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.**

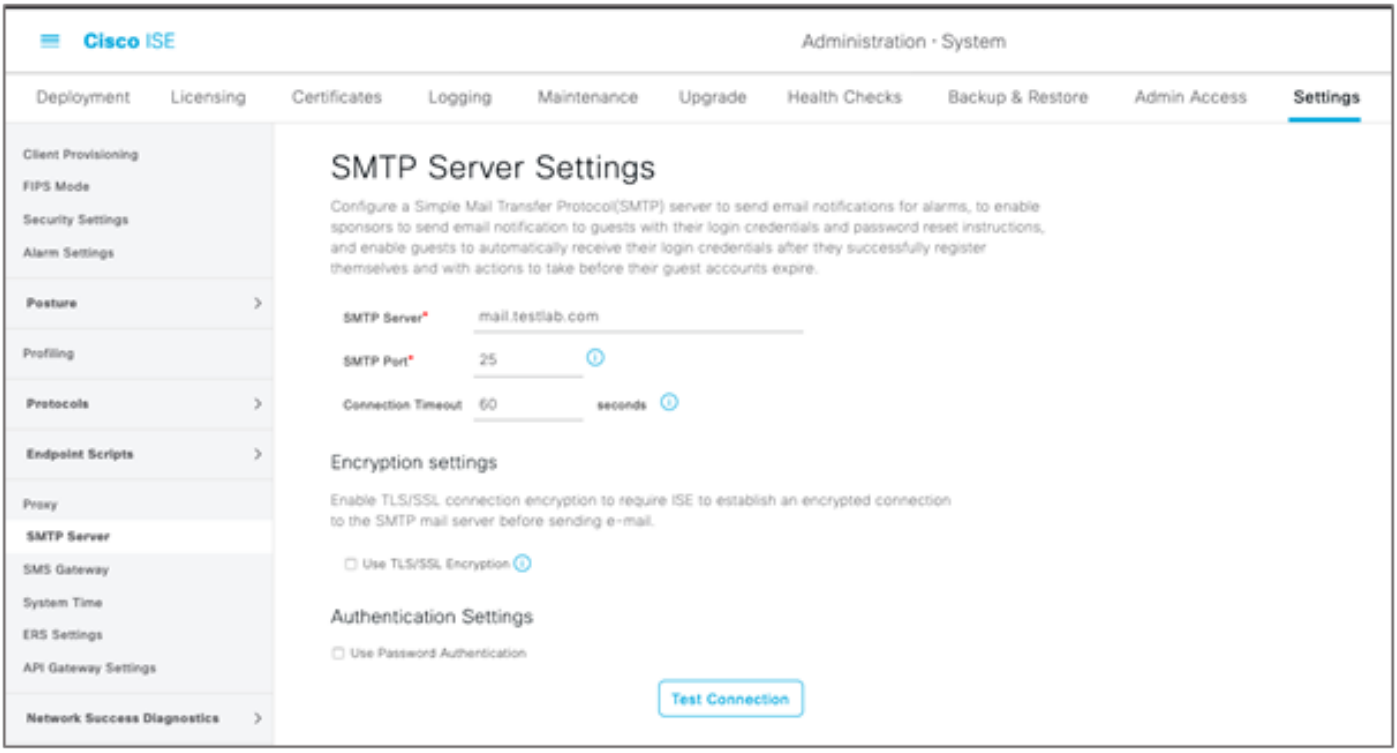
Ce tableau indique quel noeud d'un environnement ISE distribué envoie un e-mail.

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

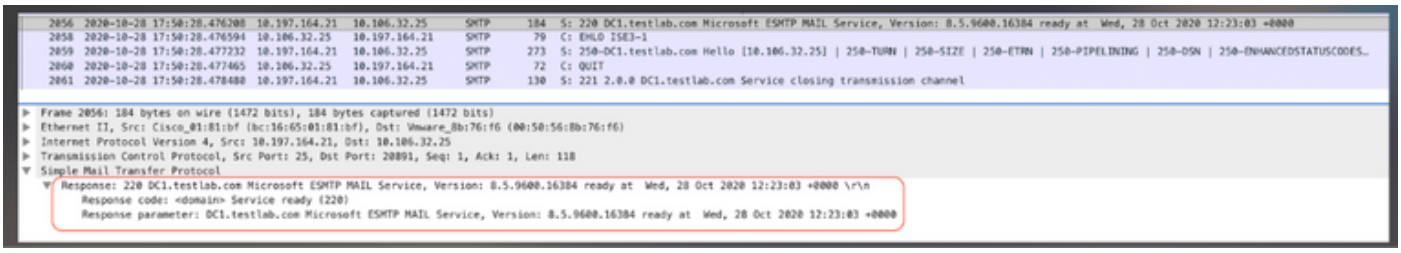
Configurez le serveur SMTP afin d'avoir la possibilité d'accepter tous les e-mails de l'ISE avec ou sans authentification ou chiffrement en fonction de vos besoins.

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

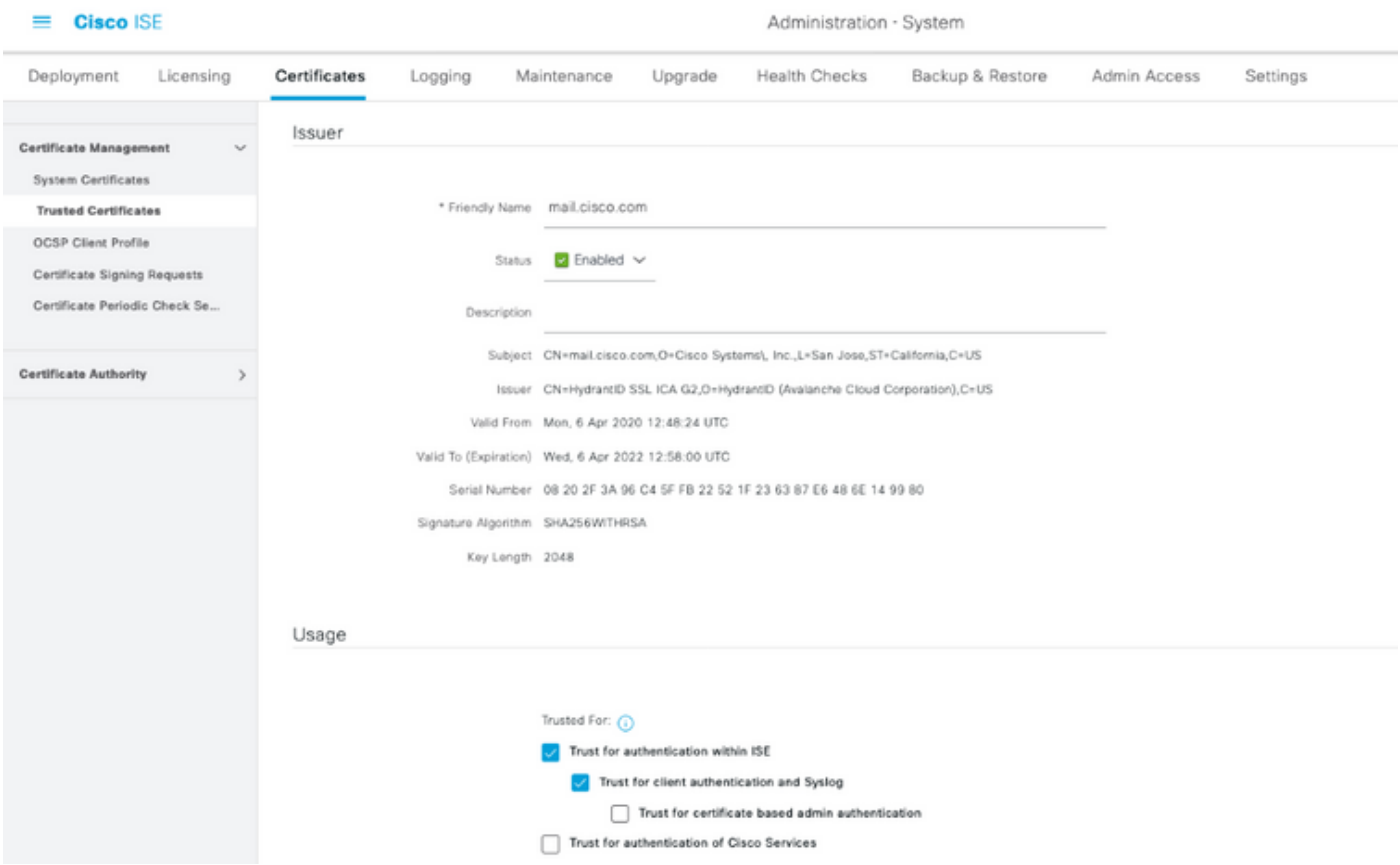
La connexion sécurisée peut être établie de deux manières :

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

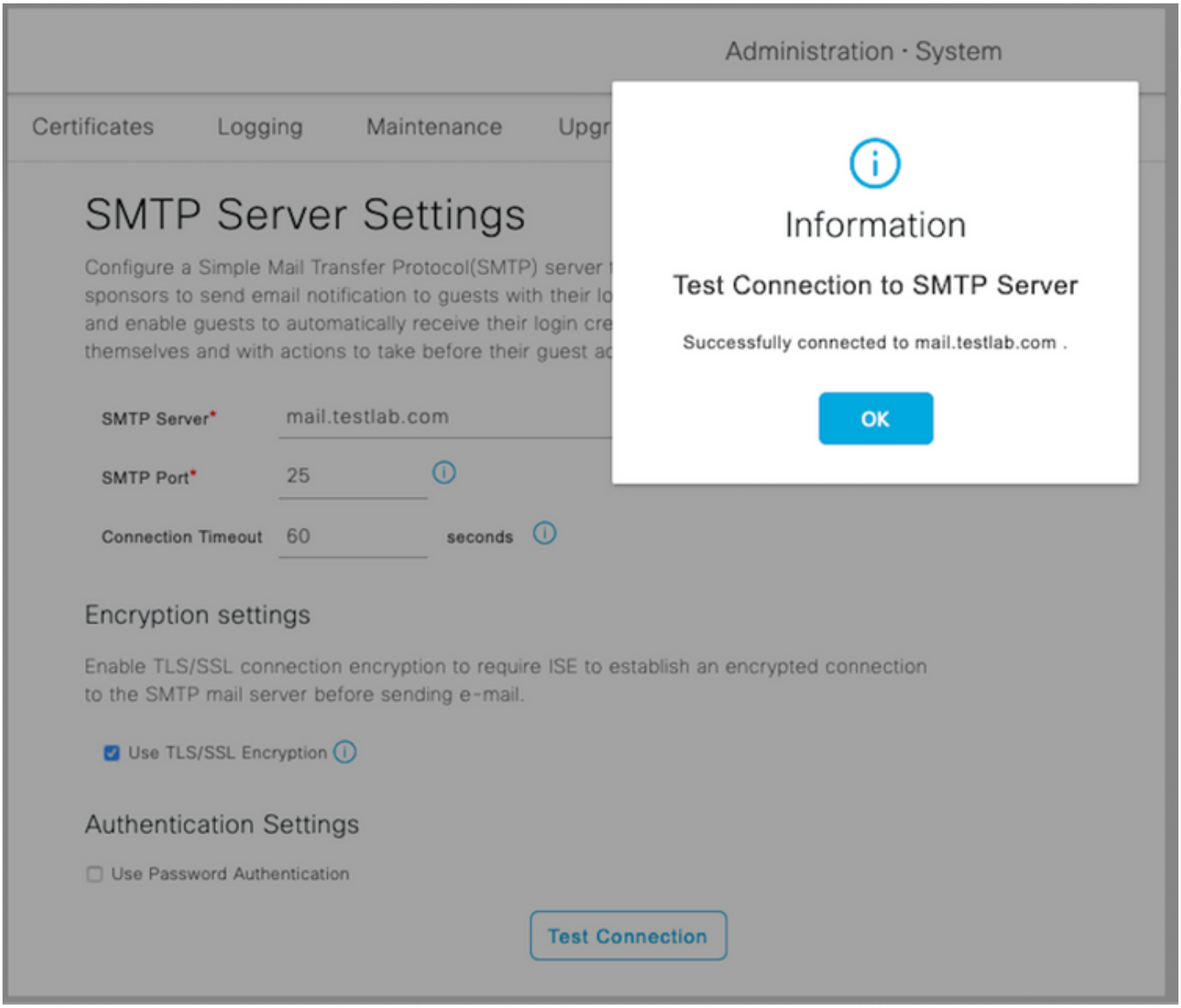
Le serveur SMTP utilisé doit prendre en charge l'authentification basée sur SSL et les informations d'identification. La communication SMTP sécurisée peut être utilisée avec l'une des options ou les deux options activées simultanément.

Communication SMTP sécurisée avec cryptage activé

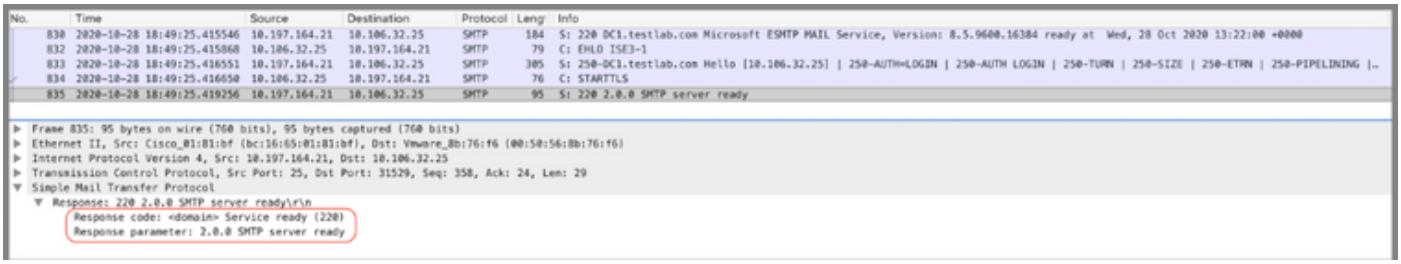
1. Importer le certificat d'autorité de certification racine du certificat du serveur SMTP dans les certificats de confiance ISE avec utilisation : **Confiance pour l'authentification dans ISE** et **Confiance pour l'authentification client et Syslog**.
2. Configurez le serveur SMTP, le port configuré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



Test Connection indique une connexion réussie au serveur SMTP.



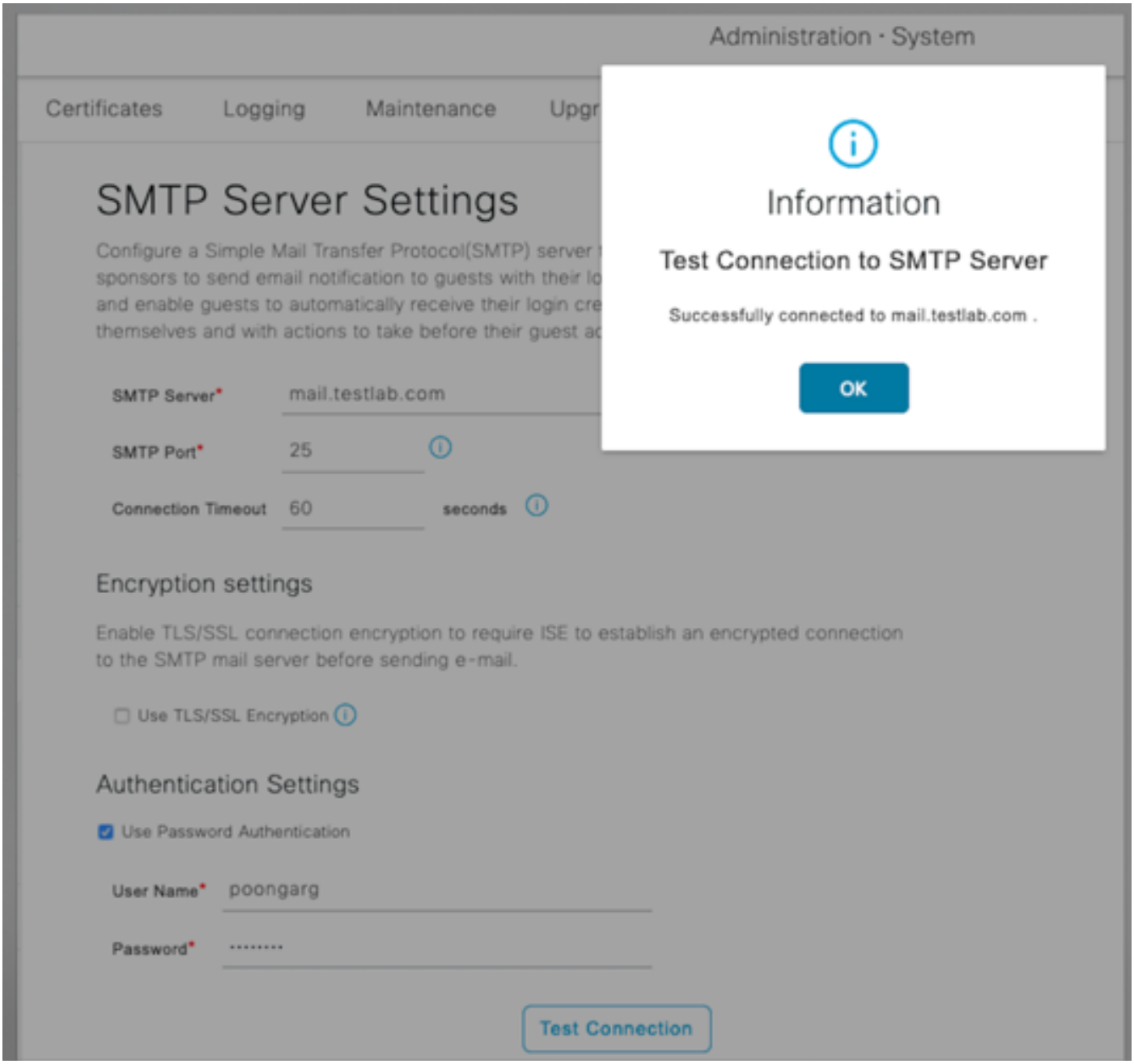
Les captures de paquets montrent que le serveur a accepté l'option **STARTTLS** comme demandé par l'ISE.



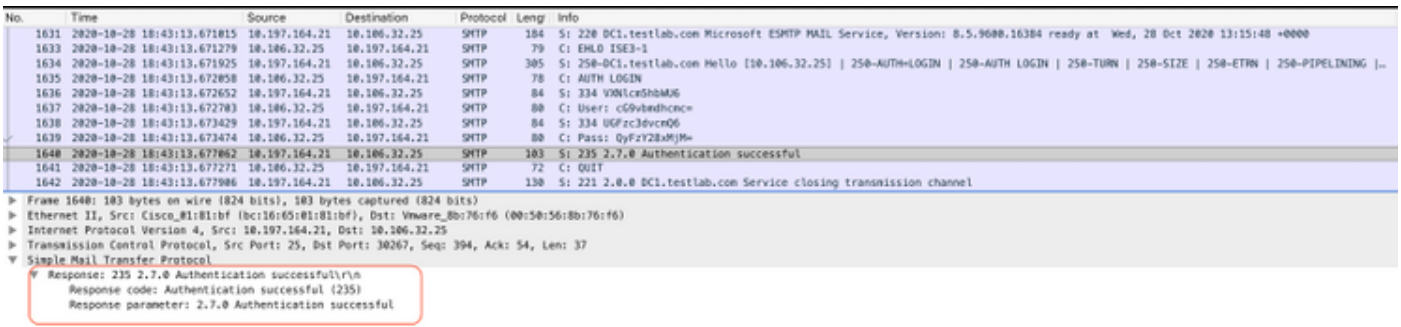
Communication SMTP sécurisée avec paramètres d'authentification activés

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 :



Vérification

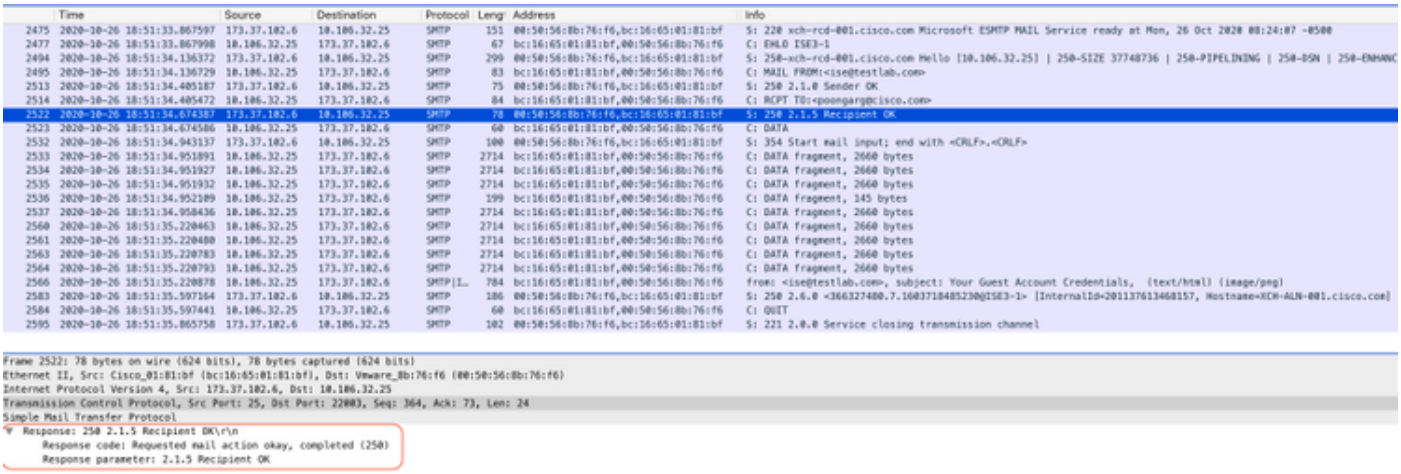
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

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

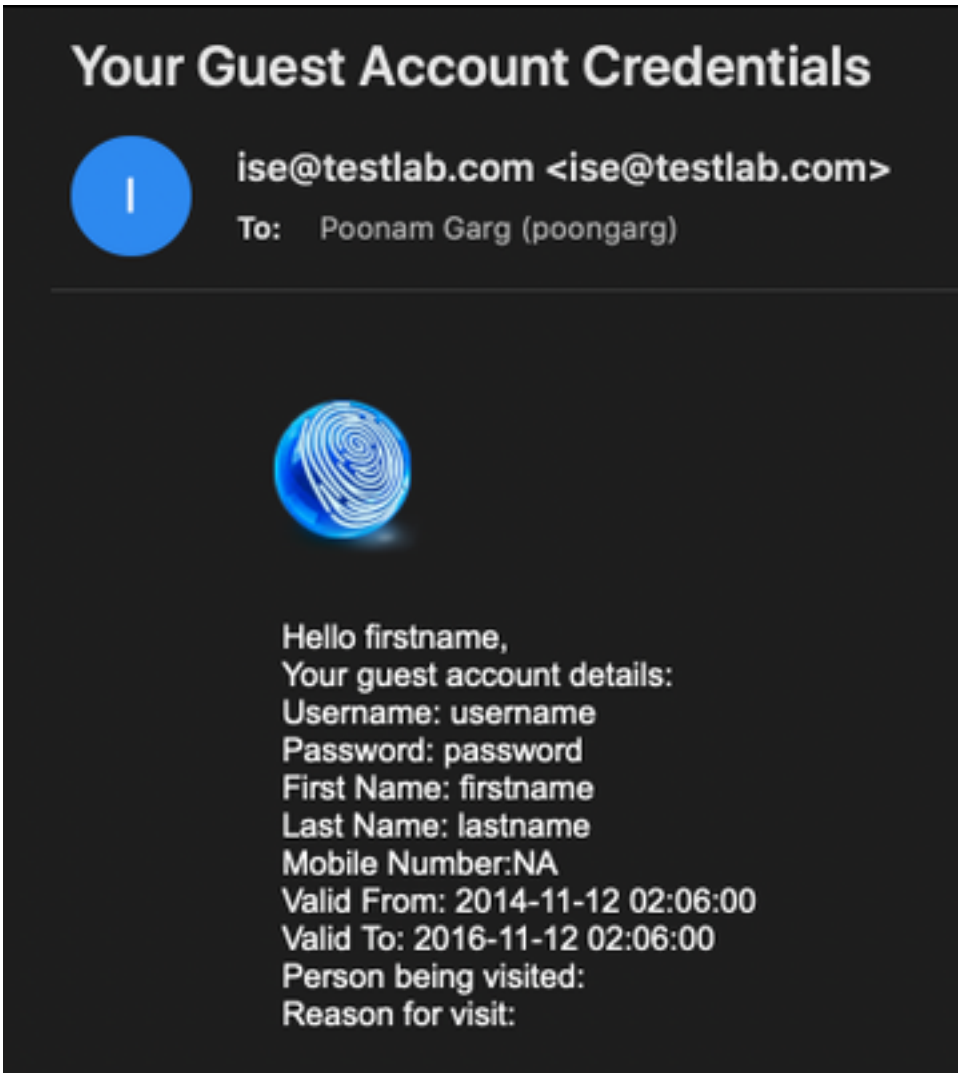
configuré.

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 :



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

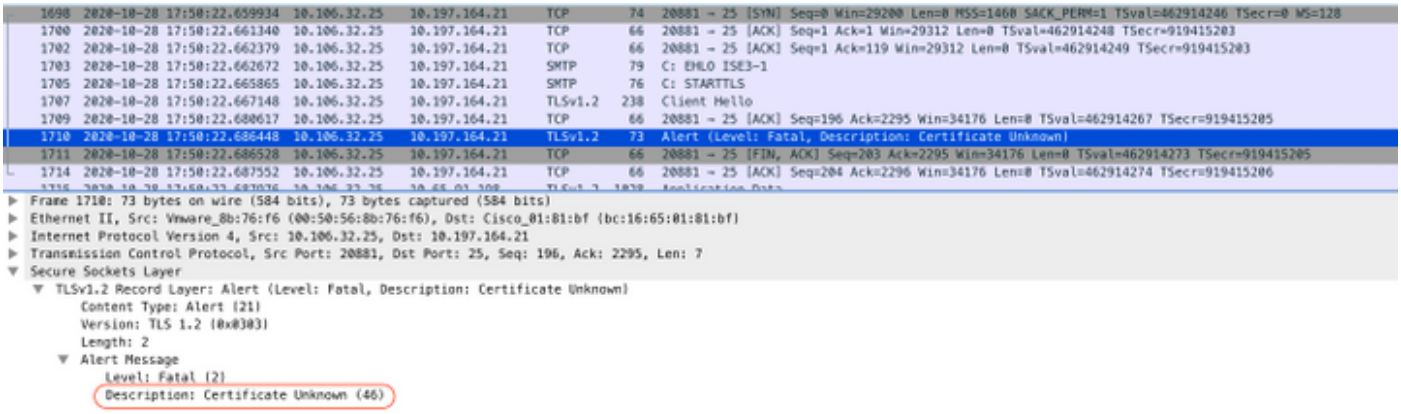


Dépannage

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 ».

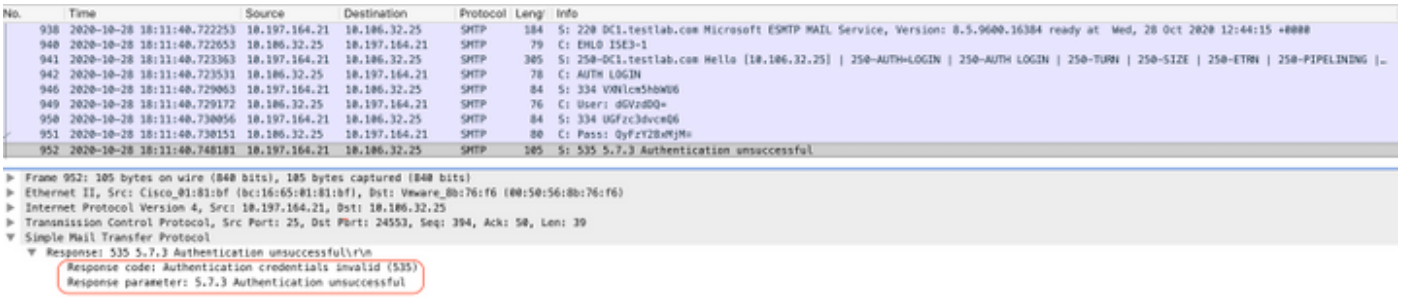
La capture de paquets montre que le certificat présenté par le serveur SMTP n'est pas fiable :



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.

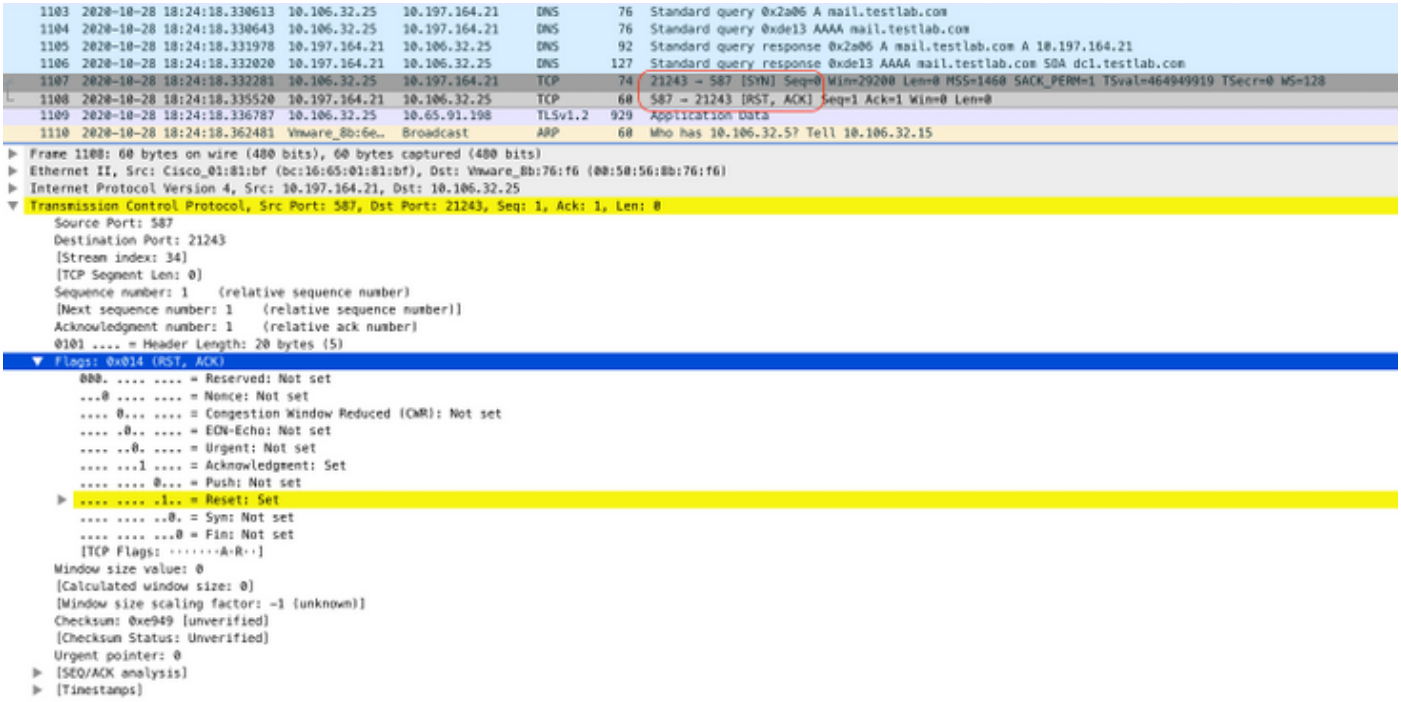


Solution : Validez le nom d'utilisateur ou le mot de passe configuré sur le serveur SMTP.

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.



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]