

Configurer le serveur SMTP sécurisé sur ISE

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Paramètres SMTP](#)

[Paramètres de communication SMTP non sécurisés sans authentification ou chiffrement](#)

[Paramètres de communication SMTP sécurisés](#)

[Communication SMTP sécurisée avec cryptage activé](#)

[Communication SMTP sécurisée avec paramètres d'authentification activés](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer le serveur SMTP (Simple Mail Transfer Protocol) sur Cisco Identity Services Engine (ISE) afin de prendre en charge les notifications par e-mail pour plusieurs services. ISE version 3.0 prend en charge les connexions sécurisées et non sécurisées au serveur SMTP.

Contribué par Poonam Garg, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande d'avoir une connaissance de base des fonctionnalités de Cisco ISE et de serveur SMTP.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Cette section décrit la configuration de ISE afin de prendre en charge les notifications par e-mail

utilisées pour :

- Envoyez des notifications d'alarme par e-mail à tous les utilisateurs internes de l'administrateur lorsque l'option Inclusion des alarmes système dans les e-mails est activée. L'adresse e-mail de l'expéditeur pour envoyer des notifications d'alarme est codée en dur comme ise@<hostname>.
- Permettre aux sponsors d'envoyer une notification par e-mail aux invités avec leurs identifiants de connexion et leurs instructions de réinitialisation de mot de passe.
- Permettre aux invités de recevoir automatiquement leurs informations d'identification de connexion après s'être inscrits correctement et les actions à entreprendre avant l'expiration de leurs comptes d'invité.
- Envoyer des e-mails de rappel aux utilisateurs d'administration ISE/aux utilisateurs internes du réseau configurés sur l'ISE avant la date d'expiration de leur mot de passe.

Paramètres SMTP

Pour que ISE puisse utiliser n'importe quel service de messagerie, un serveur de relais SMTP doit être configuré. Afin de mettre à jour les détails du serveur SMTP, accédez à **Administration > System > Settings > Proxy > SMTP server**.

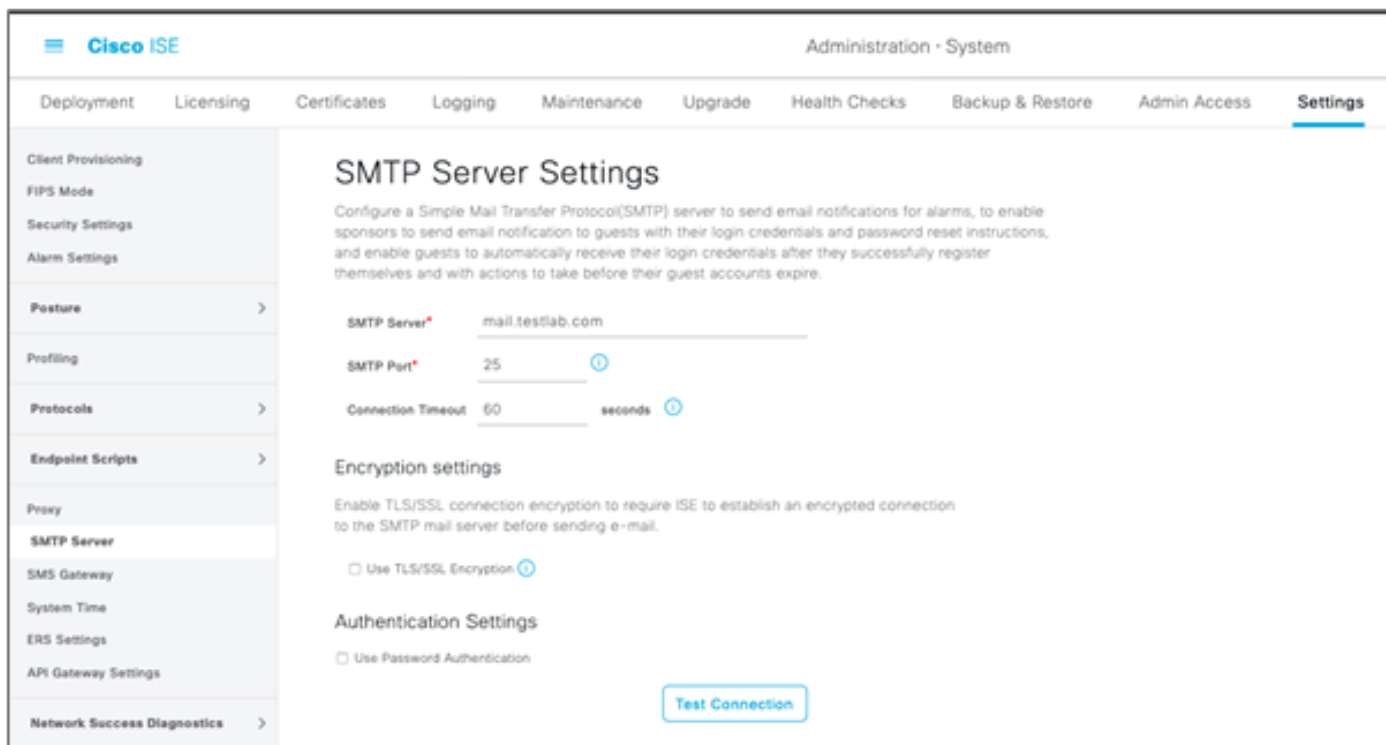
Ce tableau indique quel noeud d'un environnement ISE distribué envoie un e-mail.

Objet du courrier électronique	Noeud qui envoie l'e-mail
Expiration du compte invité	PAN principal
Alarmes	MnT actif
Notifications de compte de sponsor et d'invité depuis les portails respectifs	PSN
Expiration du mot de passe	PAN principal

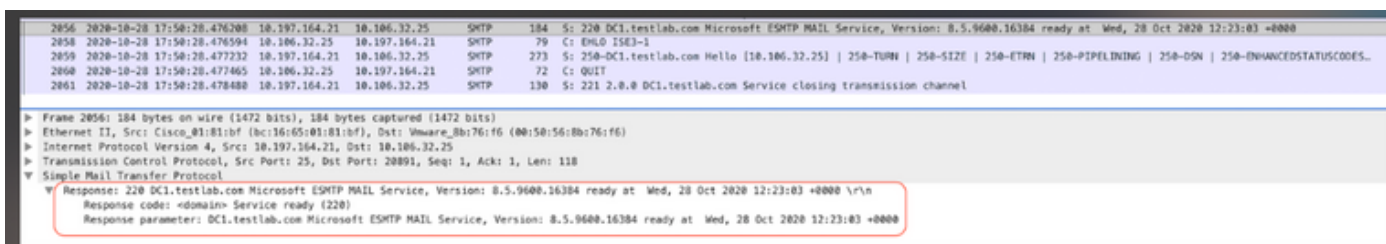
Configurez le serveur SMTP afin d'avoir la possibilité d'accepter tous les e-mails de l'ISE avec ou sans authentification ou chiffrement en fonction de vos besoins.

Paramètres de communication SMTP non sécurisés sans authentification ou chiffrement

1. Définissez le nom d'hôte du serveur SMTP (serveur SMTP sortant).
2. Port SMTP (ce port doit être ouvert sur le réseau pour se connecter au serveur SMTP).
3. Délai d'attente de connexion (saisissez le délai maximal d'attente d'une réponse du serveur SMTP par Cisco ISE).
4. Cliquez sur **Tester la connexion** et Enregistrer.



La capture de paquets montre la communication ISE avec le serveur SMTP sans authentification ni chiffrement :



Paramètres de communication SMTP sécurisés

La connexion sécurisée peut être établie de deux manières :

1. Basé sur SSL
2. Nom d'utilisateur/Mot de passe

Le serveur SMTP utilisé doit prendre en charge l'authentification basée sur SSL et les informations d'identification. La communication SMTP sécurisée peut être utilisée avec l'une des options ou les deux options activées simultanément.

Communication SMTP sécurisée avec cryptage activé

1. Importer le certificat d'autorité de certification racine du certificat du serveur SMTP dans les certificats de confiance ISE avec utilisation : **Confiance pour l'authentification dans ISE et Confiance pour l'authentification client et Syslog.**
2. Configurez le serveur SMTP, le port configuré sur le serveur SMTP pour la communication chiffrée, et cochez l'option **Utiliser le chiffrement 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

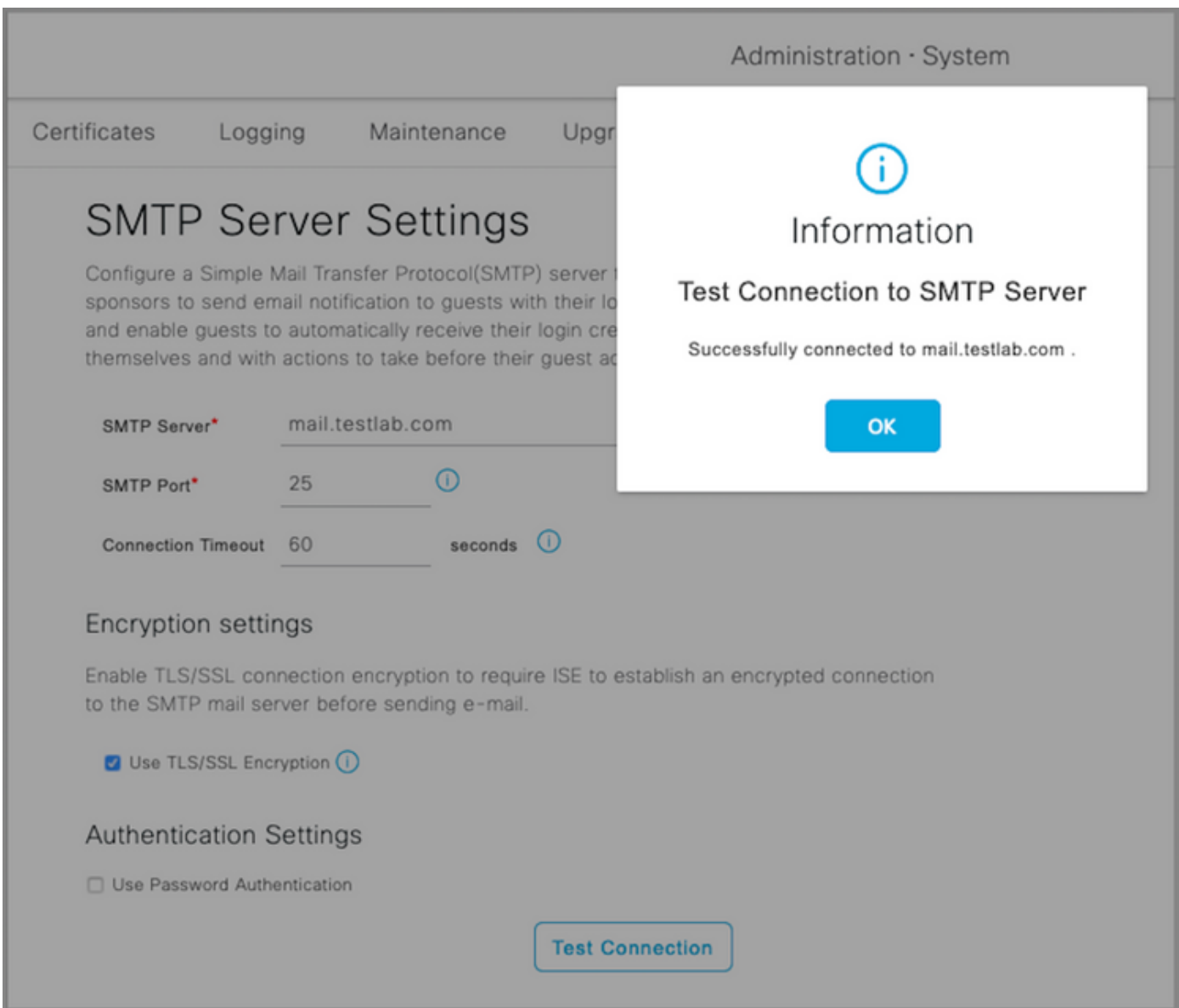
Signature Algorithm SHA256WITHRSA

Key Length 2048

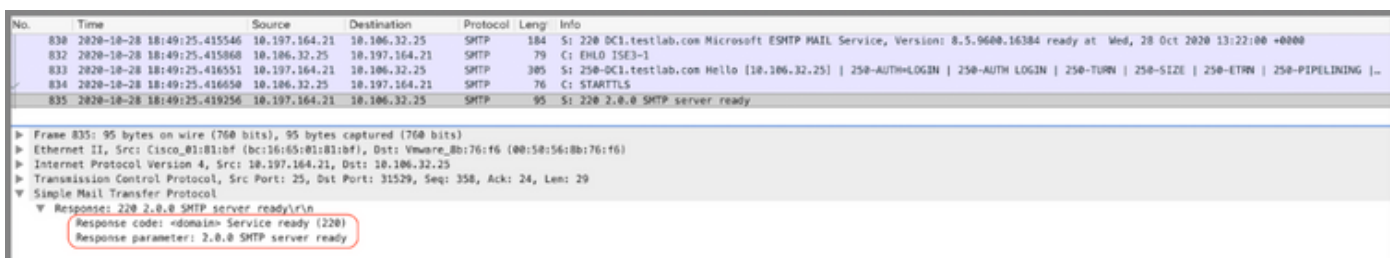
Usage

- 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 Connection indique une connexion réussie au serveur SMTP.



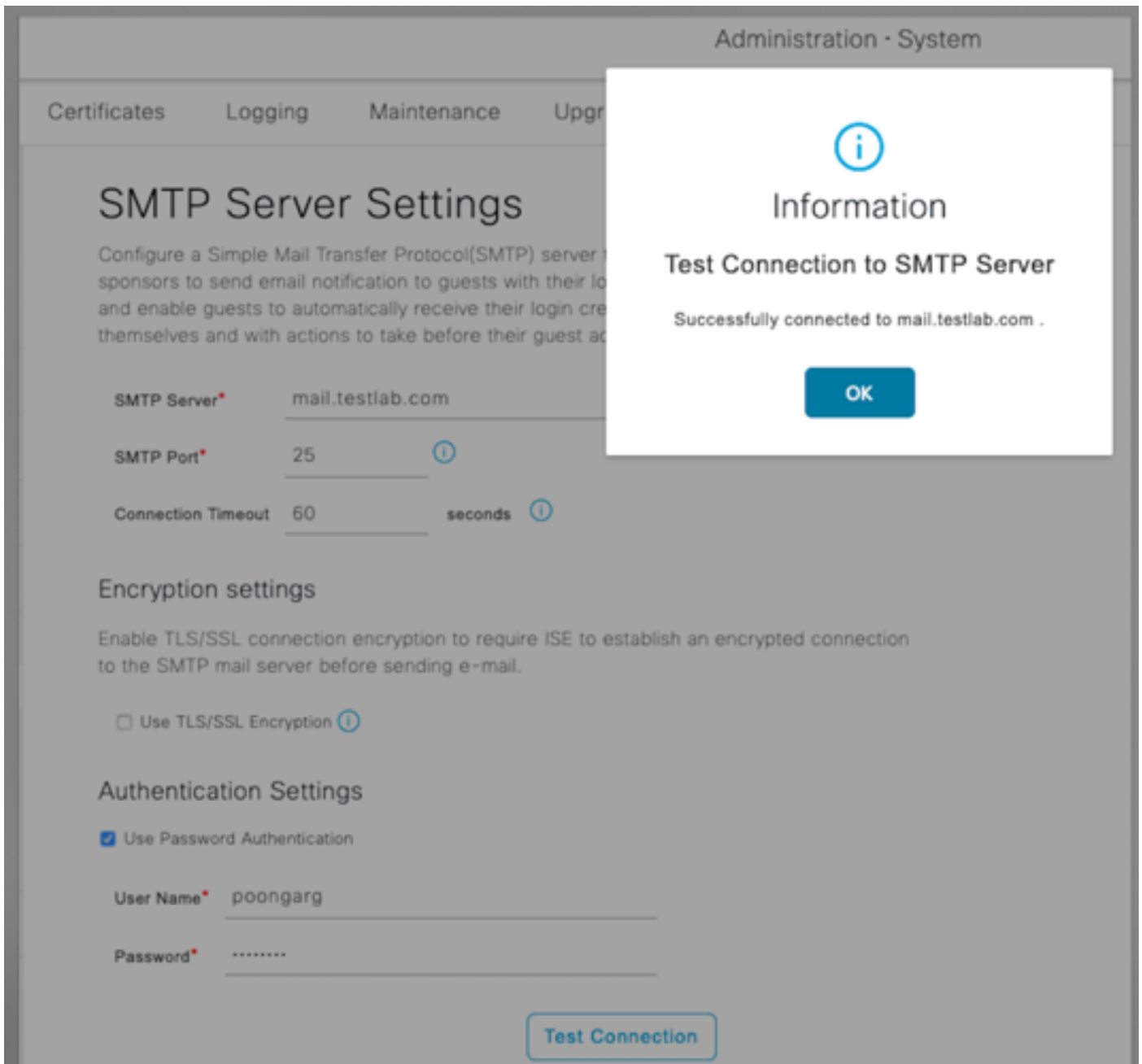
Les captures de paquets montrent que le serveur a accepté l'option **STARTTLS** comme demandé par l'ISE.



Communication SMTP sécurisée avec paramètres d'authentification activés

1. Configurez le serveur SMTP et le port SMTP.
2. Sous Authentication Settings, cochez l'option **Use Password Authentication** et indiquez le nom d'utilisateur et le mot de passe.

Test réussi de connexion lorsque l'authentification basée sur un mot de passe fonctionne :



Exemple de capture de paquets qui montre l'authentification réussie avec les informations d'identification :

No.	Time	Source	Destination	Protocol	Length	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 ESMTIP MAIL Service, Version: 6.5.9688.16384 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 V0W1cn5hbMUG
1637	2020-10-28 18:43:13.672783	10.106.32.25	10.197.164.21	SMTP	80	C: User: c69vbedhcnc=
1638	2020-10-28 18:43:13.673429	10.197.164.21	10.106.32.25	SMTP	84	S: 334 UGFzc3dvccO6
1639	2020-10-28 18:43:13.673474	10.106.32.25	10.197.164.21	SMTP	80	C: Pass: QyFz728xMjM=
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	130	S: 221 2.0.0 DC1.testlab.com Service closing transmission channel

> Frame 1640: 183 bytes on wire (1824 bits), 183 bytes captured (1824 bits)
 > Ethernet II, Src: Cisco_01:81:bf (bc:16:65:01:81:bf), Dst: Vmware_80:76:r6 (00:50:56:8b:76:r6)
 > 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

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

1. Utilisez l'option Tester la connexion afin de vérifier la connectivité au serveur SMTP

configuré.

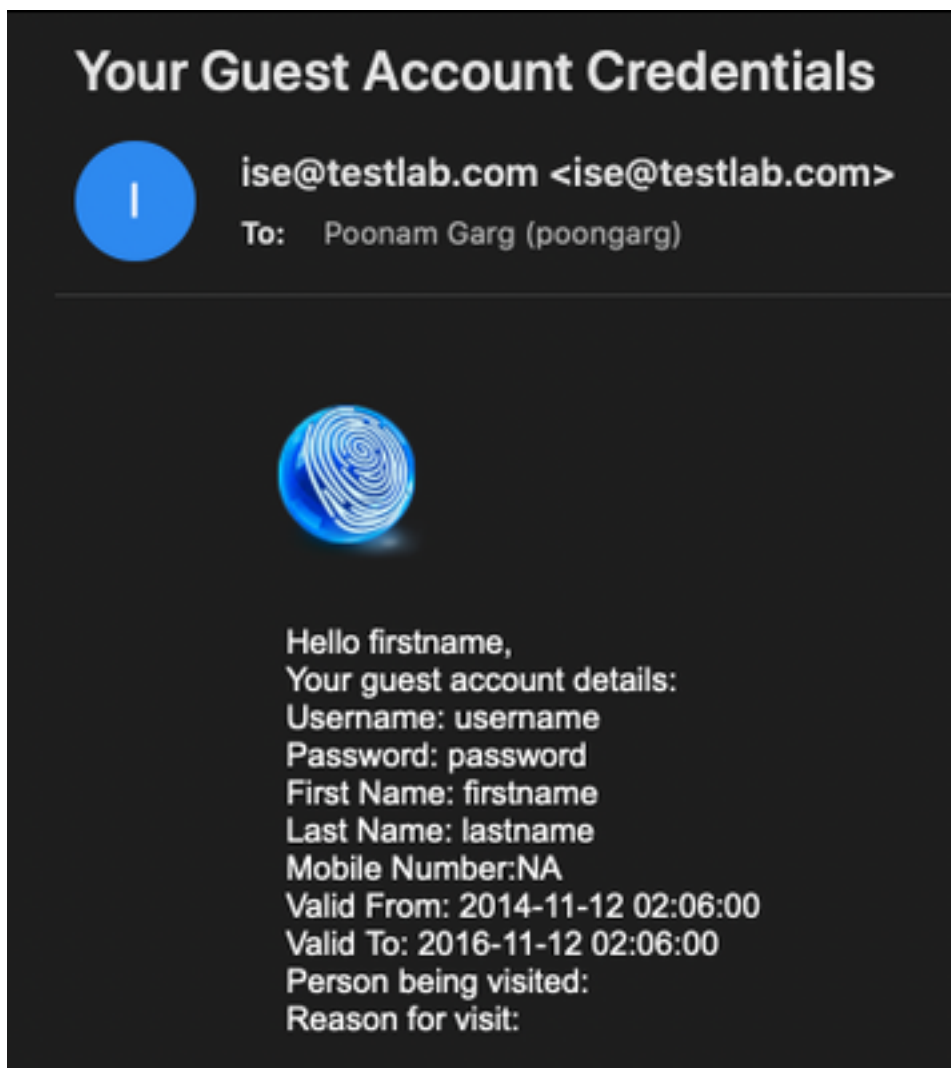
2. Envoyer un e-mail de test à partir du portail Invité à partir de **Work Centers > Guest Access > Portals & Components > Guest Portals > Self Registered Guest Portal (default) > Portal Page Customization > Notifications > Email > Preview window Settings**, saisissez une adresse e-mail valide et envoyez un e-mail de test. Le destinataire doit recevoir l'e-mail à partir de l'adresse e-mail configurée sous Guest Email Settings.

Exemple de notification par e-mail envoyée pour les informations d'identification du compte invité :

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-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 18:51:35.033511	173.37.182.6	SMTP	17	00:50:56:0b:76:f6, bc:16:65:01:81:bf	S: 250 2.1.5 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=201137613468157, 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
```

Exemple de notification par e-mail reçue par le destinataire de l'e-mail :



Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration :

Problème : La connexion de test montre : « Impossible de se connecter au serveur SMTP, erreur SSL. Veuillez vérifier les certificats de confiance ».



La capture de paquets montre que le certificat présenté par le serveur SMTP n'est pas fiable :

Time	Source IP	Destination IP	Protocol	Length	Source Port	Destination Port	Sequence	Flags	Window	Length	Source	Destination
1698	10.106.32.25	10.197.164.21	TCP	74	20881	25	29200	SYN	0	1468	SACK_PERM=1	TSeq=462914246 TSecr=0 MS=128
1700	10.106.32.25	10.197.164.21	TCP	66	20881	25	29312	ACK	1	0		TSeq=462914248 TSecr=919415203
1702	10.106.32.25	10.197.164.21	TCP	66	20881	25	29312	ACK	119	0		TSeq=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	66	20881	25	2295	ACK	196	34176		TSeq=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	66	20881	25	2295	FIN, ACK	203	34176		TSeq=462914273 TSecr=919415205
1714	10.106.32.25	10.197.164.21	TCP	66	20881	25	2296	ACK	204	34176		TSeq=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)

Solution : Importez le certificat d'autorité de certification racine du serveur SMTP dans les certificats de confiance ISE et si la prise en charge de TLS est configurée sur le port.

Problème : Test Connection affiche : Échec de l'authentification : Impossible de se connecter au serveur SMTP, le nom d'utilisateur ou le mot de passe est incorrect.



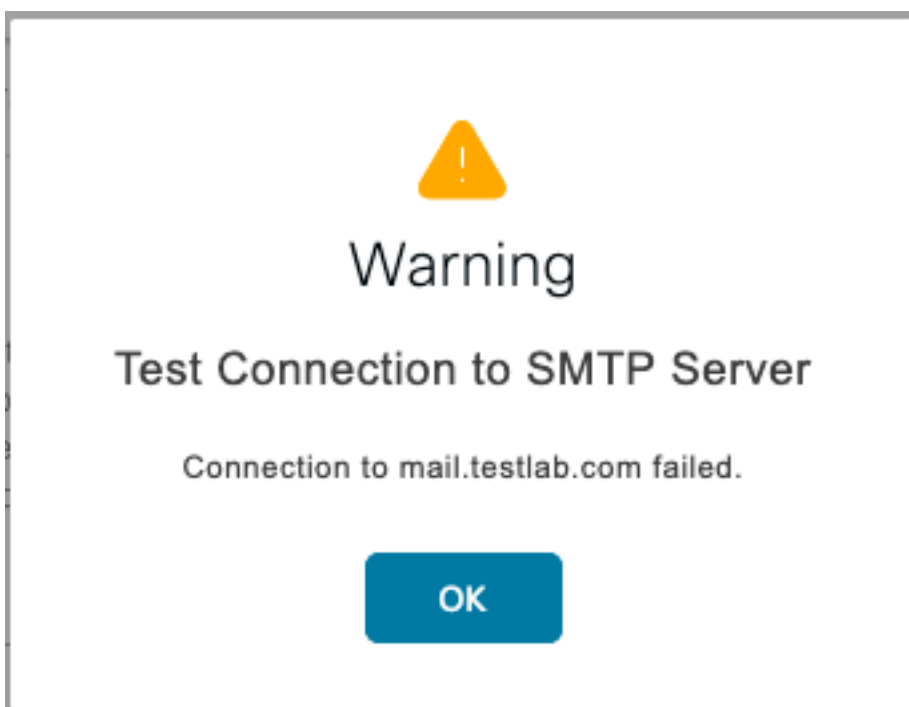
L'exemple de capture de paquets ici montre que l'authentification n'a pas réussi.

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 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_B0:76: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

Solution : Validez le nom d'utilisateur ou le mot de passe configuré sur le serveur SMTP.

Problème : Test Connection affiche : Échec de la connexion au serveur SMTP.



Solution : Vérifiez la configuration du port du serveur SMTP. Vérifiez si le nom du serveur SMTP peut être résolu par le serveur DNS configuré sur ISE.

L'exemple ci-dessous montre qu'une réinitialisation est envoyée par le serveur SMTP sur le port 587 qui n'est pas configuré pour le service 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= 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...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]
```

Informations connexes

- 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
- [Support et documentation techniques - Cisco Systems](#)