

TLS-configuratie Vaak gestelde vragen voor ESA

Inhoud

[Inleiding](#)

[Wat is TLS?](#)

[Wat is vereist om TLS op de ESA te laten aansluiten?](#)

[Hoe kunt u TLS voor ontvangst inschakelen?](#)

[Hoe kan TLS voor levering worden ingeschakeld?](#)

[Hoe kan ik bepalen of de ESA TLS gebruikt?](#)

[Gerelateerde informatie](#)

Inleiding

In dit document worden veelgestelde vragen beschreven over de configuratie van Transport Layer Security (TLS) op de E-mail security applicatie (ESA).

Wat is TLS?

Zoals gedefinieerd in RFC 3207, is "TLS een uitbreiding naar de MTP-service die een MTP-server en -client toestaat om de beveiliging van de transportlaag te gebruiken om privé, geauthentiseerde communicatie via het internet te verstrekken. TLS is een populair mechanisme voor het verbeteren van TCP-communicatie met privacy en authenticatie." De STARTTLS-implementatie op het ESA biedt privacy door middel van encryptie. Hiermee kunt u een X.509-certificaat en particuliere sleutel importeren van een certificeringsdienst of een zelfondertekend certificaat gebruiken.

Wat is vereist om TLS op de ESA te laten aansluiten?

De volgende stappen zijn nodig om TLS in te schakelen:

Opmerking: De ESA bevat een demonstratiecertificaat voor testdoeleinden. Het demo-certificaat is niet veilig en wordt niet aanbevolen voor algemeen gebruik.

Raadpleeg voor meer informatie de [installatievereisten van het ESR-certificaat](#).

Hoe kunt u TLS voor ontvangst inschakelen?

De volgende stappen zijn nodig om TLS te eisen van afstandshosts die communiceren met uw ESA-openbare luisteraar (Ontvangen). Schakel TLS in de Host Access Table (HAT) van de

luisteraar in die met externe hosts communiceert:

1. Ga naar GUI: Mail-beleid > Mail-Flow-beleid
2. Selecteer de luisteraar waaraan externe hosts verbinding zal maken met de uitrollijst in het menu op de pagina Mail Flow Policy.
3. Schakel TLS op een of meer Mail Flow-beleid in door op de beleidsnaam te klikken en het aanvinkvakje TMS gebruiken onder op de pagina Bewerken beleid te controleren.

Raadpleeg voor meer informatie [Hoe TLS voor inkomende verbindingencryptie op ESA luisteraar in te schakelen?](#)

Hoe kan TLS voor levering worden ingeschakeld?

De volgende stappen zijn nodig om TLS voor levering aan hosts in afgelegen domeinen mogelijk te maken.

1. Ga naar GUI: Mail-beleid > Bestemmingscontroles
2. Voeg een nieuwe bestemming toe voor het domein waarop u TLS gebruikt
3. Stel de conversielimiet, de limiet van de ontvanger en het aantoonprofiel in, of accepteer de standaardwaarden.
4. Pas een TLS-instelling voor het domein toe (No, Preferred, Of Required)

Raadpleeg voor meer informatie [Hoe controleer ik TLS-onderhandeling bij levering?](#)

Hoe kan ik bepalen of de ESA TLS gebruikt?

De ESR-maillogbestanden bevatten items voor succesvolle en mislukte TLS-verbindingen. U kunt gereedschappen voor opdrachtregel, zoals **grip**, gebruiken om naar specifieke logitems te zoeken. U kunt ook systeemmeldingen configureren wanneer TLS-verbindingen niet via de GUI kunnen worden uitgevoerd: Systeembeheer > Waarschuwingen pagina of de CLI alertfig opdracht.

Raadpleeg voor meer informatie [Bepaal of ESA TLS gebruikt voor levering of ontvangst](#)

Ga voor meer informatie naar Cisco AsyncOS voor e-mail gebruikershandleiding door communicatie met andere MTA's te versleutelen.

Gerelateerde informatie

- [Eindgebruikershandleidingen - AsyncOS voor e-mail](#)