

TLS ネゴシエーションは「サポートされない」 STARTTLS コマンドで STARTTLS が利用可能な、次の RFC 時失敗します

目次

[概要](#)

[背景説明](#)

[TLS ネゴシエーションはなぜ ESA からの宛先 サーバへの利用可能な STARTTLS にもかかわらず失敗しますか。](#)

[関連情報](#)

概要

この記事は STARTTLS が rfc1869 に従って EHLO SMTP コマンドおよびサーバの内で利用できないとき TLS ネゴシエーション障害を識別する方法を記述します。

背景説明

TLS は有効な証明書が付いている E メール セキュリティ アプライアンス (ESA) で有効になります。

TLS は宛先 サーバで有効になり、SMTP 接続が確立されるとき STARTTLS は見られます。

TLS ネゴシエーションが利用可能な STARTTLS にもかかわらず ESA からの宛先 サーバへの失敗する理由

ESA は TLS ネゴシエーションが ESA の mail_logs/メッセージ トラッキングの次のエラーと失敗するどんなに TLS を使用している宛先 サーバに接続することを試みます。

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

RFC rfc1869 によって、EHLO への最初の応答は ehlo 良いrsp はずで、ehlo 良いrsp 次の構文および順序を持っています:

```
ehlo 良いrsp:: = "250" ドメイン[SP メッセージ] CR LF
```

```
/( "250-" ドメイン[SP メッセージ] CR LF
```

```
* ( "250-" ehlo 行 CR LF )
```

```
"250" SP ehlo 行 CR LF )
```

不正確な RFC 構文 SMTP メッセージ交換例

```
220 mail.domain1.com ESMTP 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
```

ehlo 行 (この例の `250-mail.domain1.com`) がメッセージとして、従って考慮される前にどのすべてを意味するか ESA は 250-STARTTLS コマンドを使用可能と見なさなかつたりし、サポートされなかった STARTTLS コマンドを報告します。 <https://tools.ietf.org/html/rfc1869> を詳細については参照して下さい。

RFC 構文 SMTP メッセージ交換例を訂正して下さい

```
220 mail-esa.com ESMTPEHLO 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.
```

関連情報

- [テクニカル サポートとドキュメント – Cisco Systems](#)
- [RFC 1869 シスコのドキュメント](#)
- [ESA 広範囲の TLS ガイド](#)