

# Secure MTP-server op ISE configureren

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratie](#)

[TCP-instellingen](#)

[Onveilige TCP-communicatie-instellingen zonder verificatie of encryptie](#)

[Beveiligingsinstellingen MTP-communicatie](#)

[Beveiligde MTP-communicatie met encryptie](#)

[Beveiligde communicatie MTP met verificatie-instellingen](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft hoe u de Simple Mail Transfer Protocol (MTP) Server op Cisco Identity Services Engine (ISE) kunt configureren om e-mailberichten voor meerdere services te ondersteunen. ISE versie 3.0 ondersteunt zowel beveiligde als onbeveiligde verbindingen naar MGT-server.

Bijgedragen door Poonam Garg, Cisco TAC Engineer.

## Voorwaarden

### Vereisten

Cisco raadt u aan een basiskennis van de functionaliteit van Cisco ISE en MTP-server te hebben.

### Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Configuratie

In dit deel wordt de configuratie van de ISE beschreven ter ondersteuning van e-mailberichten die

worden gebruikt om:

- Bericht per e-mail sturen naar alle interne gebruikers van de beheerder met de optie Systeemalarmen in e-mails ingeschakeld. Het e-mailadres van de afzender om alarm te sturen is hard gecodeerd als ise@<hostname>.
- Inschakelen van sponsors om een e-mailbericht naar de gasten te sturen met hun inloggegevens en instructies voor het opnieuw instellen van een wachtwoord.
- Laat gasten in om automatisch hun logboek in geloofsbrieven te ontvangen nadat zij zich met succes registreren en met acties te ondernemen vóór hun gastrekeningen verlopen.
- Verzend herinneringse-mails naar ISE admingebruikers/interne netwerkgebruikers die op ISE zijn ingesteld voordat hun wachtwoord vervalt.

## TCP-instellingen

Voordat ISE e-maildiensten kan gebruiken, moet het een MTP relaisserver hebben ingesteld. Om de serverdetails te bijwerken, navigeer naar **Beheer > Systeem > Instellingen > Proxy > MTP server**.

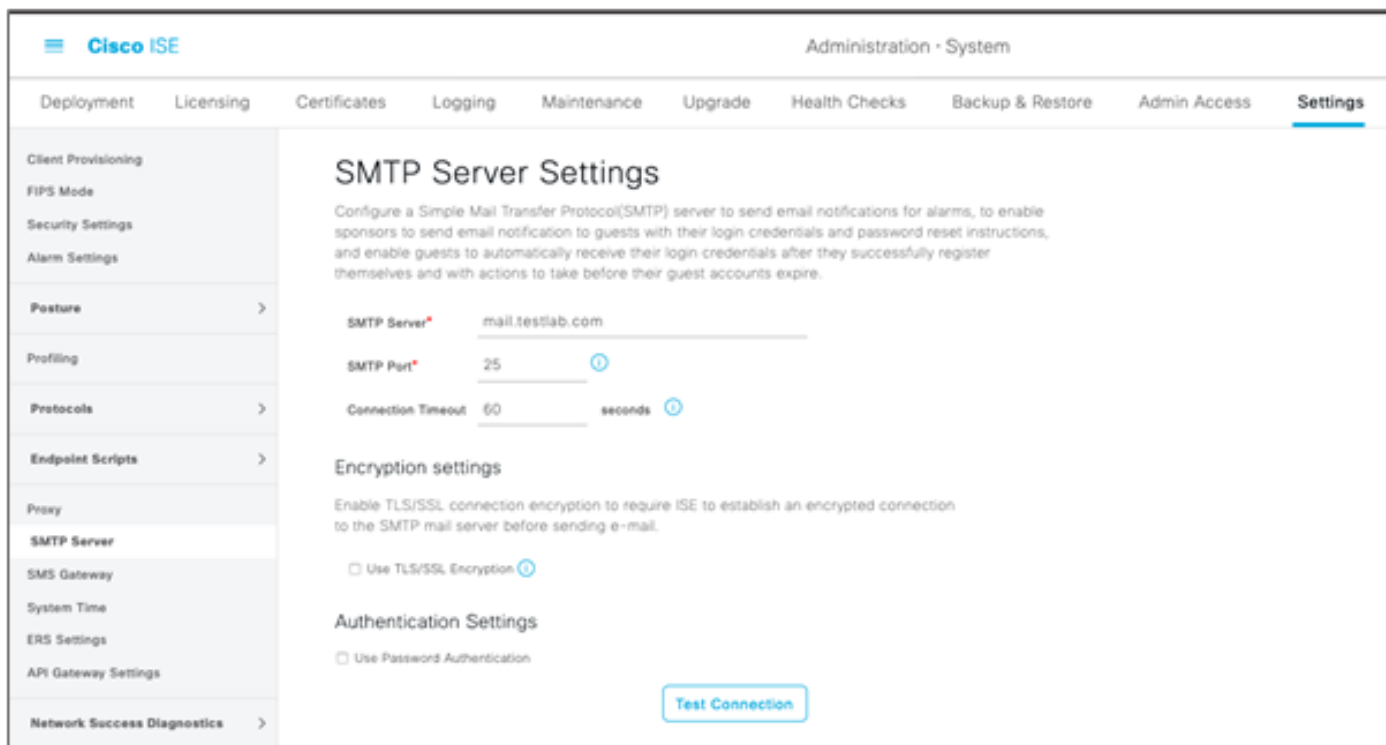
In deze tabel wordt aangegeven welk knooppunt in een gedistribueerde ISE-omgeving een e-mail verstuurt.

E-maildoel	Knooppunt dat e-mail verstuurt
Aflopen van gistaccount	Primair PAN
alarmen	Active MnT
Meldingen van sponsor- en Guest-account uit respectieve portalen	PSN
Wachtwoordverloop	Primair PAN

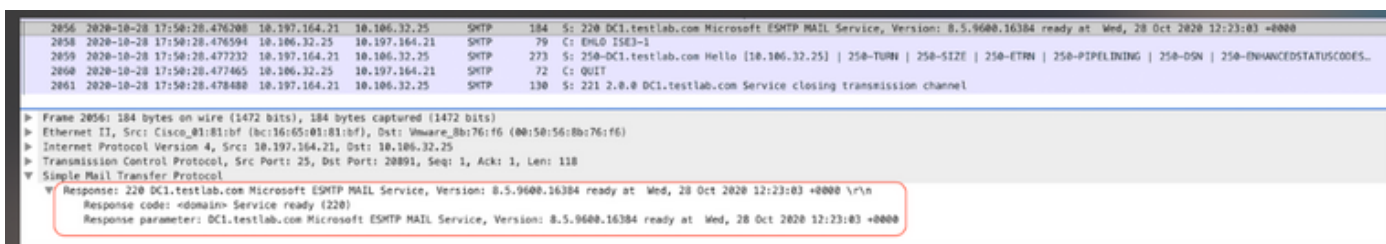
Configureer de MTP-server zodat deze alle e-mails van de ISE kan accepteren met of zonder verificatie of encryptie op basis van uw behoeften.

## Onveilige TCP-communicatie-instellingen zonder verificatie of encryptie

1. Definieert de hostname van de MTP-server (uitgaande MTP-server).
2. MTP-poort (deze poort moet in het netwerk geopend zijn om verbinding te maken met de MTP-server).
3. Time-out bij verbinding (Voer de maximale tijd in dat Cisco ISE wacht op een reactie van de MTP-server).
4. Klik op **Test Connection** en **Save**.



De pakketvastlegging toont de ISE-communicatie met de MTP-server zonder verificatie of encryptie:



## Beveiligingsinstellingen MTP-communicatie

De beveiligde verbinding kan op twee manieren tot stand worden gebracht:

1. SSL-gebaseerd
2. Gebruikersnaam/wachtwoord

De gebruikte MTP-server moet SSL- en Credentials-gebaseerde verificatie ondersteunen. Een beveiligde MTP-communicatie kan worden gebruikt met een van de opties of met beide opties die tegelijkertijd zijn ingeschakeld.

### Beveiligde MTP-communicatie met encryptie

1. Importeer Root CA-certificaat van het MTP-servercertificaat in het ISE Trusted Certificates met gebruik: **Vertrouwen voor authenticatie binnen ISE en vertrouwen op cliëntauthenticatieverklaring en Syslog.**
2. Configureer de MTP-server, poort ingesteld op de MTP-server voor versleutelde communicatie en controleer de optie **Gebruik TLS/SSL-encryptie.**

- 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

De verbinding van de test toont een succesvolle verbinding met de Server MTP.

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](#)

Packet Captures tonen aan dat de Server de optie **STARTTLS** heeft geaccepteerd zoals gevraagd door 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) on interface
> Ethernet II, Src: Cisco_01:81:b1:b1:bc:16:65:01:81:b1:b1, 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
  
```

## Beveiligde communicatie MTP met verificatie-instellingen

1. Configureer de MTP-server en de MTP-poort.
2. Controleer onder Verificatie-instellingen de optie **Wachtwoordverificatie gebruiken** en voer de gebruikersnaam en het wachtwoord in.

Succesvolle **Test Connection** wanneer op een wachtwoord gebaseerde verificatie werkt:

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

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

User Name\* poongarg

Password\* .....

Test Connection

i

**Information**

**Test Connection to SMTP Server**

Successfully connected to mail.testlab.com .

OK

Steekproef pakketopname die succesvolle authenticatie met geloofsbrieven toont:

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: 6.5.9600.16384 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 VNN1cnShobMUG
1637	2020-10-28 18:43:13.672783	10.106.32.25	10.197.164.21	SMTP	80	C: User: cG9vbnhncnc=
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

## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

1. Gebruik de optie Test Connection om de connectiviteit aan de geconfigureerde MTP-server

te verifiëren.

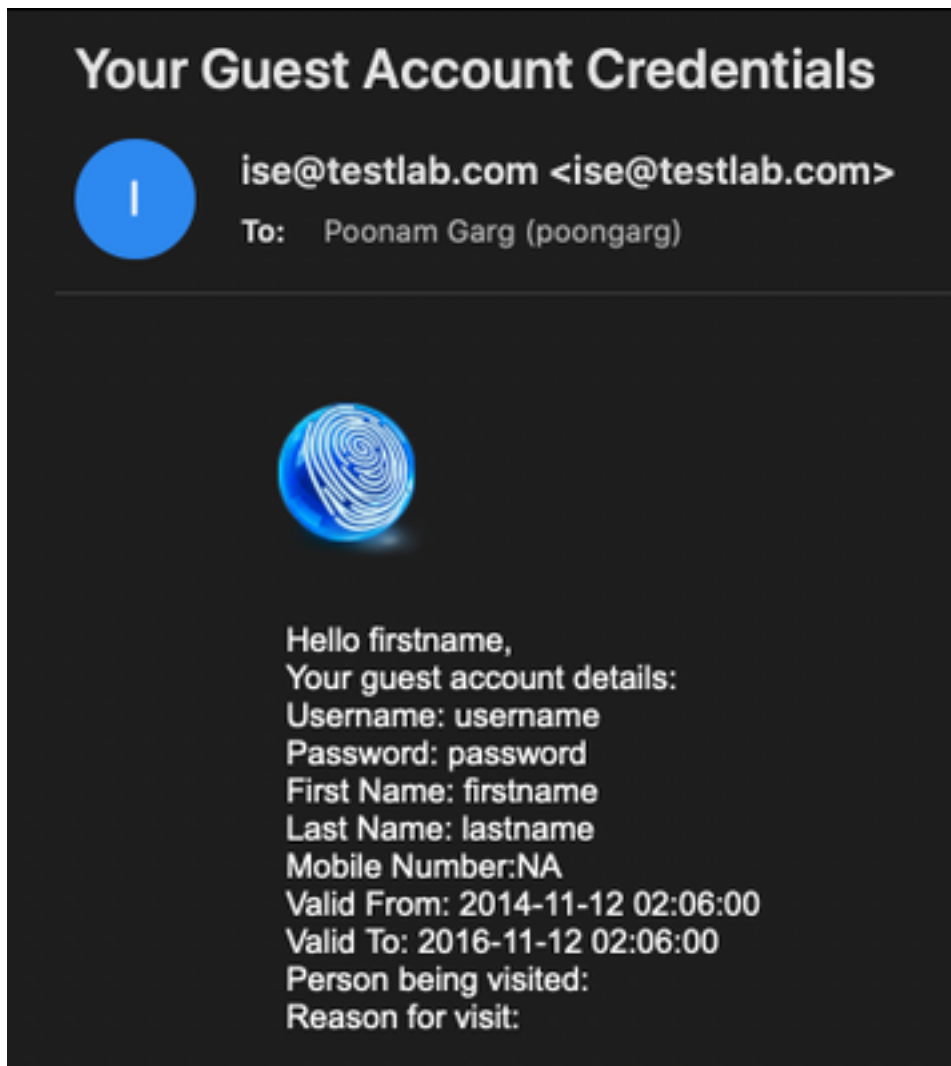
- Verzend een test-e-mail van het portaal Guest in **Workcenters > Gasttoegang > Portals & Componenten > Guest Portals > Zelfgeschreven Guest Portal (standaard) > Portal Pagina-aanpassing > Aanmeldingen > E-mail > Instellingen venster van voorbeeld**, voer een geldig e-mailadres in en Verzend Test-e-mail. De ontvanger moet de e-mail ontvangen van het geconfigureerde e-mailadres onder Instellingen voor e-mail van de gast.

Bericht per e-mail verzonden voor 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 ESMTS MAIL Service ready at Mon, 26 Oct 2020 08:24:07 -0500
2477	2020-10-26 18:51:33.867990	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-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:<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 18:51:34.638311	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 18:51:34.952109	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=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	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  
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
```

E-mailbericht per e-mail ontvangen door e-mail ontvanger:



# Problemen oplossen

Dit gedeelte bevat de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen:

Probleem: Testverbinding: "Kan geen verbinding maken met de MTP Server, SSL fout. Controleer de vertrouwde certificaten".



Uit de pakketvastlegging blijkt dat het certificaat dat door de MTP-server wordt aangeboden, niet betrouwbaar is:

Time	Source	Destination	Protocol	Length	Info
1698	2020-10-28 17:50:22.659934	10.106.32.25	TCP	74	20881 -> 25 [SYN] Seq=8 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	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	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	SMTP	79	C: EHLO ISE3-1
1705	2020-10-28 17:50:22.665865	10.106.32.25	SMTP	76	C: STARTTLS
1707	2020-10-28 17:50:22.667148	10.106.32.25	TLSv1.2	238	Client Hello
1709	2020-10-28 17:50:22.680617	10.106.32.25	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	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)
1711	2020-10-28 17:50:22.686528	10.106.32.25	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	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)

Oplossing: Importeer Root CA certificaatcertificaat van de MTP-server in de ISE Trusted Certificates en indien TLS-ondersteuning op de poort is ingesteld.

Probleem: Test Connection toont: Verificatiefout: Kan geen verbinding maken met de TCP-server, gebruikersnaam of wachtwoord is onjuist.





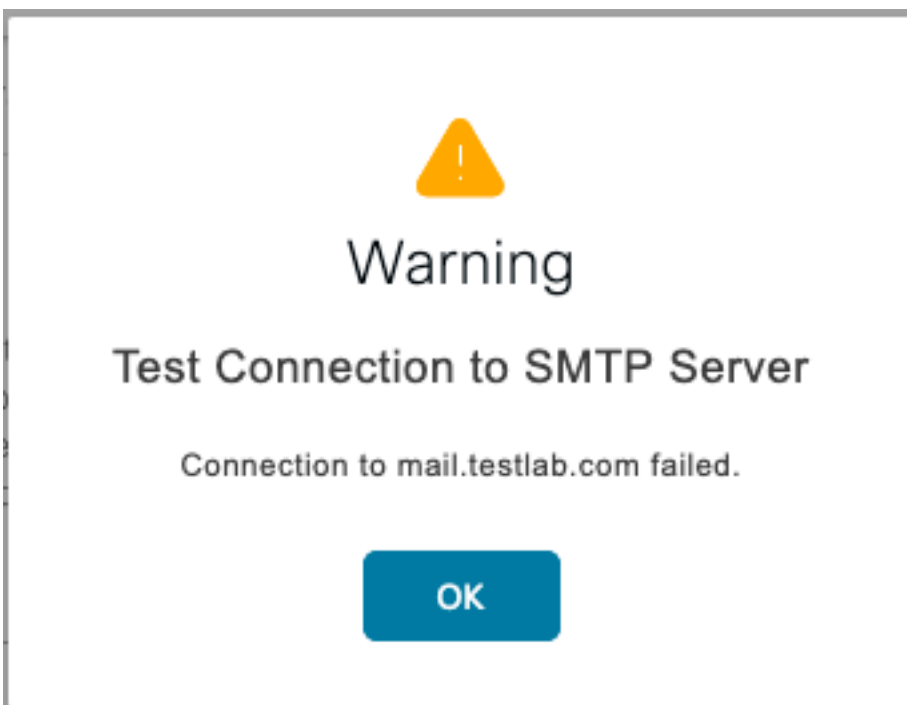
Hier bewijst de pakketheader van de steekproef dat de authenticatie niet succesvol was.

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 V0Wlce5h0w06
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: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

Oplossing: bevestig gebruikersnaam of wachtwoord dat op de TCP server is ingesteld.

Probleem: Test Connection toont: Verbinding met een SMTP-server is mislukt.



Oplossing: Controleer de configuratie van de SMTP-serverpoort of de naam van de SMTP-server kan worden opgelost door de geconfigureerde DNS-server op ISE.

Het voorbeeld hier toont een reset wordt verzonden door de MTP-server op 587 poorten die niet is ingesteld voor de MTP-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= 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)
  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]
```

## Gerelateerde informatie

- [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)
- [Technische ondersteuning en documentatie – Cisco Systems](#)