

# ISEでのセキュアSMTPサーバの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[コンフィギュレーション](#)

[SMTP 設定](#)

[認証または暗号化を使用しないセキュアでないSMTP通信設定](#)

[セキュアSMTP通信設定](#)

[暗号化が有効なセキュアSMTP通信](#)

[認証設定を有効にしたセキュアSMTP通信](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、Cisco Identity Services Engine(ISE)でSimple Mail Transfer Protocol(SMTP)サーバを設定して、複数のサービスの電子メール通知をサポートする方法について説明します。ISEバージョン3.0は、SMTPサーバへのセキュアな接続とセキュアでない接続の両方をサポートします。

著者 : Cisco TACエンジニア、Poonam Garg

## 前提条件

### 要件

Cisco ISEおよびSMTPサーバの機能に関する基本的な知識があることが推奨されます。

### 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## コンフィギュレーション

このセクションでは、次の目的で使用される電子メール通知をサポートするためのISEの設定について説明します。

- [Inclusion of system alarms in emails]オプションが有効になっている内部管理者ユーザに電子メールアラーム通知を送信します。アラーム通知を送信する送信者の電子メールアドレスは、ise@<hostname>としてハードコードされています。
- スポンサーが、ログイン認証情報とパスワードのリセット手順を使用してゲストに電子メール通知を送信できるようにします。
- ゲストがログイン資格情報を自動的に受信できるようにし、登録が成功した後、ゲストアカウントが期限切れになる前に実行するアクションを設定します。
- パスワードの有効期限が切れる前に、ISEで設定されたISE管理者ユーザ/内部ネットワークユーザにリマインダ電子メールを送信します。

## SMTP 設定

ISEが任意の電子メールサービスを使用するには、SMTPリレーサーバが設定されている必要があります。SMTPサーバの詳細を更新するには、[Administration] > [System] > [Settings] > [Proxy] > [SMTP server]に移動します。

次の表に、分散ISE環境のどのノードが電子メールを送信するかを示します。

電子メールの目的	電子メールを送信するノード
ゲストアカウントの有効期限	プライマリPAN
アラーム	アクティブMnT
各ポータルからのスポンサーおよびゲストアカウント通知	PSN
パスワードの有効期限	プライマリPAN

要件に基づいて、認証または暗号化の有無に関係なく、ISEからの電子メールを受け入れることができるように、SMTPサーバを設定します。

### 認証または暗号化を使用しないセキュアでないSMTP通信設定

1. SMTPサーバのホスト名 (送信SMTPサーバ) を定義します。
2. SMTPポート (SMTPサーバに接続するには、このポートがネットワークで開いている必要があります)。
3. 接続タイムアウト (Cisco ISEがSMTPサーバからの応答を待機する最大時間を入力します)。
4. [接続のテストと保存]をクリックします。

パケットキャプチャは、認証または暗号化を使用しないSMTPサーバとのISE通信を示します。

```

2856 2020-10-28 17:58:28.476288 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 12:23:03 +0000
2858 2020-10-28 17:58:28.476594 10.106.32.25 10.197.164.21 SMTP 79 C: EHLO ISE3-1
2859 2020-10-28 17:58:28.477232 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...
2860 2020-10-28 17:58:28.477465 10.106.32.25 10.197.164.21 SMTP 72 C: QUIT
2861 2020-10-28 17:58:28.478888 10.197.164.21 10.106.32.25 SMTP 130 S: 221 2.0@ DC1.testlab.com Service closing transmission channel

> Frame 2856: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits) on interface 0
> Ethernet II, Src: Cisco_01:81:bf:(bc:16:65:01:81:bf), Dst: Vmware_08:00:56:76: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
Simple Mail Transfer Protocol
  Response: 220 DC1.testlab.com Microsoft ESMTPL 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 ESMTPL MAIL Service, Version: 8.5.9600.16384 ready at Wed, 28 Oct 2020 12:23:03 +0000

```

## セキュアSMTP通信設定

セキュアな接続は、次の2つの方法で行うことができます。

1. SSLベース
2. ユーザ名/パスワードベース

使用するSMTPサーバは、SSLおよびクレデンシャルに基づく認証をサポートしている必要があります。セキュアなSMTP通信は、オプションのいずれかまたは両方のオプションを同時に有効にして使用できます。

### 暗号化が有効なセキュアSMTP通信

1. ISEの信頼できる証明書でSMTPサーバ証明書のルートCA証明書を次の使用法でインポートします。ISE内の認証に対する信頼と、クライアント認証およびSyslogに対する信頼。
2. SMTPサーバ、暗号化通信のためにSMTPサーバに構成されたポートを構成し、[Use TLS/SSL encryption]オプションをオンにします。

## 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]には、SMTPサーバへの正常な接続が表示されます。

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\* 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

パケットキャプチャは、サーバがISEの要求に応じてSTARTTLSオプションを受け入れたことを示します。

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 ESMTPL MAIL Service, Version: 8.5.9600.16384 ready at Wed, 28 Oct 2020 13:22:00 +0000
832	2020-10-28 18:49:25.415860	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), 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
  
```

## 認証設定を有効にしたセキュアSMTP通信

1. SMTPサーバとSMTPポートを設定します。
2. [Authentication Settings]で、[Use Password Authentication]オプションをオンにし、ユーザー名とパスワードを入力します。

パスワードベースの認証が動作する場合の接続のテストに成功しました :

Administration · System

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 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](#)

i

### Information

**Test Connection to SMTP Server**

Successfully connected to mail.testlab.com .

[OK](#)

クレデンシアルを使用した正常な認証を示すパケットキャプチャの例：

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 ESMTS 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 VMM1cmDh0mJUG
1637	2020-10-20 18:43:13.672793	10.106.32.25	10.197.164.21	SMTP	80	C: User: cG9vbnRhdncnc=
1638	2020-10-20 18:43:13.673429	10.197.164.21	10.106.32.25	SMTP	84	S: 334 UGFzc3dvccnDQ6
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	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\_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

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

1. 設定されたSMTPサーバへの接続を確認するには、[Test Connection]オプションを使用しま

す。

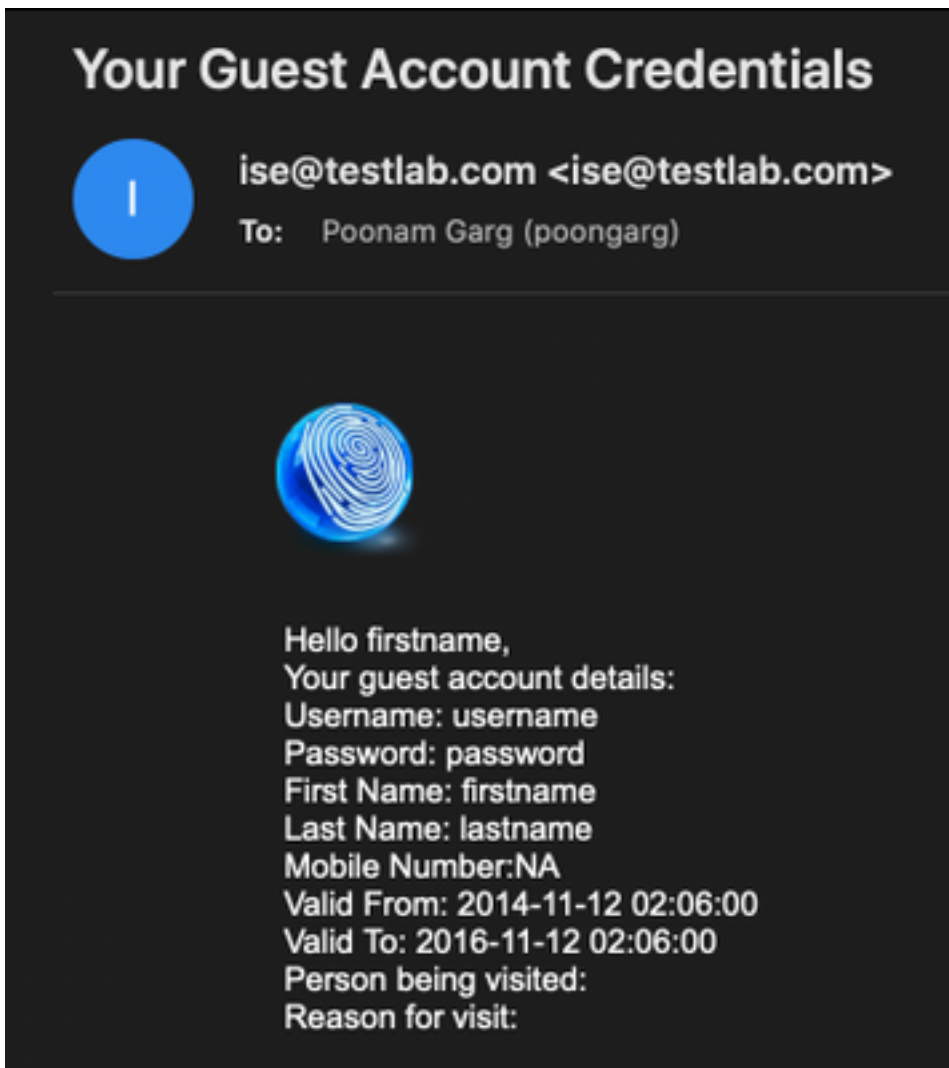
2. テストメールをゲストポータルから [Work Centers] > [Guest Access] > [Portals & Components] > [Guest Portals] > [Self-Registered Guest Portal(default)] > [Portal Page Customization] > [Notifications] > [Email] > [Preview window Settings]で送信します。受信者は、[Guest Email Settings]の設定された電子メールアドレスから電子メールを受信する必要があります。

ゲストアカウントのクレデンシャルに送信される電子メール通知の例：

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 18:51:33.867998	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 18:51:34.405811	173.37.182.6	SMTP	17	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 18:51:35.597344	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	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
```

電子メール受信者が受信した電子メール通知の例：





# トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

問題：テスト接続の表示：「Could not connect to SMTP Server, SSL Error.Please check the trusted certificates」。



パケットキャプチャは、SMTPサーバによって提示された証明書が信頼されていないことを示します。

Time	Source IP	Destination IP	Protocol	Source Port	Destination Port	Length	Info
1698	10.106.32.25	10.197.164.21	TCP	20881	25	74	20881 -> 25 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=462914246 TSecr=0 MS=128
1700	10.106.32.25	10.197.164.21	TCP	20881	25	66	20881 -> 25 [ACK] Seq=1 Ack=1 Min=29312 Len=0 TSval=462914248 TSecr=919415203
1702	10.106.32.25	10.197.164.21	TCP	20881	25	66	20881 -> 25 [ACK] Seq=1 Ack=119 Min=29312 Len=0 TSval=462914249 TSecr=919415203
1703	10.106.32.25	10.197.164.21	SMTP			79	C: EHLO ISE3-1
1705	10.106.32.25	10.197.164.21	SMTP			76	C: STARTTLS
1707	10.106.32.25	10.197.164.21	TLSv1.2			238	Client Hello
1709	10.106.32.25	10.197.164.21	TCP	20881	25	66	20881 -> 25 [ACK] Seq=196 Ack=2295 Win=34176 Len=0 TSval=462914267 TSecr=919415205
1710	10.106.32.25	10.197.164.21	TLSv1.2			73	Alert (Level: Fatal, Description: Certificate Unknown)
1711	10.106.32.25	10.197.164.21	TCP	20881	25	66	20881 -> 25 [FIN, ACK] Seq=203 Ack=2295 Win=34176 Len=0 TSval=462914273 TSecr=919415205
1714	10.106.32.25	10.197.164.21	TCP	20881	25	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)

ソリューション：ISEの[Trusted Certificates]にSMTPサーバのルートCA証明書をインポートします。また、ポートでTLSサポートが設定されている場合は、

問題：[Test Connection]に次のように表示されます。認証の失敗:SMTPサーバーに接続できませんでした。ユーザー名またはパスワードが正しくありません。





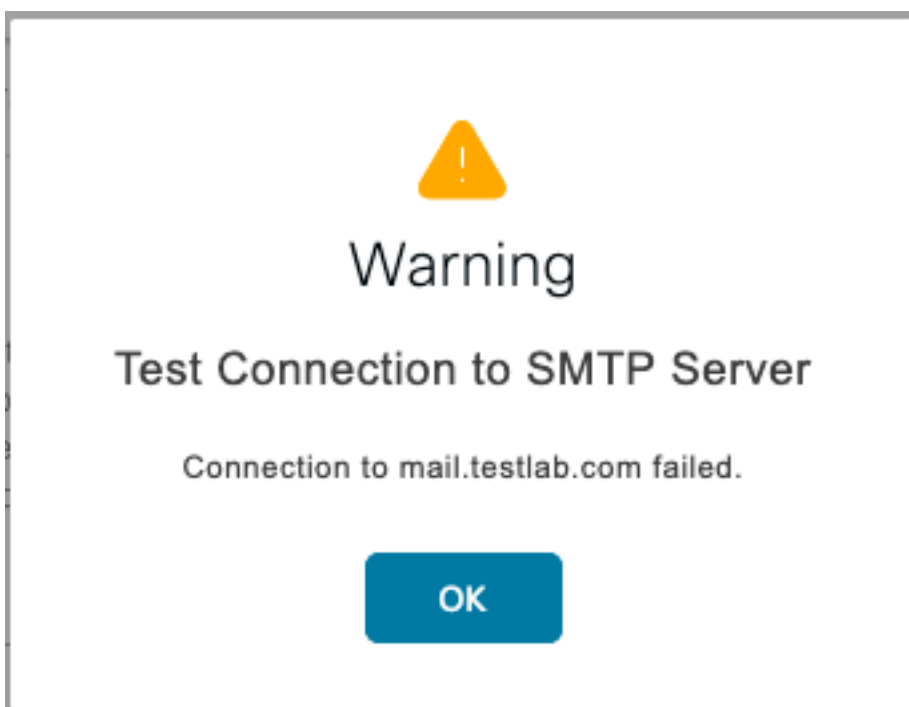
次のパケットキャプチャ例は、認証が失敗したことを示しています。

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 VbWlce5hbw06
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

ソリューション：SMTPサーバに設定されているユーザ名またはパスワードを確認します。

問題：[Test Connection]に次のように表示されます。SMTPサーバーへの接続に失敗しました。



ソリューション：SMTPサーバポートの設定を確認し、SMTPサーバ名がISE上の設定済みDNSサーバによって解決できるかどうかを確認します。

次の例は、SMTPサービスに設定されていない587ポートのSMTPサーバからリセットが送信されることを示しています。

```
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 [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
▶ ....01 = Reset: Set
  ....00 = Syn: Not set
  ....00 = 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]
```

## 関連情報

- [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)
- [テクニカル サポートとドキュメント - Cisco Systems](#)