Verify and Troubleshoot TLS Certificates on Cisco ESA

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Functional Overview and Requirements

Configure and Assign a Certificate

Verify

- Verify TLS for HTTPS
- Verify TLS for Email Delivery or Receiving
  - TLS Success Example When Receiving Mail
  - TLS Failure Example When Receiving Mail
  - TLS Success Example When Delivering Mail
  - TLS Failure Example When Delivering Mail
- Verify TLS for LDAP

Troubleshoot

- Check Intermediate Certificates
- Enable Notifications for Required TLS Connection Failures
- Troubleshooting Using Third-Party Tools
- Resolution

Related Information

Introduction

This document describes how to create, configure, and troubleshoot TLS certificates on the Cisco Email Security Appliance (ESA).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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.

Background Information

The TLS implementation on the ESA provides privacy for point-to-point transmission of emails through encryption. This implementation allows an administrator to import a certificate and private key from a Certificate Authority (CA) service, or use a self-signed certificate.

Cisco AsyncOS for Email Security supports the STARTTLS extension to Simple Mail Transfer Protocol (SMTP) (Secure SMTP over TLS).



Note: This document describes how to install certificates at the cluster level with the use of the Centralized Management feature on the ESA. Certificates can be applied at the machine level; however, if the machine is removed from the cluster and then added back, the machine-level certificates are lost.

Functional Overview and Requirements

An administrator can utilize a certificate on the appliance for any of these reasons:

- To encrypt the SMTP conversations with other MTAs that use TLS (both inbound and outbound conversations).
- To enable the HTTPS service on the appliance for access to the GUI via HTTPS.
- For use as a client certificate for Lightweight Directory Access Protocols (LDAPs), if the LDAP server requires a client certificate.
- To allow secure communication between the appliance and a Cisco Advanced Malware Protection (AMP) Threat Grid Appliance.

The ESA comes preconfigured with a demonstration certificate that can be used to establish TLS connections.



Caution: While the demonstration certificate is sufficient for the establishment of a secure TLS connection, be aware that it cannot offer a verifiable connection. Cisco recommends that you obtain an X.509, or Privacy Enhanced Email (PEM) certificate from a CA.

Configure and Assign a Certificate

Before proceeding, ensure you have completed the steps for creating and assigning a certificate as outlined in the User Guide. These links provide the necessary instructions:

- Deploying a Signed Certificate
- Assigning a Certificate

Verify

Verify TLS for HTTPS

1. **Access the GUI:**Navigate to your ESA device using the HTTPS URL (for example, **https://esa.example.com**).

2. **Open Certificate Details:**Click the **Site Information** icon (usually a padlock) located to the left of the URL in the browser address bar.

3. **Validate based on your Browser:**

a. **Google Chrome:** Click the**Padlock icon**>**Connection is secure**>**Certificate is valid**.

b. **Microsoft Edge:** Click the**Padlock icon**>**Connection is secure**>**Certificate icon**(top right of the flyout).

c. **Mozilla Firefox:** Click the**Padlock icon**>**Connection secure**>**More information**>**View Certificate**.

4. Confirm Validity: Review the "Validity Period" or "Status" in the certificate viewer. If the certificate shows as**Valid**, the connection is secure and the certificate is correctly recognized by the browser.

Verify TLS for Email Delivery or Receiving

While **Message Tracking** in the GUI provides this information, using the Command Line Interface (CLI) is often more efficient for bulk review or rapid troubleshooting.

Review these steps to review TLS status via the CLI:

1. **Log in to the CLI:**Access the appliance via SSH using your administrative credentials.
2. **Run the Grep Command:**Use the **grep**utility to filter the mail logs for TLS-related activity.
3. **Analyze Connection IDs:**Review the output based on the connection type:
    - **ICID (Incoming Connection ID):**Review these entries to verify TLS for connections being**received** on the listener.
    - **DCID (Delivery Connection ID):**Review these entries to verify TLS for connections

being **delivered**to the next hop MTA.



Note: You can search for specific strings like "TLS success" or "TLS failed" to narrow down results.

TLS Success Example When Receiving Mail

<#root>

```
(Machine esa.example.com)>
```

grep "ICID.*TLS success" mail_logs

```
Sat Feb 14 19:14:38 2026 Info: ICID 111395123 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-
Sat Feb 14 19:14:41 2026 Info: ICID 111395456 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA38
```

TLS Failure Example When Receiving Mail

<#root>

```
(Machine esa.example.com)>
```

grep "ICID.*TLS failed" mail_logs

```
Sat Feb 14 19:20:28 2026 Info: ICID 111396123 TLS failed: [Errno 0] Error
Sat Feb 14 19:20:28 2026 Info: ICID 111396456 TLS failed: ('SSL routines:tls_early_post_process_client_
```

TLS Success Example When Delivering Mail

<#root>

```
(Machine esa.example.com)>
```

grep "DCID.*TLS success" mail_logs

```
Sat Feb 14 19:12:56 2026 Info: DCID 21966123 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-S
Sat Feb 14 19:13:00 2026 Info: DCID 21966456 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

TLS Failure Example When Delivering Mail

```
<#root>

(Machine esa.example.com)>

grep "DCID.*TLS failed" mail_logs



Sat Feb 14 19:58:43 2026 Info: DCID 21967123 TLS failed: TLS required, STARTTLS unavailable, destinatio
Sat Feb 14 20:58:44 2026 Info: DCID 21967456 TLS failed: TLS required, STARTTLS unavailable, destinatio
```

Verify TLS for LDAP

Although the ldap_debug logs do not show a specific TLS string, you can determine whether TLS is successful or has failed by examining the LDAP response and the port(s) in use. For LDAPS connections, this typically means port 3269 for Active Directory or port 636 for OpenLDAP.

TLS Example for LDAP

```
<#root>

(Machine esa.example.com) (SERVICE)>

tail ldap_debug



Wed Feb 25 03:24:23 2026 Debug: LDAP: (group) Query (proxyAddresses=smtp:user@example.com) to server LD

:3269

)
Wed Feb 25 03:24:23 2026 Debug: LDAP: (group) Query (proxyAddresses=smtp:user@example.com) lookup succe

:3269

) returned 0 results timestamp=1771989863.189580
```

Note: For a more detailed analysis of LDAP traffic and TLS activity, Cisco recommends capturing network packets on the relevant hosts and ports.

Troubleshoot

This section describes how to troubleshoot basic TLS issues on the ESA.

Check Intermediate Certificates

Look for duplicate intermediate certificates when current certificates are updated instead of a new certificate creation. The intermediate certificates can change or be improperly chained, and the certificate can upload multiple intermediate certificates. This can introduce certificate chaining and verification issues.

Enable Notifications for Required TLS Connection Failures

You can configure the ESA to send an alert if the TLS negotiation fails when messages are delivered to a domain that requires a TLS connection. The alert message contains the name of the destination domain for the failed TLS negotiation. The ESA sends the alert message to all recipients set to receive warning severity level alerts for system alert types.

 **Note**: This is a global setting, so it cannot be set on a per-domain basis.

Complete these steps to enable TLS connection alerts:

1. Navigate to **Mail Policies** > **Destination Controls**.
2. Click **Edit Global Settings**.
3. Check the **Send an alert when a required TLS connection fails** check box.

 **Tip**: You can also configure this setting with the **destconfig** > **setup** CLI command.

The ESA also logs the instances for which TLS is required for a domain, but could not be used in the appliance **mail_logs**. This occurs when any of these conditions are met:

- The remote MTA does not support ESMTP (for example, it did not understand the EHLO command from the ESA).
- The remote MTA supports ESMTP, but the STARTTLS command was not in the list of extensions advertised in the EHLO response.
- The remote MTA advertised the STARTTLS extension, but responded with an error when the ESA sent the STARTTLS command.

Troubleshooting Using Third-Party Tools

- Ensure the certificate is applied at the **Listener** where the appliance receives inbound mail before you begin the test.

Third-party tools such as CheckTLS.com and SSL-Tools.net can be used to verify the proper chaining of the certificate when **Receiving**. Review the documentation for each tool to understand how to validate the certificate.

Note: If a self-signed certificate is in use, a failure is expected.

Resolution

If a CA signed certificate is in use and TLS-verify fails, verify that these items match:

- Certificate common name
- Hostname (at **GUI** > **Network** > **Interface**)
- MX record hostname: this is the MX Server column in the TestReceiver table

Related Information

- Cisco Email Security Appliance - End-User Guides