMTP 서버에 대한 성공적인 연결을 표시합니다.

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 account is created.

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



Information

Test Connection to SMTP Server

Successfully connected to mail.testlab.com .

OK

패킷 캡처는 서버가 ISE에서 요청한 **STARTTLS** 옵션을 수락했음을 보여줍니다.

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 +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 18:49:25.416658	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

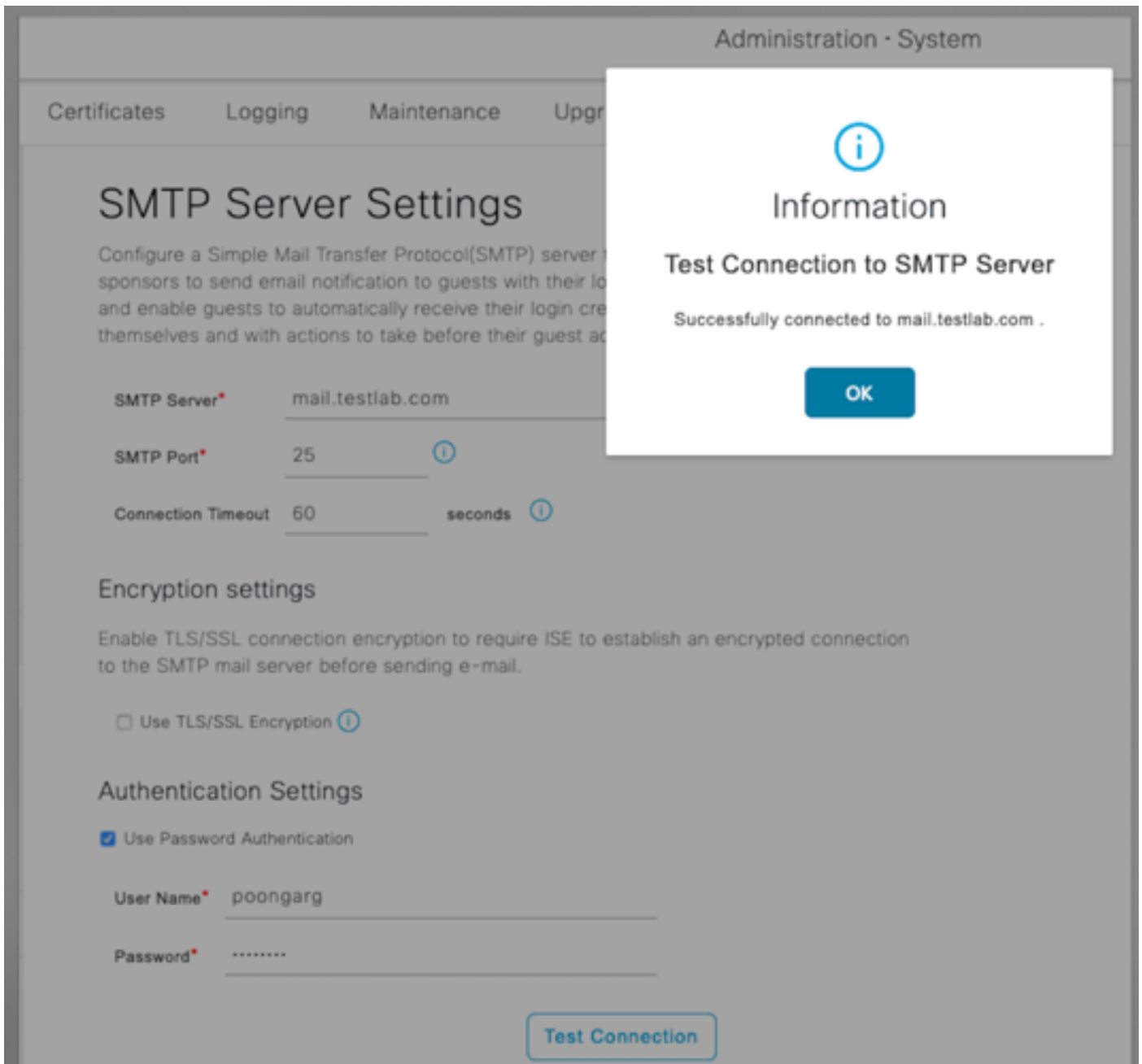
```

Frame 835: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0
Ethernet II, Src: Cisco_01:00:0c:00:00:00 (bc:16:65:01:01:01), 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: 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
  
```

인증 설정과의 보안 SMTP 통신 사용

1. SMTP 서버 및 SMTP 포트를 구성합니다.
2. Authentication Settings(인증 설정)에서 Use Password Authentication(비밀번호 인증 사용) 옵션을 선택하고 사용자 이름과 비밀번호를 입력합니다.

비밀번호 기반 인증이 작동할 때 연결 테스트 성공:



자격 증명을 사용한 성공적인 인증을 보여 주는 샘플 패킷 캡처:

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: 6.5.9608.10384 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 VxM1cnDh0mAG
1637	2020-10-28 18:43:13.672783	10.106.32.25	10.197.164.21	SMTP	80	C: User: c0pvaadhcnx=
1638	2020-10-28 18:43:13.673429	10.197.164.21	10.106.32.25	SMTP	84	S: 334 UGFrc3dvccnD6
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

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

1. 구성된 SMTP 서버에 대한 연결을 확인하려면 Test Connection 옵션을 사용합니다.

2. 게스트 포털에서 Work Centers(작업 센터) > Guest Access(게스트 액세스) > Portals & Components(포털 및 구성 요소) > Guest Portals(게스트 포털) > Self-Registered Guest Portal(기본값) > Portal Page Customization(포털 페이지 사용자 맞춤화) > Notifications(알림) > Email(이메일) > Preview window Settings(미리 보기 창 설정)에서 유효한 이메일 주소를 입력하고 Send Test Email(테스트 이메일 보내기)를 입력합니다.수신자는 Guest Email Settings(게스트 이메일 설정) 아래의 구성된 이메일 주소에서 이메일을 받아야 합니다.

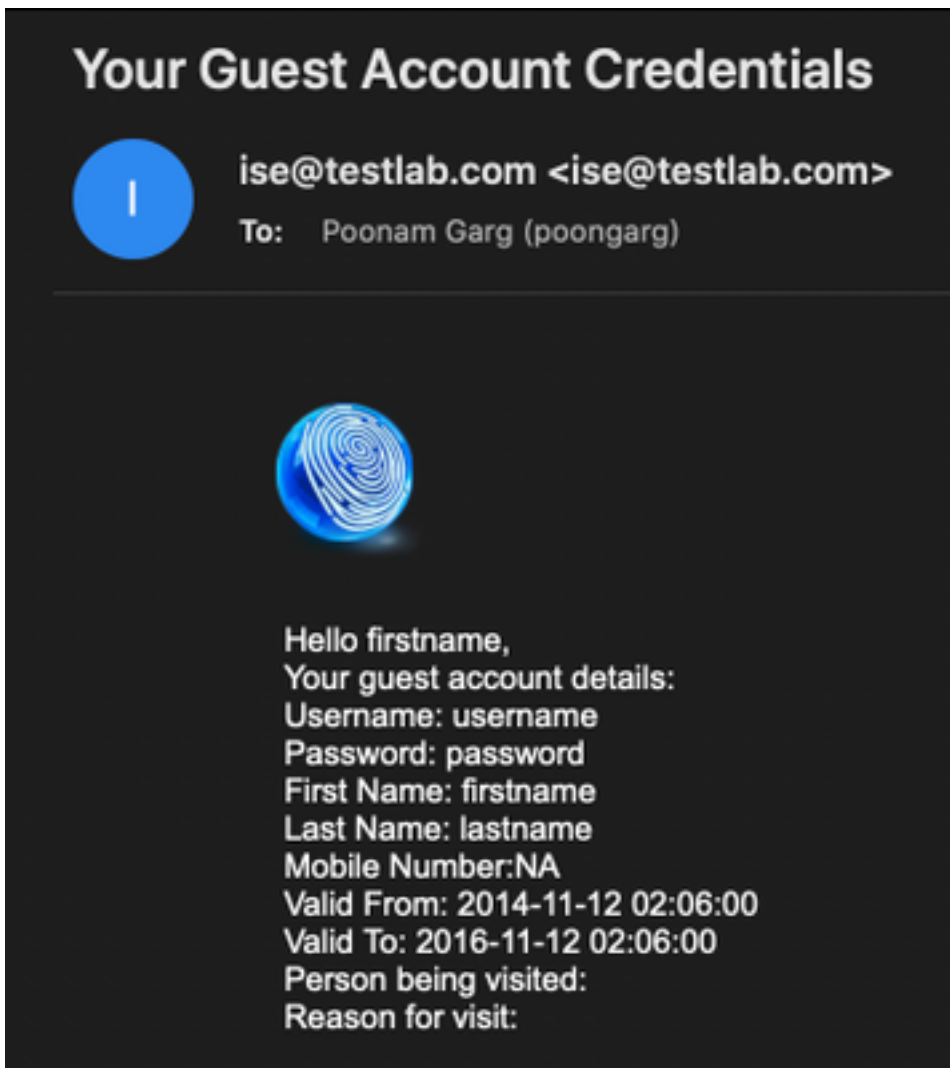
게스트 계정 자격 증명에 대해 전송된 샘플 이메일 알림:

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 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: 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 18:51:35.033121	173.37.182.6	SMTP	18	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 18:51:34.952189	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 18:51:34.956436	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 18:51:35.228463	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 18:51:35.597344	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=20117613468157, 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	182	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
    
```

이메일 수신자가 수신한 샘플 이메일 알림:



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제/장애:테스트 연결에는 다음이 표시됩니다."SMTP 서버에 연결할 수 없습니다. SSL 오류입니다. 신뢰할 수 있는 인증서를 확인하십시오."



패킷 캡처는 SMTP 서버에서 제공하는 인증서를 신뢰할 수 없음을 보여줍니다.

```
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 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 17:50:22.686448 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 Min=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 1839 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)
```

해결책:ISE Trusted Certificates(ISE 신뢰할 수 있는 인증서)에서 SMTP 서버의 루트 CA 인증서를 가져오고 TLS 지원이 포트에 구성되어 있는 경우

문제/장애:테스트 연결에는 다음이 표시됩니다.인증 실패:SMTP 서버에 연결할 수 없습니다. 사용자 이름 또는 암호가 잘못되었습니다.



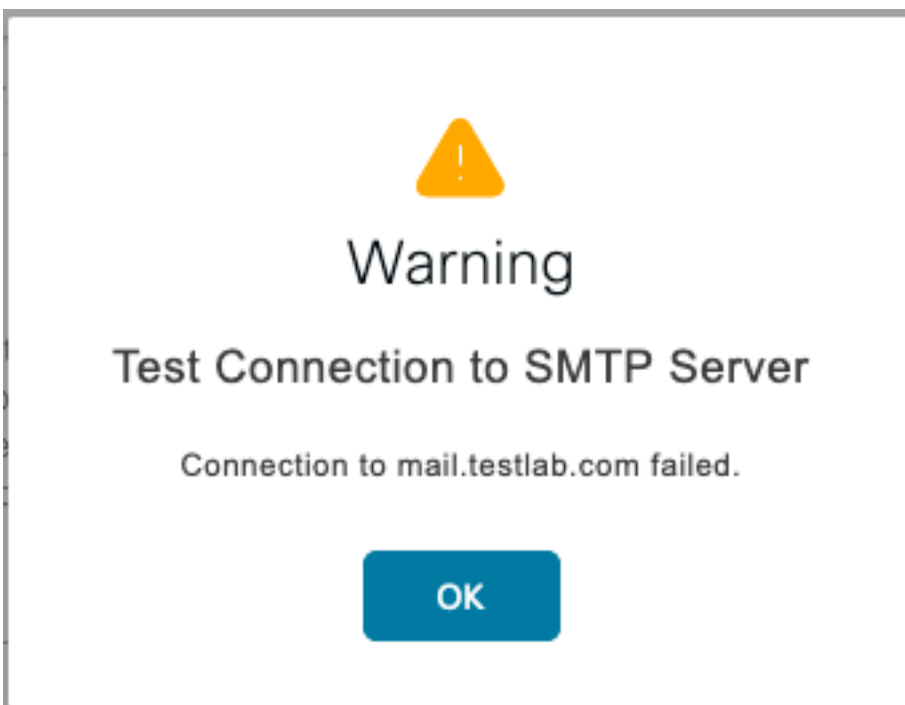
샘플 패킷 캡처는 인증이 실패했음을 보여줍니다.

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 ESMTP MAIL Service, Version: 8.5.9600.36384 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 VbWlca5hbw06
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

해결책:SMTP 서버에 구성된 사용자 이름 또는 비밀번호 검증

문제/장애:테스트 연결에는 다음이 표시됩니다.SMTP 서버에 연결하지 못했습니다.



해결책:SMTP 서버 포트 컨피그레이션을 확인하고 ISE의 구성된 DNS 서버에서 SMTP 서버 이름을 확인할 수 있는지 확인합니다.

이 예에서는 SMTP 서비스에 대해 구성되지 않은 587 포트에서 SMTP 서버가 재설정을 전송한 것을 보여줍니다.

```

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 [SYN] 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... = Push: Not set
▶ ....01. = 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]

```

관련 정보

- 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
- [기술 지원 및 문서 - Cisco Systems](#)