

Konfigurieren eines sicheren SMTP-Servers auf der ISE

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfiguration](#)

[SMTP-Einstellungen](#)

[Unsichere SMTP-Kommunikationseinstellungen ohne Authentifizierung oder Verschlüsselung](#)

[Sichere SMTP-Kommunikationseinstellungen](#)

[Sichere SMTP-Kommunikation mit Verschlüsselung](#)

[Sichere SMTP-Kommunikation mit aktivierten Authentifizierungseinstellungen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Konfiguration des SMTP-Servers auf der Cisco ISE zur Unterstützung von E-Mail-Benachrichtigungen für mehrere Dienste beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse der Cisco Identity Services Engine (ISE) und des Simple Mail Transfer Protocol (SMTP)-Servers verfügen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt. ISE Version 3.0 unterstützt sowohl gesicherte als auch ungesicherte Verbindungen zum SMTP-Server.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfiguration

In diesem Abschnitt wird die Konfiguration der ISE zur Unterstützung von E-Mail-Benachrichtigungen beschrieben, mit denen folgende Aufgaben durchgeführt werden:

- Senden Sie E-Mail-Warnmeldungen an alle internen Administratoren, wenn die Option Systemwarnungen in E-Mails einschließen aktiviert ist. Die E-Mail-Adresse des Absenders, an die Alarmmeldungen gesendet werden sollen, ist mit `ise@<hostname>` fest codiert.
- Ermöglichen Sie es Sponsoren, Gästen eine E-Mail-Benachrichtigung mit ihren Anmeldeinformationen und Anweisungen zum Zurücksetzen des Kennworts zu senden.
- Ermöglicht Gästen, ihre Anmeldeinformationen automatisch zu erhalten, nachdem sie sich erfolgreich registriert haben, und Maßnahmen zu ergreifen, bevor ihre Gastkonten ablaufen.
- Senden Sie Erinnerungs-E-Mails an ISE-Administratoren/interne Netzwerkbenutzer, die auf der ISE vor Ablauf ihres Kennworts konfiguriert wurden.

SMTP-Einstellungen

Bevor die ISE E-Mail-Services verwenden kann, muss ein SMTP-Relay-Server konfiguriert sein. Um die SMTP-Serverdetails zu aktualisieren, navigieren Sie zu Administration > System > Settings > Proxy > SMTP Server.

Diese Tabelle zeigt, welcher Knoten in einer verteilten ISE-Umgebung eine E-Mail sendet.

Zweck der E-Mail	Knoten, der die E-Mail sendet
Ablauf des Gastkontos	Primärer PAN
Alarmer	Aktives MnT
Benachrichtigungen über Sponsoren- und Gastkonten aus den jeweiligen Portalen	PSN
Kennwortablaufzeiten	Primärer PAN

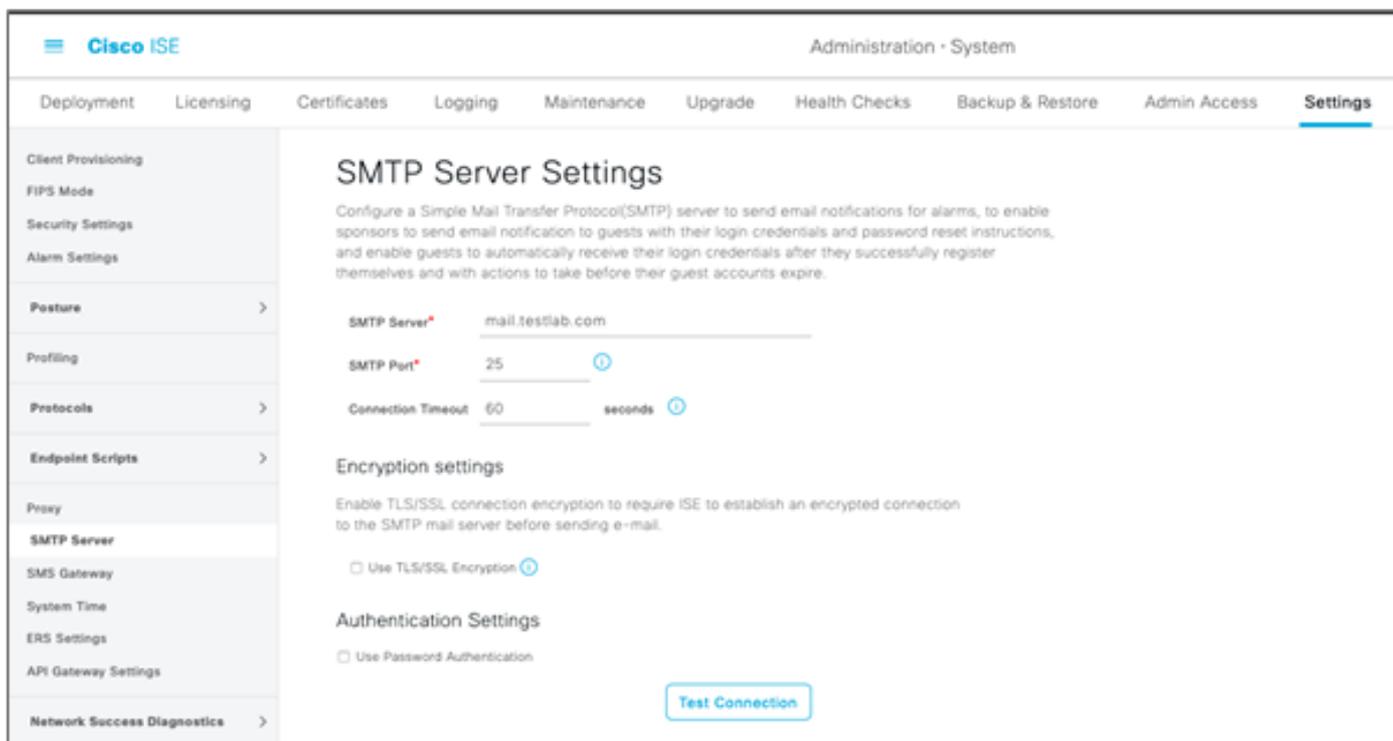
Konfigurieren Sie den SMTP-Server so, dass Sie E-Mails von der ISE mit oder ohne Authentifizierung oder Verschlüsselung je nach Anforderung annehmen können.

Unsichere SMTP-Kommunikationseinstellungen ohne Authentifizierung oder Verschlüsselung

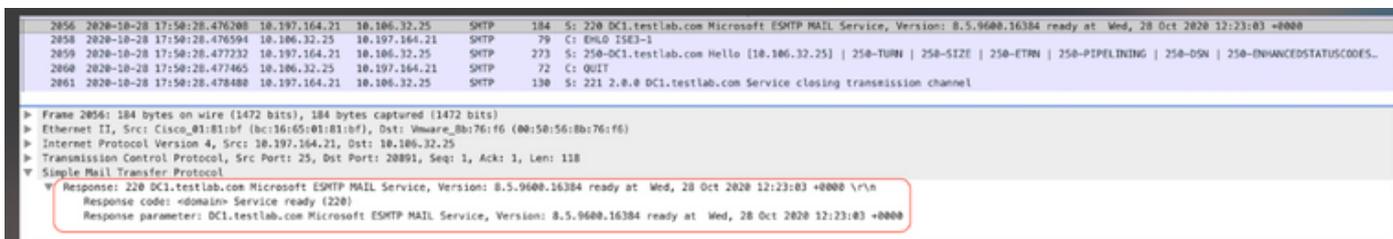
1. Definieren Sie den Hostnamen des SMTP-Servers (ausgehender SMTP-Server).
2. SMTP-Port (dieser Port muss im Netzwerk offen sein, um eine Verbindung zum SMTP-Server herstellen zu können).
3. Connection Timeout (Verbindungszeitüberschreitung) (Geben Sie die maximale Zeit ein, die

Cisco ISE auf eine Antwort vom SMTP-Server wartet.)

4. Klicken Sie auf Verbindung testen und speichern.



Die Paketerfassung zeigt die ISE-Kommunikation mit dem SMTP-Server ohne Authentifizierung oder Verschlüsselung:



Sichere SMTP-Kommunikationseinstellungen

Die gesicherte Verbindung kann auf zwei Arten erfolgen:

1. SSL-basiert
2. Benutzername/Kennwort-basiert

Der verwendete SMTP-Server muss eine SSL- und anmeldeinformationsbasierte Authentifizierung unterstützen. Eine sichere SMTP-Kommunikation kann mit einer der beiden Optionen oder mit beiden Optionen gleichzeitig verwendet werden.

Sichere SMTP-Kommunikation mit Verschlüsselung

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. Konfigurieren Sie den SMTP-Server, konfigurieren den Port auf dem SMTP-Server für verschlüsselte Kommunikation, und aktivieren Sie die Option TLS/SSL-Verschlüsselung verwenden.

The screenshot shows the Cisco ISE Administration - System interface. The left sidebar contains navigation menus for 'Certificate Management' (System Certificates, Trusted Certificates, OCSP Client Profile, Certificate Signing Requests, Certificate Periodic Check Se...) and 'Certificate Authority'. The main content area is titled 'Issuer' and displays the following configuration details:

- * Friendly Name: mail.cisco.com
- Status: Enabled
- Description: (empty)
- 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

Below the configuration details is the 'Usage' section, which includes a 'Trusted For:' dropdown menu and four checkboxes:

- Trust for authentication within ISE
- Trust for client authentication and Syslog
- Trust for certificate based admin authentication
- Trust for authentication of Cisco Services

Die Testverbindung zeigt eine erfolgreiche Verbindung mit dem SMTP-Server an.

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](#)

i

Information

Test Connection to SMTP Server

Successfully connected to mail.testlab.com .

[OK](#)

Paketerfassungen zeigen, dass der Server die STARTTLS-Option akzeptiert hat, wie von der ISE angefordert.

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 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 18:49:25.416658	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_01:01:bf (bc:16:05:01:01:bf), Dst: Vmware_Bb:76:f6 (00:50:56:bb: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
  
```

Sichere SMTP-Kommunikation mit aktivierten Authentifizierungseinstellungen

1. Konfigurieren Sie den SMTP-Server und den SMTP-Port.
2. Aktivieren Sie unter Authentication Settings die Option Use Password Authentication (Kennwortauthentifizierung verwenden), und geben Sie den Benutzernamen und das Kennwort ein.

Erfolgreiche Testverbindung bei passwortbasierter Authentifizierung:

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 information 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](#)

Information

Test Connection to SMTP Server

Successfully connected to mail.testlab.com .

[OK](#)

Beispiel für die Paketerfassung, die eine erfolgreiche Authentifizierung mit Anmeldeinformationen anzeigt:

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 ESMTPL 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 18:43:13.672858	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 VwNlcm5hbwJg
1637	2020-10-28 18:43:13.672703	10.106.32.25	10.197.164.21	SMTP	80	C: User: cG9vbnRhdmcw
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: OyFzY28xMjM=
1640	2020-10-28 18:43:13.672862	10.197.164.21	10.106.32.25	SMTP	103	S: 235 2.7.0 Authentication successful
1641	2020-10-28 18:43:13.672771	10.106.32.25	10.197.164.21	SMTP	72	C: QUIT
1642	2020-10-28 18:43:13.672906	10.197.164.21	10.106.32.25	SMTP	130	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_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: 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

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Verwenden Sie die Option "Verbindung testen", um die Verbindung zum konfigurierten SMTP-Server zu überprüfen.
2. Senden Sie eine Test-E-Mail vom Gastportal unter Work Centers > Guest Access > Portals & Components > Guest Portals > Self-Registered Guest Portal(default) > Portal Page Customization > Notifications > Email > Preview window Settings. Geben Sie eine gültige E-Mail-Adresse ein, und senden Sie eine Test-E-Mail. Der Empfänger muss die E-Mail von der konfigurierten E-Mail-Adresse in den Einstellungen für Gast-E-Mail erhalten.

Beispiel-E-Mail-Benachrichtigung für die Anmeldeinformationen des Gastkontos:

Time	Source	Destination	Protocol	Len	Address	Info
2475	2020-10-26 18:51:33.867597	173.37.102.6	10.106.32.25	SMTP	151 00:50:56:8b:76:f6, bc:16:65:01:81:bf	S: 220 xch-rcc-001.cisco.com Microsoft ESMTS MAIL Service ready at Mon, 26 Oct 2020 08:24:07 -0500
2477	2020-10-26 18:51:33.867998	10.106.32.25	173.37.102.6	SMTP	67 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	C: EHLO ISE3-1
2494	2020-10-26 18:51:34.136372	173.37.102.6	10.106.32.25	SMTP	299 00:50:56:8b:76:f6, bc:16:65:01:81:bf	S: 250 xch-rcc-001.cisco.com Hello [10.106.32.25] 250-SIZE 37748736 250-PIPELINING 250-DSN 250-ENHANCED MAIL FROM: cise@testlab.com
2495	2020-10-26 18:51:34.136729	10.106.32.25	173.37.102.6	SMTP	83 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	C: MAIL FROM: cise@testlab.com
2513	2020-10-26 18:51:34.405187	173.37.102.6	10.106.32.25	SMTP	75 00:50:56:8b:76:f6, bc:16:65:01:81:bf	S: 250 2.1.0 Sender OK
2514	2020-10-26 18:51:34.405472	10.106.32.25	173.37.102.6	SMTP	84 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	C: RCPT TO: spoonarg@cisco.com
2522	2020-10-26 18:51:34.674387	173.37.102.6	10.106.32.25	SMTP	78 00:50:56:8b:76:f6, bc:16:65:01:81:bf	S: 250 2.1.5 Recipient OK
2523	2020-10-26 18:51:34.674586	10.106.32.25	173.37.102.6	SMTP	60 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	C: DATA
2532	2020-10-26 18:51:34.943137	173.37.102.6	10.106.32.25	SMTP	100 00:50:56:8b:76:f6, bc:16:65:01:81:bf	S: 354 Start mail input; end with <CRLF>.<CRLF>
2533	2020-10-26 18:51:34.951091	10.106.32.25	173.37.102.6	SMTP	2714 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	C: DATA Fragment, 2660 bytes
2534	2020-10-26 18:51:34.951927	10.106.32.25	173.37.102.6	SMTP	2714 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	C: DATA Fragment, 2660 bytes
2535	2020-10-26 18:51:34.951932	10.106.32.25	173.37.102.6	SMTP	2714 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	C: DATA Fragment, 2660 bytes
2536	2020-10-26 18:51:34.952109	10.106.32.25	173.37.102.6	SMTP	199 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	C: DATA Fragment, 145 bytes
2537	2020-10-26 18:51:34.950436	10.106.32.25	173.37.102.6	SMTP	2714 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	C: DATA Fragment, 2660 bytes
2540	2020-10-26 18:51:35.220463	10.106.32.25	173.37.102.6	SMTP	2714 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	C: DATA Fragment, 2660 bytes
2561	2020-10-26 18:51:35.220480	10.106.32.25	173.37.102.6	SMTP	2714 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	C: DATA Fragment, 2660 bytes
2563	2020-10-26 18:51:35.220783	10.106.32.25	173.37.102.6	SMTP	2714 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	C: DATA Fragment, 2660 bytes
2564	2020-10-26 18:51:35.220793	10.106.32.25	173.37.102.6	SMTP	2714 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	C: DATA Fragment, 2660 bytes
2566	2020-10-26 18:51:35.220878	10.106.32.25	173.37.102.6	SMTP]	784 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	from: cise@testlab.com, subject: Your Guest Account Credentials, (text/html) (image/png)
2583	2020-10-26 18:51:35.597164	173.37.102.6	10.106.32.25	SMTP	186 00:50:56:8b:76:f6, bc:16:65:01:81:bf	S: 250 2.6.0 <366327400.7.1603718485290@ISE3-1> [InternalId=201137613468157, Hostname=XCH-ALN-001.cisco.com]
2584	2020-10-26 18:51:35.597441	10.106.32.25	173.37.102.6	SMTP	60 bc:16:65:01:81:bf, 00:50:56:8b:76:f6	C: QUIT
2595	2020-10-26 18:51:35.865758	173.37.102.6	10.106.32.25	SMTP	102 00:50:56:8b: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 (00:50:56:8b:76:f6)
Internet Protocol Version 4, Src: 173.37.102.6, Dst: 10.106.32.25
Transmission Control Protocol, Src Port: 25, Dst Port: 22003, 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
    
```

Beispiel für eine E-Mail-Benachrichtigung, die vom E-Mail-Empfänger empfangen wurde:

Your Guest Account Credentials



ise@testlab.com <ise@testlab.com>

To: Poonam Garg (poongarg)



Hello firstname,
Your guest account details:
Username: username
Password: password
First Name: firstname
Last Name: lastname
Mobile Number:NA
Valid From: 2014-11-12 02:06:00
Valid To: 2016-11-12 02:06:00
Person being visited:
Reason for visit:

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration:

Problem: Testverbindung zeigt Folgendes an: "Verbindung zum SMTP-Server konnte nicht hergestellt werden, SSL-Fehler. Bitte überprüfen Sie die vertrauenswürdigen Zertifikate".



Warning

Test Connection to SMTP Server

Connection to mail.testlab.com failed.

Could not connect to SMTP Server, SSL Error. Please check the trusted certificates.

OK

Die Paketerfassung zeigt, dass das vom SMTP-Server bereitgestellte Zertifikat nicht vertrauenswürdig ist:

```
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 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 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 17:50:22.686448 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
1715 2020-10-28 17:50:22.687076 10.106.32.25 10.197.164.21 TLSv1.2 1039 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)
```

Lösung: Importieren Sie das Zertifikat der Stammzertifizierungsstelle des SMTP-Servers in die vertrauenswürdigen ISE-Zertifikate, und wenn auf dem Port die TLS-Unterstützung konfiguriert ist.

Problem: Testverbindung zeigt Folgendes an: "Authentifizierungsfehler: Verbindung zum SMTP-Server konnte nicht hergestellt werden, Benutzername oder Kennwort sind falsch".



Warning

Test Connection to SMTP Server

Connection to mail.testlab.com failed.
Could not connect to SMTP Server, User Name or Password is incorrect.

OK

Die Beispielpaketerfassung hier zeigt, dass die Authentifizierung nicht erfolgreich war.

No.	Time	Source	Destination	Protocol	Length	Info
938	2020-10-28 18:11:40.722253	10.197.164.21	10.106.32.25	SMTP	184	S: 220 DC1.testlab.com Microsoft ESMTP MAIL Service, Version: 0.5.9600.16384 ready at Wed, 28 Oct 2020 12:44:15 +0000
940	2020-10-28 18:11:40.722653	10.106.32.25	10.197.164.21	SMTP	79	C: EHLO ISE3-1
941	2020-10-28 18:11:40.723363	10.197.164.21	10.106.32.25	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
942	2020-10-28 18:11:40.723531	10.106.32.25	10.197.164.21	SMTP	78	C: AUTH LOGIN
946	2020-10-28 18:11:40.729063	10.197.164.21	10.106.32.25	SMTP	84	S: 334 VNW1cm5h0w06
949	2020-10-28 18:11:40.729172	10.106.32.25	10.197.164.21	SMTP	76	C: User: dGVud00u
950	2020-10-28 18:11:40.730056	10.197.164.21	10.106.32.25	SMTP	84	S: 334 UGfzc3dvcm06
951	2020-10-28 18:11:40.730151	10.106.32.25	10.197.164.21	SMTP	80	C: Pass: QyFrY28wMjM=
952	2020-10-28 18:11:40.740181	10.197.164.21	10.106.32.25	SMTP	185	S: 535 5.7.3 Authentication unsuccessful

► Frame 952: 185 bytes on wire (840 bits), 185 bytes captured (840 bits)
► Ethernet II, Src: Cisco_01:81:bf (bc:16:65:81:81: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: 24553, Seq: 394, Ack: 50, Len: 39
▼ Simple Mail Transfer Protocol
 ▼ Response: 535 5.7.3 Authentication unsuccessful
 Response code: Authentication credentials invalid (535)
 Response parameter: 5.7.3 Authentication unsuccessful

Lösung: Validieren Sie den auf dem SMTP-Server konfigurierten Benutzernamen oder das Kennwort.

Problem: Testverbindung zeigt an: "Verbindung zum SMTP-Server fehlgeschlagen".



Warning

Test Connection to SMTP Server

Connection to mail.testlab.com failed.

OK

Lösung: Überprüfen der Konfiguration des SMTP-Server-Ports Überprüfen Sie, ob der SMTP-Servername vom konfigurierten DNS-Server auf der ISE aufgelöst werden kann.

Das Beispiel zeigt, dass ein Reset vom SMTP-Server an einem 587-Port gesendet wird, der nicht für den SMTP-Dienst konfiguriert ist.

```

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 18:24:18.332201 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]

```

Zugehörige Informationen

- [Administratorleitfaden für die Cisco Identity Services Engine, Version 3.0](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.