

# TLSVERIFY gebruiken om problemen met TLS-levering op te lossen

## Inhoud

[Inleiding](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft hoe u TLSVERIFY kunt gebruiken om problemen met de levering van TLS op te lossen.

Met betrekking tot e-mailverwerking op de Cisco Email Security Appliance (ESA) kunt u zien dat TLS geen fout of waarschuwing geeft of teruggeeft.

Gebruik **TMS** om de communicatie tussen het apparaat en het externe domein te testen van de CLI op het apparaat.

```
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.
```

De bovenstaande uitvoer van de opdracht **Tlsverify**-verificatie van dit apparaat naar de bestemming met IP-adres 1.1.1.1.

## Gerelateerde informatie

- [Cisco e-mail security applicatie - eindgebruikershandleidingen](#)

- [Technische ondersteuning en documentatie – Cisco Systems](#)