# Verwenden von TLSVERIFY zur Fehlerbehebung bei TLS-Bereitstellungsproblemen

## Inhalt



## Einführung

In diesem Dokument wird beschrieben, wie Sie TLSVERIFY zur Fehlerbehebung bei TLS-Zustellungsproblemen verwenden.

Hinsichtlich der E-Mail-Verarbeitung auf der Cisco E-Mail Security Appliance (ESA) sehen Sie möglicherweise, dass TLS keinen Fehler oder keine Warnmeldung ausgibt oder zurückgibt.

Verwenden Sie in der CLI der Appliance **"tlsverify"**, um die TLS-Kommunikation von der Appliance zur externen Domäne zu testen.

```
mail3.example.com> tlsverify

Enter the TLS domain to verify against:
[]> example.com

Enter the destination host to connect to. Append the port
(example.com:26) if you are not connecting on port 25:
[example.com]> mxe.example.com:25

Connecting to 1.1.1.1 on port 25.
Connected to 1.1.1.1 from interface 10.10.10.10.
Checking TLS connection.
TLS connection established: protocol TLSv1, cipher RC4-SHA.
Verifying peer certificate.
Verifying certificate common name mxe.example.com.
TLS certificate match mxe.example.com
TLS certificate verified.
TLS connection to 1.1.1.1 succeeded.

TLS successfully connected to mxe.example.com.
TLS verification completed.
```

Die obige Ausgabe des Befehls **tlsverify (TLS) zeigt die TLS-Verifizierung von dieser Appliance bis zum Ziel mit der IP-Adresse 1.1.1.1.**

## Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems