

Configurazione di Secure SMTP Server su ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Impostazioni SMTP](#)

[Impostazioni di comunicazione SMTP non sicure senza autenticazione o crittografia](#)

[Impostazioni comunicazioni SMTP protette](#)

[Comunicazione SMTP sicura con crittografia abilitata](#)

[Comunicazione SMTP sicura con impostazioni di autenticazione abilitate](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare il server SMTP (Simple Mail Transfer Protocol) su Cisco Identity Services Engine (ISE) per supportare le notifiche e-mail per più servizi. ISE versione 3.0 supporta connessioni protette e non protette al server SMTP.

Contributo di Poonam Garg, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda una conoscenza di base delle funzionalità di Cisco ISE e del server SMTP.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

In questa sezione viene descritta la configurazione dell'ISE per il supporto delle notifiche e-mail utilizzate per:

- Inviare notifiche di allarme via e-mail a tutti gli utenti amministratori interni con l'opzione Inclusione di allarmi di sistema nelle e-mail abilitata. L'indirizzo e-mail del mittente a cui inviare le notifiche di allarme è hardcoded come ise@<hostname>.
- Consentire agli sponsor di inviare una notifica e-mail agli ospiti con le credenziali di accesso e le istruzioni per la reimpostazione della password.
- Consentire agli utenti guest di ricevere automaticamente le credenziali di accesso dopo la registrazione e le azioni da eseguire prima della scadenza degli account guest.
- Inviare un promemoria via e-mail agli utenti amministratori ISE/agli utenti della rete interna configurati sull'ISE prima della data di scadenza della password.

Impostazioni SMTP

Per poter utilizzare i servizi e-mail, ISE deve disporre di un Relay Server SMTP configurato. Per aggiornare i dettagli del server SMTP, selezionare **Amministrazione > Sistema > Impostazioni > Proxy > Server SMTP**.

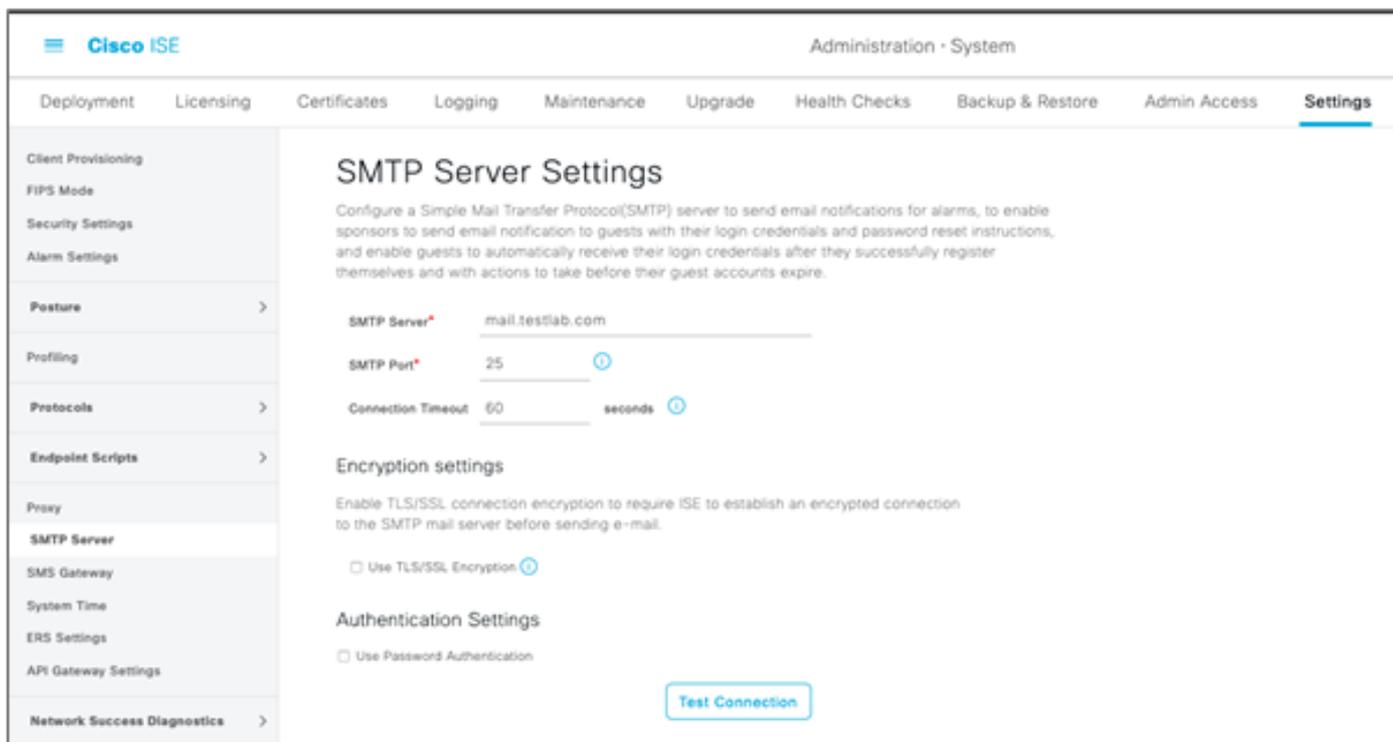
La tabella mostra il nodo di un ambiente ISE distribuito che invia un'e-mail.

Scopo posta elettronica	Nodo che invia l'e-mail
Scadenza account Guest	PAN principale
Allarmi	MnT attivo
Notifiche di account sponsor e guest dai rispettivi portali	PSN
Scadenze password	PAN principale

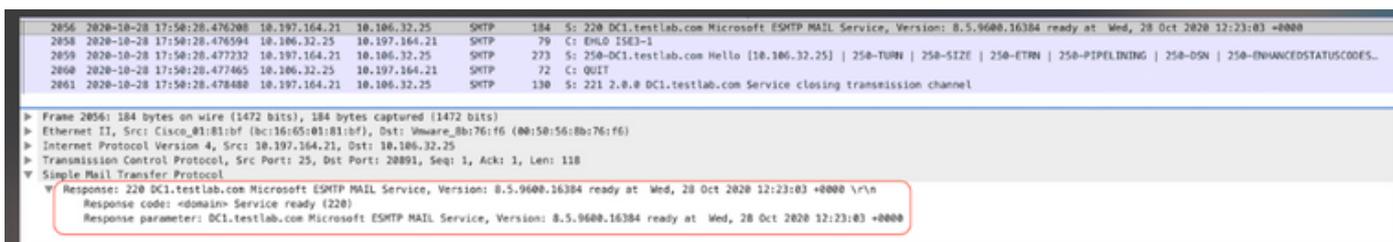
Configurare il server SMTP in modo da poter accettare qualsiasi e-mail dall'ISE con o senza autenticazione o crittografia in base alle proprie esigenze.

Impostazioni di comunicazione SMTP non sicure senza autenticazione o crittografia

1. Definire il nome host del server SMTP (server SMTP in uscita).
2. Porta SMTP (questa porta deve essere aperta nella rete per la connessione al server SMTP).
3. Timeout connessione (immettere il tempo massimo in cui Cisco ISE attende una risposta dal server SMTP).
4. Fare clic su **Test connessione** e su Salva.



Packet Capture mostra la comunicazione ISE con il server SMTP senza autenticazione o crittografia:



Impostazioni comunicazioni SMTP protette

La connessione protetta può essere effettuata in due modi:

1. Basato su SSL
2. Basato su nome utente/password

Il server SMTP utilizzato deve supportare l'autenticazione SSL e basata su credenziali. La comunicazione SMTP protetta può essere utilizzata con una delle due opzioni o entrambe abilitate contemporaneamente.

Comunicazione SMTP sicura con crittografia abilitata

1. Importare il certificato CA radice del certificato del server SMTP nei certificati attendibili ISE con utilizzo: **Trust per l'autenticazione con ISE** e **Trust per l'autenticazione dei client e Syslog**.
2. Configurare il server SMTP, la porta configurata sul server SMTP per la comunicazione crittografata e selezionare l'opzione **Usa crittografia TLS/SSL**.

- 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 connessione: connessione al server SMTP riuscita.

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

Le acquisizioni dei pacchetti mostrano che il server ha accettato l'opzione **STARTTLS** come richiesto da 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)
> Ethernet II, Src: Cisco_01:81:b1:b1 (bc:16:65:01:81: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
  
```

Comunicazione SMTP sicura con impostazioni di autenticazione abilitate

1. Configurare il server SMTP e la porta SMTP.
2. In Authentication Settings (Impostazioni di autenticazione), selezionare l'opzione **Use Password Authentication** (Usa autenticazione password) e fornire il nome utente e la password.

Test connessione riuscito quando l'autenticazione basata su password funziona:

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

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](#)

i

Information

Test Connection to SMTP Server

Successfully connected to mail.testlab.com .

[OK](#)

Esempio di acquisizione di pacchetti con autenticazione riuscita e credenziali:

No.	Time	Source	Destination	Protocol	Leng	Info
1631	2020-10-20 18:43:13.671815	10.197.164.21	10.106.32.25	SMTP	184	S: 220 DC1.testlab.com Microsoft ESMTPL MAIL Service, Version: 8.5.9080.10384 ready at Wed, 20 Oct 2020 13:15:48 +0000
1633	2020-10-20 18:43:13.671279	10.106.32.25	10.197.164.21	SMTP	79	C: EHLO ISE3-1
1634	2020-10-20 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	2020-10-20 18:43:13.672058	10.106.32.25	10.197.164.21	SMTP	78	C: AUTH LOGIN
1636	2020-10-20 18:43:13.672652	10.197.164.21	10.106.32.25	SMTP	84	S: 334 VNN1cmShobMUG
1637	2020-10-20 18:43:13.672793	10.106.32.25	10.197.164.21	SMTP	80	C: User: cG9vbnhncnc=
1638	2020-10-20 18:43:13.673429	10.197.164.21	10.106.32.25	SMTP	84	S: 334 UGFzc3dvccDQ6
1639	2020-10-20 18:43:13.673474	10.106.32.25	10.197.164.21	SMTP	80	C: Pass: DyFzY2BxMjM=
1640	2020-10-20 18:43:13.677862	10.197.164.21	10.106.32.25	SMTP	103	S: 235 2.7.0 Authentication successful
1641	2020-10-20 18:43:13.677271	10.106.32.25	10.197.164.21	SMTP	72	C: QUIT
1642	2020-10-20 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

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

1. Utilizzare l'opzione Test connessione per verificare la connettività al server SMTP

configurato.

2. Invia un messaggio di prova dal portale per gli ospiti nei centri di lavoro > **Accesso guest > Portali e componenti > Portali per gli ospiti > Portale per gli ospiti con registrazione automatica (impostazione predefinita) > Personalizzazione pagina portale > Notifiche > Posta elettronica > Impostazioni finestra di anteprima**, immetti un indirizzo di posta elettronica valido e Invia messaggio di prova. Il destinatario deve ricevere l'e-mail dall'indirizzo e-mail configurato in Impostazioni e-mail guest.

Esempio di notifica tramite posta elettronica inviata per le credenziali dell'account guest:

Time	Source	Destination	Protocol	Leng	Address	Info
2475	2020-10-26 18:51:33.867597	173.37.182.6	SMTP	151	00:50:56:0b:76:f6, bc16:65:01:81:b1:f6	S: 220 xch-rcd-001.cisco.com Microsoft ESMTMP MAIL Service ready at Mon, 26 Oct 2020 08:24:07 -0500
2477	2020-10-26 18:51:33.867980	18.186.32.25	SMTP	67	bc16:65:01:81:b1:f6, 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, bc16:65:01:81:b1:f6	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	bc16:65:01:81:b1:f6, 00:50:56:0b:76:f6	C: MAIL FROM:ciso@testlab.com
2513	2020-10-26 18:51:34.405187	173.37.182.6	SMTP	75	00:50:56:0b:76:f6, bc16:65:01:81:b1:f6	S: 250 2.1.8 Sender OK
2514	2020-10-26 18:51:34.405472	18.186.32.25	SMTP	84	bc16:65:01:81:b1:f6, 00:50:56:0b:76:f6	C: RCPT TO:poongarg@cisco.com
2522	2020-10-26 18:51:34.674387	173.37.182.6	SMTP	78	00:50:56:0b:76:f6, bc16:65:01:81:b1:f6	S: 250 2.1.5 Recipient OK
2523	2020-10-26 18:51:34.674586	18.186.32.25	SMTP	60	bc16:65:01:81:b1:f6, 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, bc16:65:01:81:b1:f6	S: 354 Start mail input; end with <CRLF>.<CRLF>
2533	2020-10-26 18:51:34.951891	18.186.32.25	SMTP	2714	bc16:65:01:81:b1:f6, 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	bc16:65:01:81:b1:f6, 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	bc16:65:01:81:b1:f6, 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	bc16:65:01:81:b1:f6, 00:50:56:0b:76:f6	C: DATA Fragment, 145 bytes
2537	2020-10-26 18:51:34.950436	18.186.32.25	SMTP	2714	bc16:65:01:81:b1:f6, 00:50:56:0b:76:f6	C: DATA Fragment, 2660 bytes
2560	2020-10-26 18:51:35.220463	18.186.32.25	SMTP	2714	bc16:65:01:81:b1:f6, 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	bc16:65:01:81:b1:f6, 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	bc16:65:01:81:b1:f6, 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	bc16:65:01:81:b1:f6, 00:50:56:0b:76:f6	C: DATA Fragment, 2660 bytes
2566	2020-10-26 18:51:35.220870	18.186.32.25	SMTP	764	bc16:65:01:81:b1:f6, 00:50:56:0b:76:f6	From: iseg@testlab.com, subject: Your Guest Account Credentials, (text/html) (image/png)
2583	2020-10-26 18:51:35.597144	173.37.182.6	SMTP	186	00:50:56:0b:76:f6, bc16:65:01:81:b1:f6	S: 250 2.6.0 <366327480.7.160371848320q[ISE3-1]@internal20-201137613468157.Hostname=KCH-ALN-001.cisco.com>
2584	2020-10-26 18:51:35.597441	18.186.32.25	SMTP	60	bc16:65:01:81:b1:f6, 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, bc16:65:01:81:b1:f6	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:b1:f6 (bc16:65:01:81:b1:f6), Dst: Vwarrn_0b: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

Esempio di notifica e-mail ricevuta dal destinatario e-mail:

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:

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione:

Problema: Test connessione: "Impossibile connettersi al server SMTP. Errore SSL. Verificare i certificati protetti".



Packet Capture indica che il certificato presentato dal server SMTP non è attendibile:

```
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 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 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 17:50:22.688448 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
1718 2020-10-28 17:50:22.688076 10.106.32.25 10.197.164.21 TLSv1.2 1038 Application Data
▶ Frame 1710: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on 0
▶ 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)
```

Soluzione: Importare il certificato CA radice del server SMTP nei certificati ISE Trusted e se il supporto TLS è configurato sulla porta.

Problema: Test connessione: Errore di autenticazione: Impossibile connettersi al server SMTP. Nome utente o password non corretti.



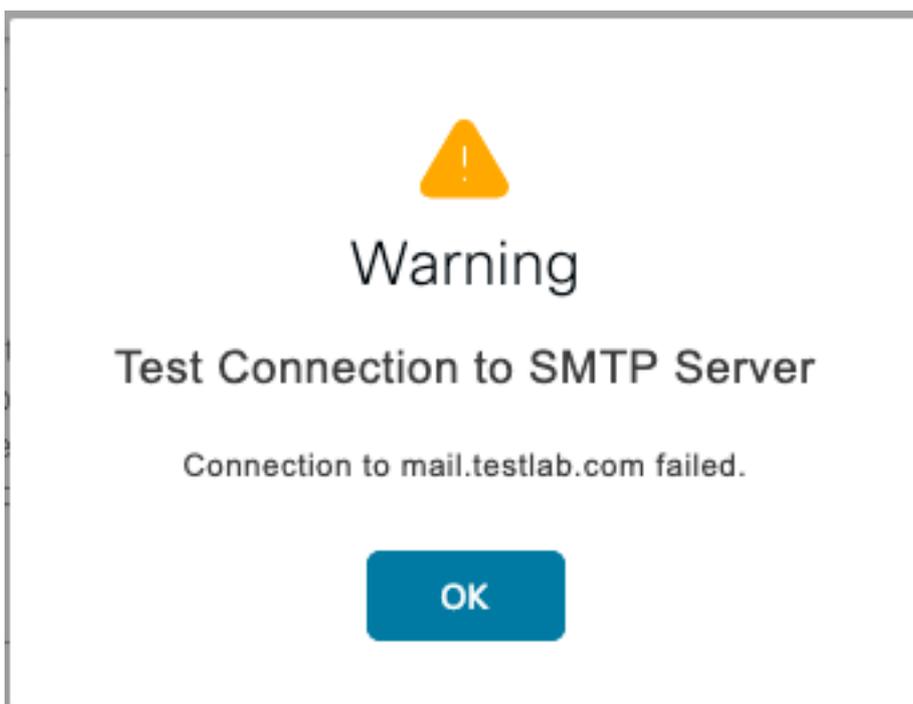
L'acquisizione di un pacchetto di esempio mostra che l'autenticazione non è riuscita.

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 ESMTM 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 VbVlcw5hbw06
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 UGFzc3dvcw06
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

Soluzione: Convalida nome utente o password configurati sul server SMTP.

Problema: Test connessione: Connessione al server SMTP non riuscita.



Soluzione: Verificare la configurazione della porta del server SMTP e verificare se il nome del server SMTP può essere risolto dal server DNS configurato in ISE.

Nell'esempio riportato di seguito viene indicato che il server SMTP invia una reimpostazione sulla porta 587 che non è configurata per il servizio SMTP.

```
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... @... = 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]
```

Informazioni correlate

- 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
- [Documentazione e supporto tecnico – Cisco Systems](#)