Configure Secure SMTP server on ISE

Contents

Introduction

This document describes how to configure the Simple Mail Transfer Protocol (SMTP) Server on the Cisco Identity Services Engine (ISE) in order to support Email notifications for multiple services. ISE version 3.0 supports both secured and unsecured connections to SMTP Server.

Contributed by Poonam Garg, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have a basic knowledge of the Cisco ISE and SMTP Server functionality.

Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is live, ensure that you understand the potential impact of any command.

Configuration

This section describes the configuration of the ISE in order to support email notifications used to:

- Send email alarm notifications to any internal admin users with the Inclusion of system alarms in emails option enabled. The sender’s email address to send alarm notifications is hardcoded as ise@<hostname>.
- Enable sponsors to send an email notification to guests with their log In credentials and password reset instructions.
- Enable guests to automatically receive their log In credentials after they successfully register themselves and with actions to take before their guest accounts expire.
- Send reminder emails to ISE admin users/Internal network users configured on the ISE prior to their password expiration date.

SMTP Settings

Before ISE can use any email services, it must have an SMTP relay server configured. In order to update the SMTP server details, navigate to **Administration > System > Settings > Proxy > SMTP server.**

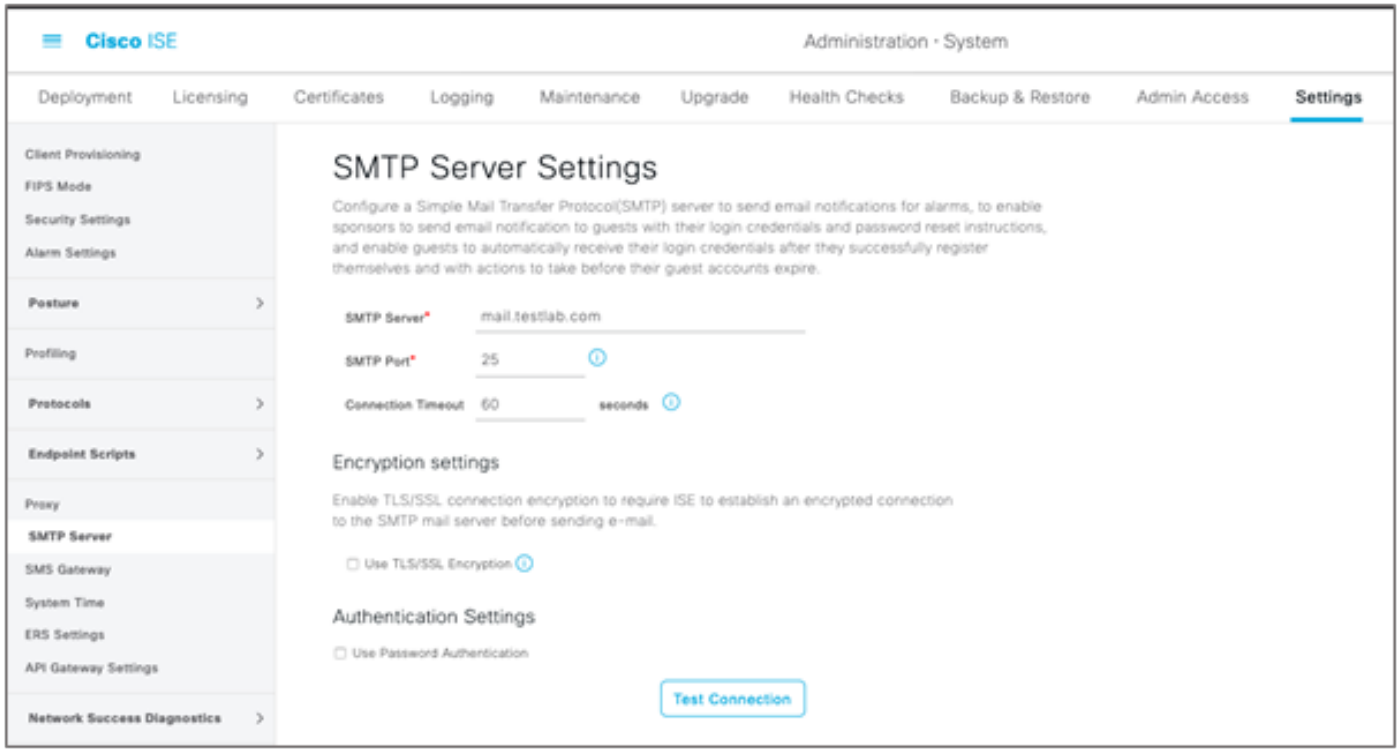
This table shows which node in a distributed ISE environment sends an email.

Email Purpose	Node that sends the Email
Guest account expiration	Primary PAN
Alarms	Active MnT
Sponsor and Guest account notifications from respective portals	PSN
Password expirations	Primary PAN

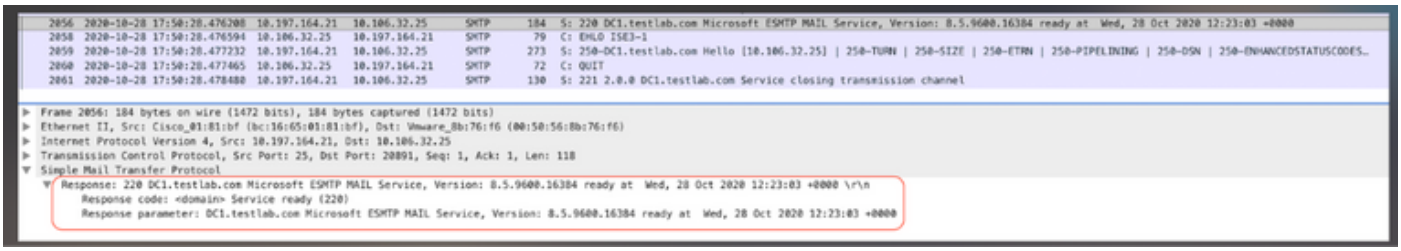
Configure the SMTP server in order to have the ability to accept any Emails from the ISE with or without authentication or encryption based on your requirement.

Unsecure SMTP Communication Settings without Authentication or Encryption

1. Define the SMTP Server hostname (outbound SMTP server).
2. SMTP Port (this port must be open in the network to connect to the SMTP server).
3. Connection Timeout (Enter the maximum time Cisco ISE waits for a response from the SMTP server).
4. Click **Test Connection** and Save.



Packet capture shows the ISE communication with the SMTP Server without Authentication or Encryption:



Secure SMTP Communication Settings

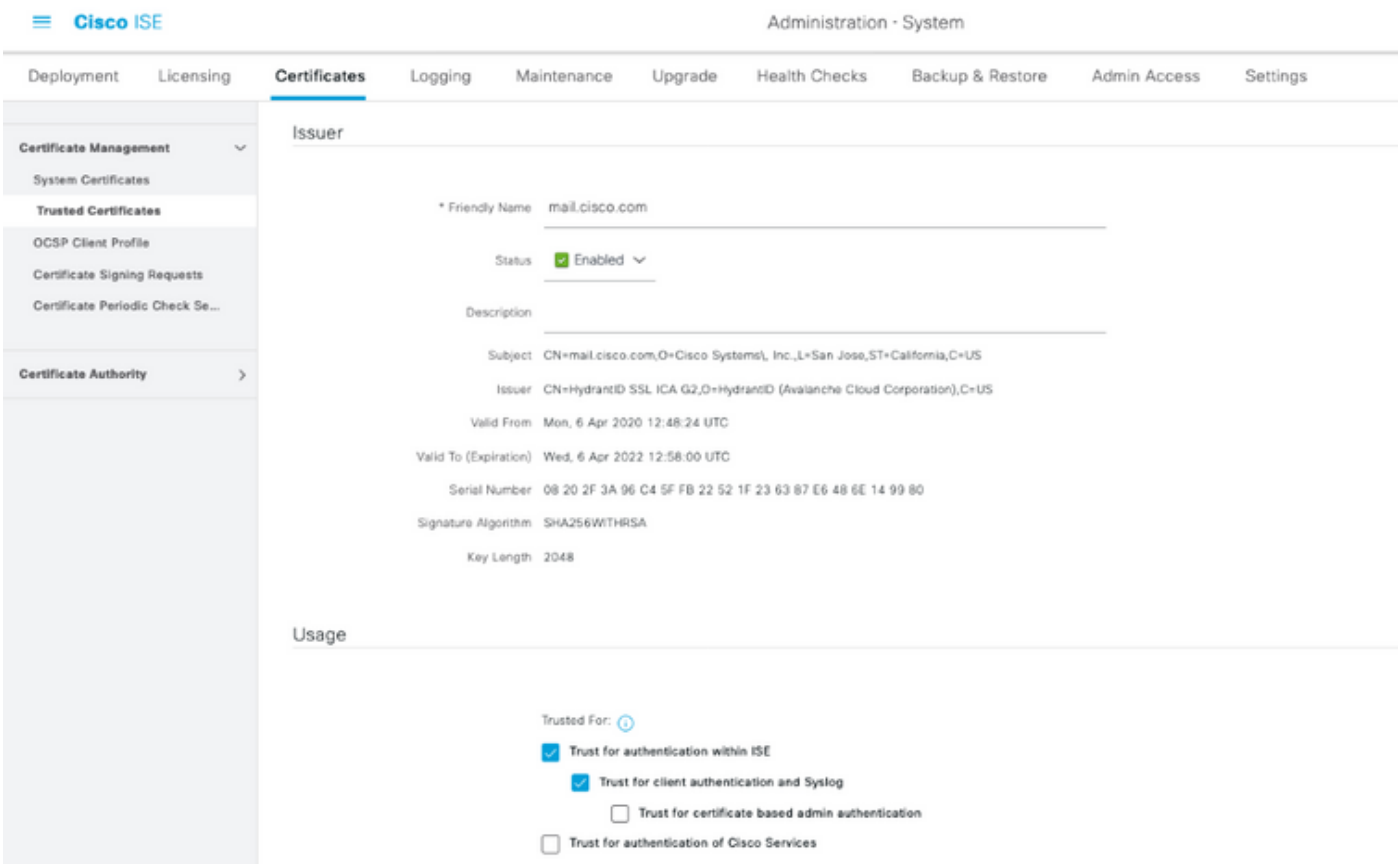
The secured connection can be made in two ways:

1. SSL Based
2. Username/Password-based

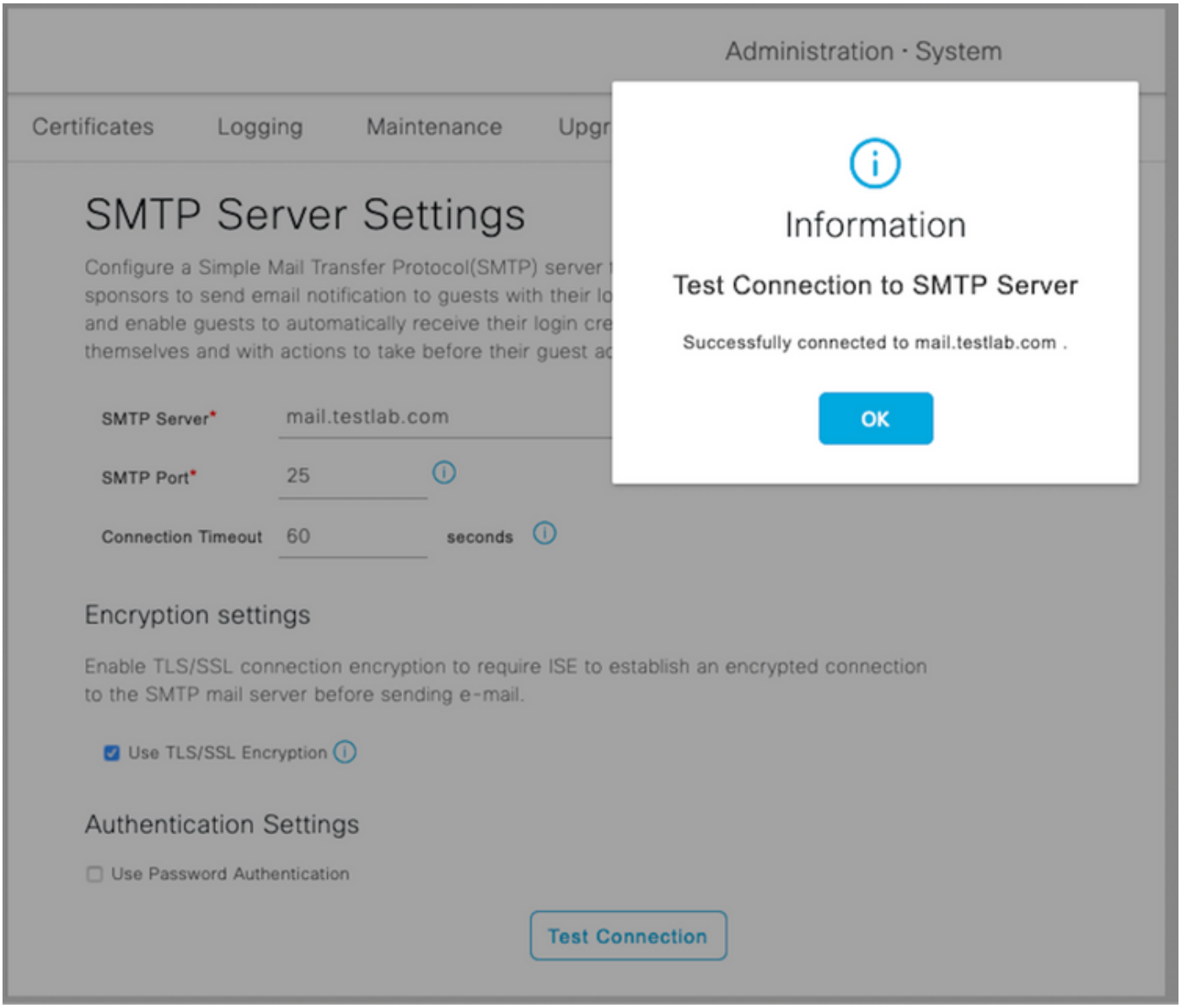
The SMTP Server used must support SSL and Credentials based authentication. Secured SMTP communication can be used with either of the options or both the options enabled simultaneously.

Secure SMTP Communication with Encryption Enabled

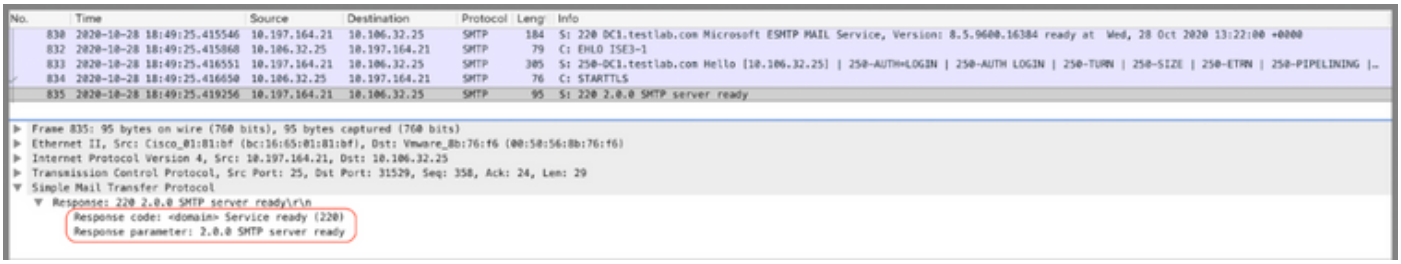
1. Import Root CA Certificate of the SMTP server certificate in the ISE Trusted Certificates with usage: **Trust for authentication within ISE** and **Trust for client authentication and Syslog**.
2. Configure the SMTP server, Port configured on the SMTP server for encrypted communication, and check the option **Use TLS/SSL encryption**.



Test Connection shows a successful connection to the SMTP Server.



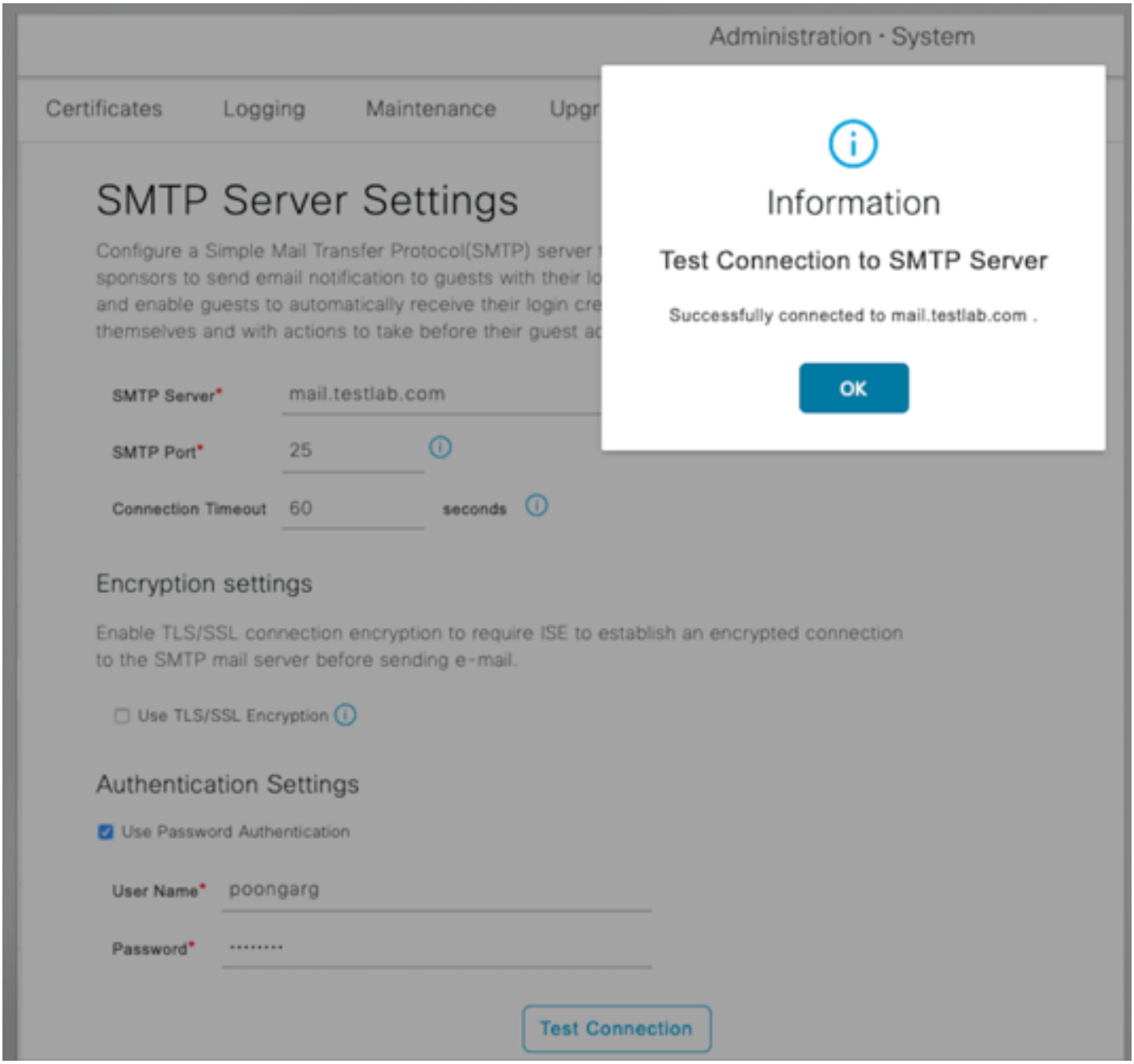
Packet captures show that the Server has accepted the **STARTTLS** option as requested by the ISE.



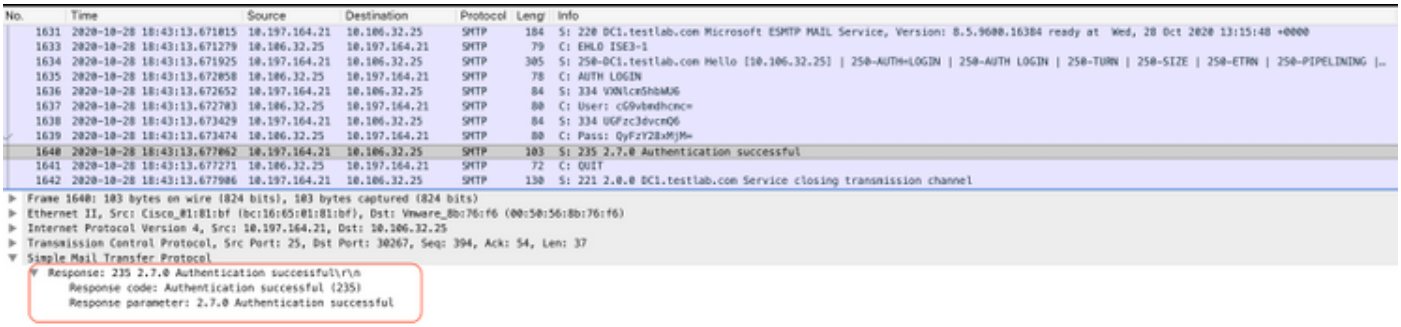
Secure SMTP Communication with Authentication Settings Enabled

1. Configure the SMTP Server and SMTP Port.
2. Under Authentication Settings, check the **Use Password Authentication** option and provide the username and password.

Successful **Test Connection** when password-based authentication works :



Sample packet capture that shows successful authentication with credentials:



Verify

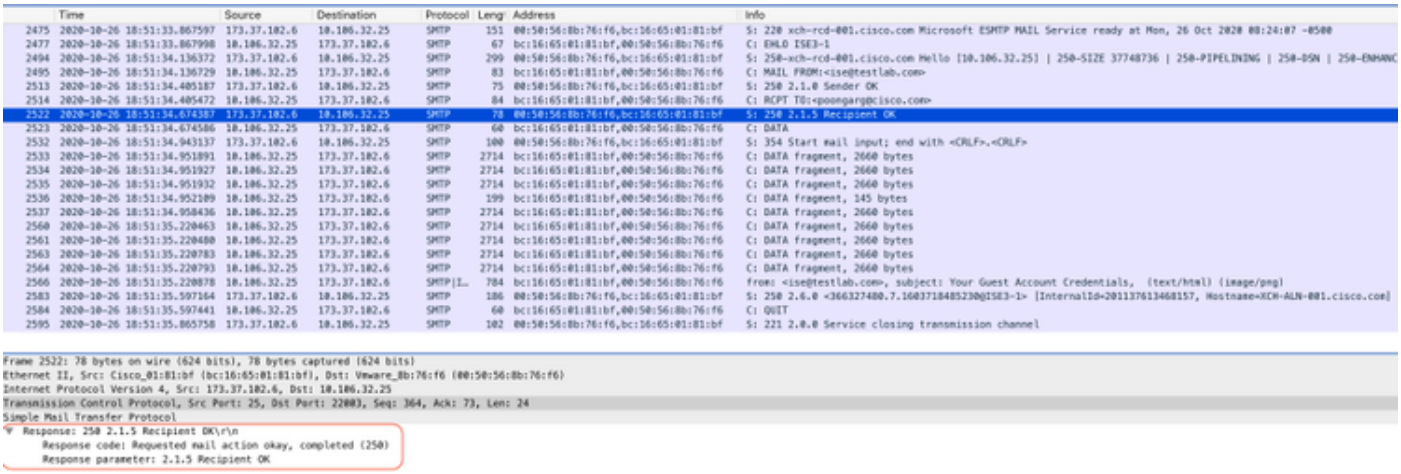
Use this section to confirm that your configuration works properly.

1. Use the Test Connection option in order to verify the connectivity to the configured SMTP

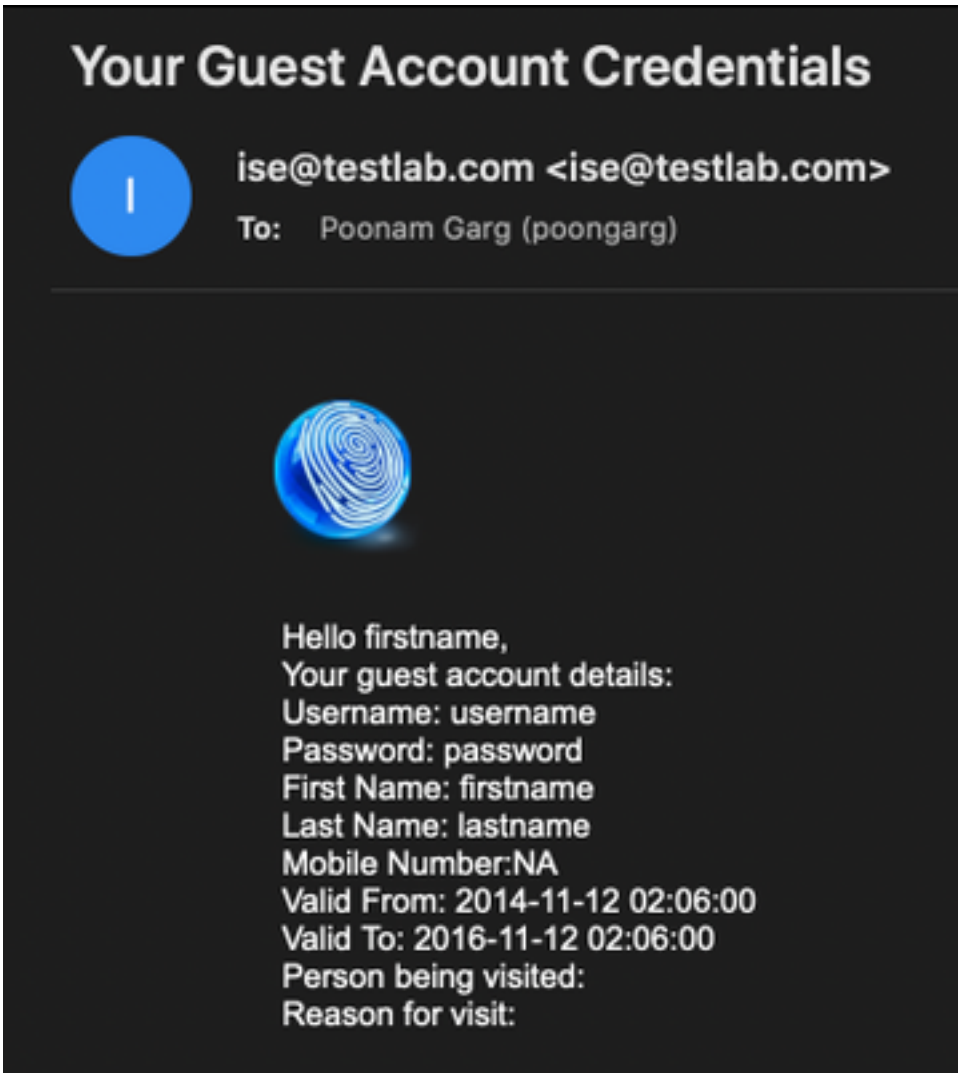
server.

2. Send a test email from Guest portal at **Work Centers > Guest Access > Portals & Components > Guest Portals > Self-Registered Guest Portal(default) > Portal Page Customization > Notifications > Email > Preview window Settings**, enter a valid email address and Send Test Email. The recipient must receive the Email from the configured email address under Guest Email Settings.

Sample email notification sent for Guest Account Credentials:



Sample email notification received by Email recipient:

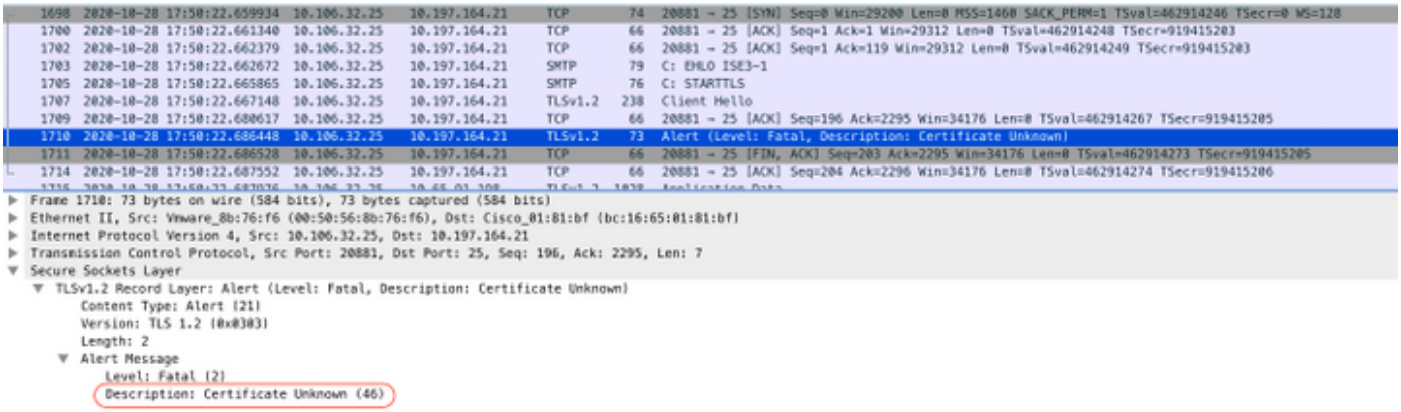


Troubleshoot

This section provides the information you can use in order to troubleshoot your configuration:

Problem: Test connection shows: "Could not connect to SMTP Server, SSL Error. Please check the trusted certificates".

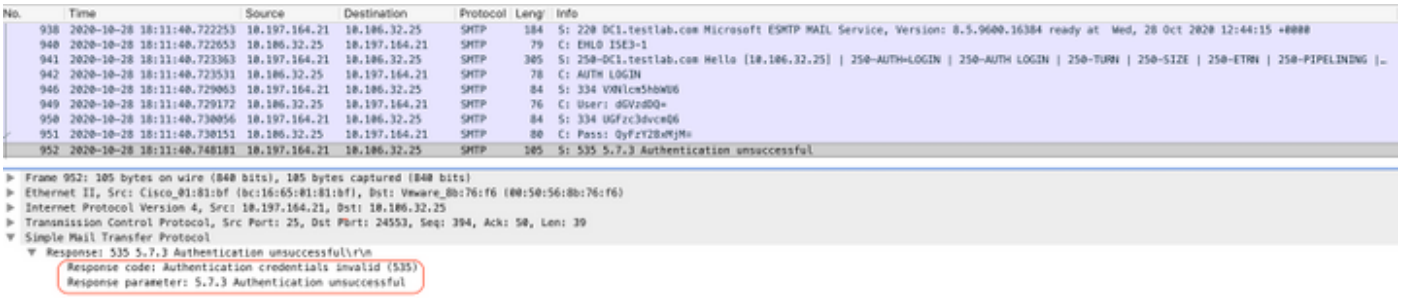
Packet capture shows that the certificate presented by the SMTP server is not trusted:



Solution: Import Root CA Certificate of the SMTP server in the ISE Trusted Certificates and if TLS support is configured on the port.

Problem: Test Connection shows: Authentication failure: Could not connect to SMTP Server, User Name or Password is incorrect.

Sample packet capture here shows that the authentication was not successful.

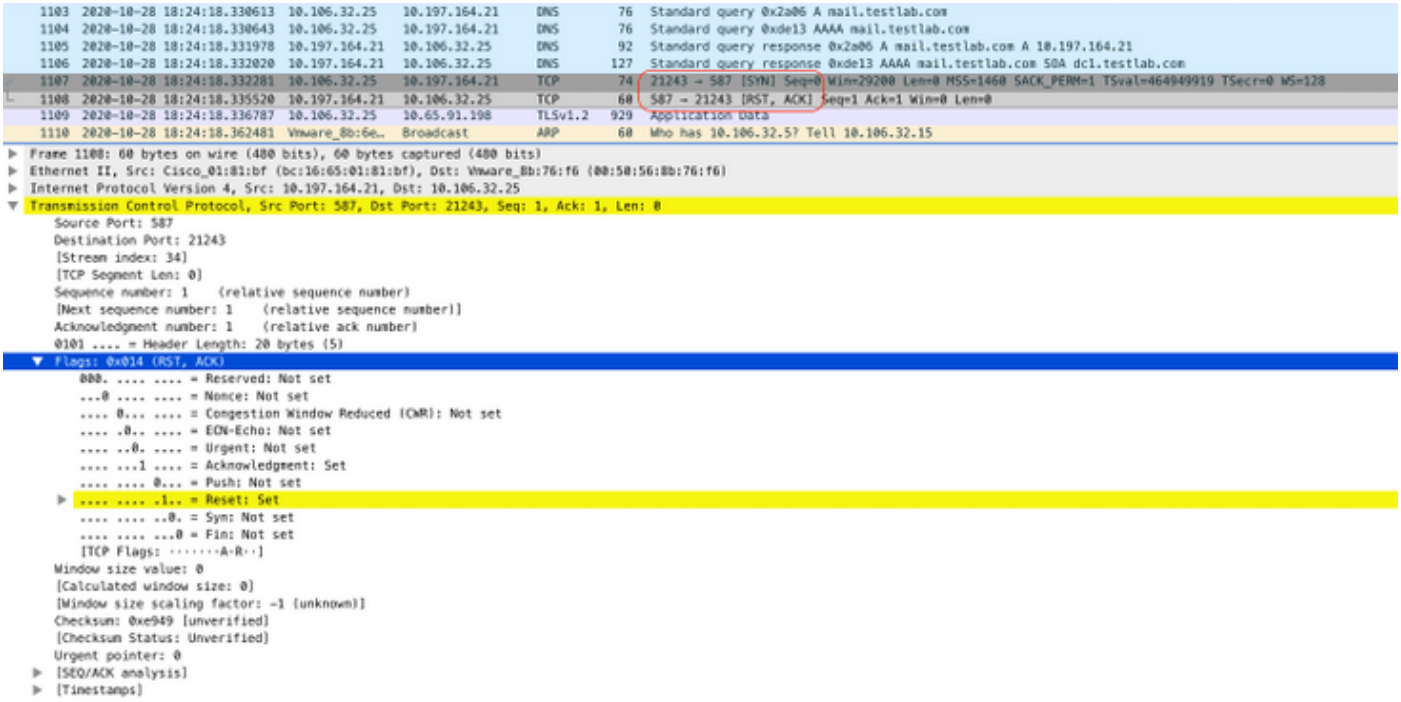


Solution: Validate Username or Password configured on the SMTP server.

Problem: Test Connection shows: Connection to SMTP server failed.

Solution: Verify the SMTP Server Port configuration, Check if the SMTP server name is resolvable by the configured DNS server on ISE.

The example here shows a reset is sent by the SMTP server on 587 port which is not configured for SMTP service.



Related Information

- 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
- [Technical Support & Documentation - Cisco Systems]