

# Waarom mislukt de TLS-onderhandeling van de ESA naar een server van de bestemming ondanks dat STARTTLS beschikbaar is?

## Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Waarom mislukt de TLS-onderhandeling van de ESA naar een server van de bestemming ondanks dat STARTTLS beschikbaar is?](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft hoe TLS-onderhandelingshoofd (Transfer Layer Security) moet worden geïdentificeerd wanneer **STARTTLS** beschikbaar is binnen de opdrachten EHLO Simple Mail Transfer Protocol (SMTP) en de server niet voldoet aan RFC1869.

## Achtergrondinformatie

TLS is ingeschakeld op e-mail security applicatie (ESA) met een geldig certificaat. TLS is ingeschakeld op de doelserver en STARTTLS wordt gezien wanneer er een verbinding met het midden- en kleinbedrijf wordt ingesteld.

## Waarom mislukt de TLS-onderhandeling van de ESA naar een server van de bestemming ondanks dat STARTTLS beschikbaar is?

ESA probeert met behulp van TLS verbinding te maken met de server van de bestemming, maar TLS-onderhandeling faalt met deze fout in de `mail_logs/Message Tracking` van de ESA.

```
Info: DCID xxxxxx STARTTLS command not supported.
```

Volgens RFC1869 moet de eerste reactie op EHLO `ehlo-ok-rsp` zijn en `ehlo-ok-rsp` deze syntax en order hebben:

```
ehlo-ok-rsp ::= "250" domain [ SP greeting ] CR LF
/ ( "250-" domain [ SP greeting ] CR LF
*( "250-" ehlo-line CR LF )
"250" SP ehlo-line CR LF )
```

**Onjuist RFC-voorbeeld van synchrone TCP-conversie**

```
220 mail.domain1.com ESMTTP Service ready
EHLO ESA.com
250-STARTTLS <--- 250-STARTTLS is before the server greeting.
250-mail.domain1.com <--- This is the 250 destination server greeting.
250-8BITMIME
250-PIPELINING
250-HELP
250-DELIVERBY 300
250 SIZE 30000000
```

Het betekent dat alles wat er is voordat de **ehlo-line** (250-mail.domain1.com, in dit voorbeeld) als een groet wordt beschouwd. ESA zal dus de **250-STARTTLS** opdracht niet beschikbaar achten en **STARTTLS opdracht niet ondersteund** rapporteren. Raadpleeg <https://tools.ietf.org/html/rfc1869> voor meer informatie.

## Correcte RFC-gespreksvoorbeeld voor Synthetisch MTP

```
220 mail-esa.com ESMTTP
EHLO connecting.server.com
250-mail-esa.com <--- This is the 250 destination server greeting.
250-8BITMIME
250-SIZE 33554432
250 STARTTLS <--- STARTTLS is available after the greeting, it's not considered a greeting as
per RFC.
```

## Gerelateerde informatie

- [RFC 1869-documentatie](#)
- [ESR-uitgebreide TLS-handleiding](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)