# Configureer beveiligde e-mailgateway uitgaande MTA-STS

## Inhoud



## Inleiding

Dit document beschrijft stappen om de Secure Email Gateway (SEG) Uitgaande Mail Transfer Agent - Strict Transport Security (MTA-STS) te configureren.

## Voorwaarden

### Vereisten

Algemene kennis van de algemene instellingen en configuratie van Cisco Secure Email Gateway (SEG).

### Gebruikte componenten

Voor deze instelling is het volgende vereist:

- Cisco Secure Email Gateway (SEG) AsyncOS 16.0 of nieuwer.
- Bestemmingscontroleprofielen.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Overzicht

Mail Transfer Agent - Strict Transport Security (MTA-STS) is een protocol dat het gebruik van beveiligde TLS-verbindingen met een extra beveiligde beveiligingslaag afdwingt. MTA-STS helpt bij het voorkomen van man-in-the-middle aanvallen en afluisteren door ervoor te zorgen dat e-mails worden verzonden via beveiligde, versleutelde kanalen.

SEG AsyncOS 16 en nieuwer kunnen uitgaande MTA-STS berichtlevering aan MTA-STS geconfigureerd ontvangstdomeinen uitvoeren.

Indien ingeschakeld, controleert de SEG de doelcontroleprofielen op MTA-STS-instellingen. De SEG initieert het MTA-STS-proces om het gedefinieerde record en beleid op te halen, te valideren en toe te passen, waarbij ervoor wordt gezorgd dat de verbinding met de ontvangende MTA veilig is via TLSv1.2 of hoger.

De ontvangende domeineigenaren zijn verantwoordelijk voor het creëren, publiceren en onderhouden van het DNS Record en het MTA-STS beleid.

## Hoe MTA-STS werkt voor SEG

- Het ontvangende domein onderhoudt het MTA-STS-beleid en MTA-STS DNS-tekstrecord.
- De MTA-STS van het verzendende domein moet MTA-STS zijn die het MTA-STS-beleid van het bestemmingsdomein kan oplossen en er gevolg aan kan geven.

De eigenaar van het ontvangende e-maildomein publiceert een MTA-STS-txt-record via DNS zoals hier beschreven:

- De txt record activeert de SEG om het MTA-STS-beleid te controleren, gehost op een HTTPS-webserver.
- Het beleid bepaalt de parameters voor communicatie naar het domein.
    - Bevat MTA-STS MX hosts om te ontvangen.
    - De modus is gedefinieerd als testmodus of afdwingingsmodus
    - TLSv1.2 of hoger is vereist.

- MTA-STS gebruikt DNS TXT-records voor beleidsdetectie. Het haalt het MTA-STS-beleid van een HTTPS-host.
- Tijdens de TLS-handdruk, die wordt gestart om een nieuw of bijgewerkt beleid van de beleidshost te halen, moet de HTTPS-server een geldig X.509-certificaat voor de "MTA-STS" DNS-ID presenteren.

De aspecten van het verzendende e-maildomein:

- Wanneer een SEG (die MTA verzenden) een e-mail naar een MTA-STS domein verstuurt, controleert het eerst op het beleid van het ontvangende domein MTA-STS.
- Als het beleid is geconfigureerd met Enforce Mode, probeert de verzendende e-mailserver een beveiligde, versleutelde verbinding te maken met de ontvangende e-mailserver (ontvangt MTA). Als een beveiligde verbinding niet tot stand kan worden gebracht

(bijvoorbeeld als het TLS-certificaat ongeldig is of de verbinding is gedegradeerd naar een onveilig protocol), mislukt de levering van de e-mail en wordt de afzender op de hoogte gesteld van de storing.

RFC 8461

# Configureren

Tijdens de installatie worden voorbereidende acties aanbevolen:

1. Controleer of het doeldomein een goed geconfigureerd MTA-STS DNS-record en beleidsrecord heeft, voordat u het SEG-doelcontroleprofiel configureert.

- Dit wordt het meest efficiënt uitgevoerd door toegang te krijgen tot MTA-STS checker webpagina's.
  - Google zoekopdracht "verify-mta-sts domain"
  - Kies een verificatiewebsite uit de zoekresultaten.
  - Voer het doeldomein in.
- Configureer alleen domeinen nadat de controle is voltooid.

2. Gebruik MTA-STS niet op het standaardbeleid Bestemmingscontroles.

- Elk doelcontroleprofiel dat is geconfigureerd om MTA-STS te gebruiken, voegt een kleine belasting toe aan de SEG. Als het standaard Bestemmingscontrolebeleid MTA-STS had geconfigureerd, zonder het domein te verifiëren, zou dit de SEG-service kunnen beïnvloeden.

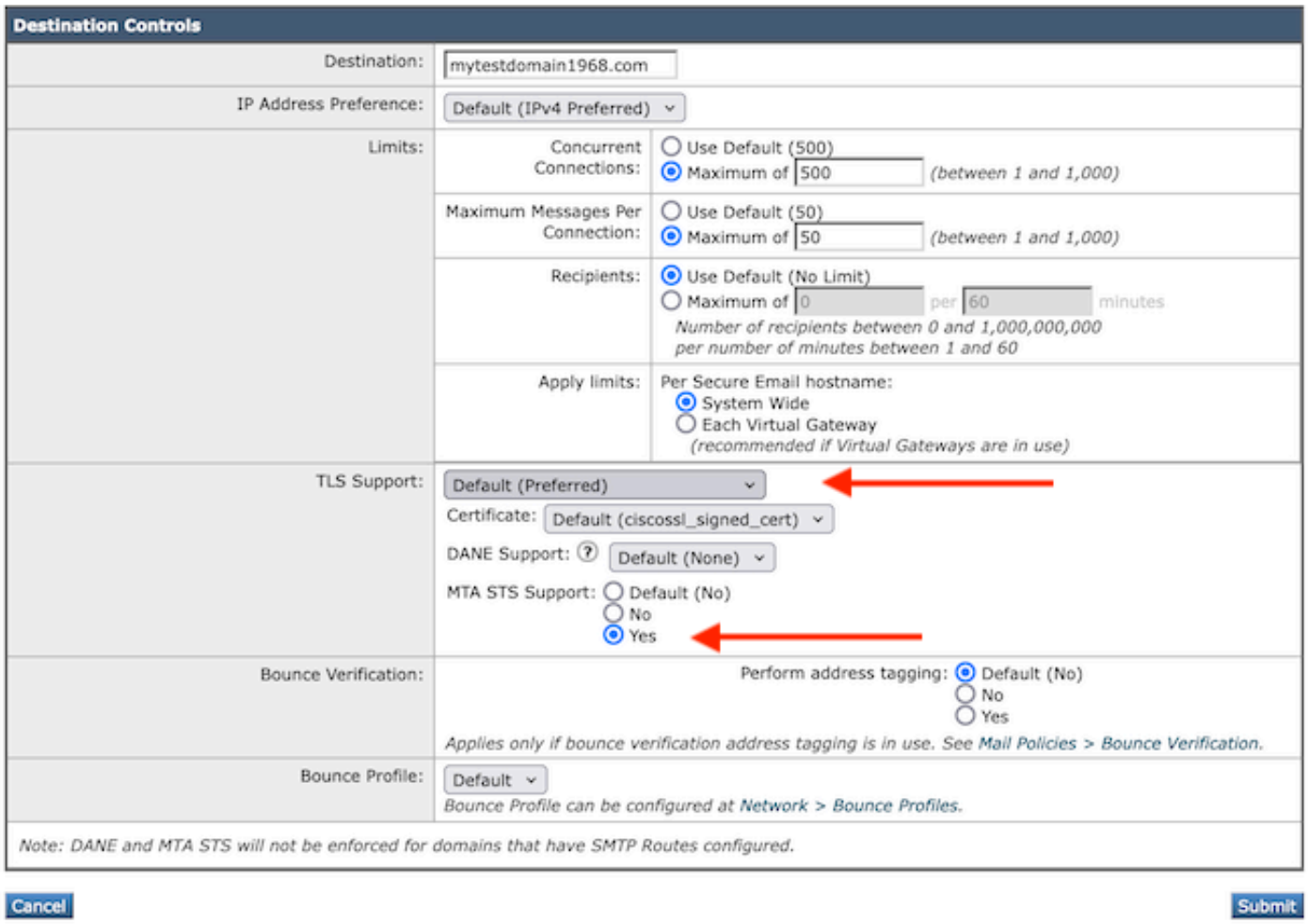
## WebUI-configuratie

- Navigeer naar Mail Policies > Bestemmingscontrole pagina.
- Selecteer Bestemmingsbesturingselementen toevoegen of een bestaand Bestemmingscontroleprofiel bewerken.
  - De TLS-ondersteuningsinstellingen staan alle instellingen toe, behalve Geen, die geschikt zijn voor verschillende TLS-ondersteuningsopties.
  - Het submenu Deen Support Options bevat Verplicht, Opportunistisch, of Geen.
  - MTA-STS ondersteuningsinstelling = Ja
- Selecteer Indienen gevolgd door Toezeggen om de wijzigingen toe te passen.

---

Opmerking: Als de Ontvangende MTA zich in een gehoste omgeving zoals Gsuite of O365 bevindt, configureer dan de Bestemmingsbesturingselementen TLS om TLS Required-verify gehoste domeinen te verifiëren.

---




Bestemmingscontroleprofiel

Interoperabiliteitsvoorbehouden:

DANE Support heeft voorrang op MTA STS en kan de genomen maatregelen beïnvloeden:

- Als DANE slaagt, wordt MTA-STS overgeslagen en wordt post bezorgd.
- Indien DANE verplicht faalt, wordt de post niet bezorgd.
- Als DANE Opportunistic mislukt, en MTA-STS wordt overgeslagen vanwege configuratiefouten, probeert de SEG te leveren met behulp van de geconfigureerde TLS-instelling.
- MTA-STS wordt niet toegepast als een SMTP-route voor het domein is geconfigureerd.

## CLI-configuratie

- destructie
  - nieuw/bewerken
    - Voer de gewenste opties in totdat de menuoptie TLS-opties wordt weergegeven.
    - Opties 2-6 voor TLS ondersteunt MTA-STS.

Wilt u een specifieke TLS-instelling voor dit domein toepassen? [N]> y

Wilt u TLS-ondersteuning gebruiken?
1. Neen

2. Voorkeursbehandeling
3. Vereist
4. Voorkeur - Verifiëren
5. Vereist - Verifiëren
6. Vereist - Controleer gehoste domeinen
[2]

U hebt ervoor gekozen TLS in te schakelen. Gebruik de opdracht certconfig om er zeker van te zijn dat er een geldig certificaat is geconfigureerd.
Wilt u Deens ondersteuning configureren? [N]>

Wilt u MTA STS-ondersteuning configureren? [N]> y

Wilt u MTA STS ondersteuning gebruiken?
1. Uit
2. Aan
[1]> 2

MTA STS wordt niet afgedwongen voor domeinen waarvoor SMTP-routes zijn geconfigureerd:

1. Voltooi de resterende opties om het specifieke doelcontroleprofiel te voltooien.
2. Pas de wijzigingen toe met Indienen > Toewijzen.

# Verifiëren

info level mail_logs:

```
Thu Sep 26 15:23:39 2024 Info: Successfully fetched MTA-STS TXT record for domain(mta-test.domain.com)
Thu Sep 26 15:23:40 2024 Info: New SMTP DCID 834833 interface 10.1.1.2 address 10.1.1.3 port 25
Thu Sep 26 15:23:41 2024 Info: DCID 834833 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384 s
Thu Sep 26 15:23:41 2024 Info: MTA-STS policy for the domain (domain.com) Successful.
Thu Sep 26 15:23:41 2024 Info: Delivery start DCID 834833 MID 5444 to RID [0]
Thu Sep 26 15:23:44 2024 Info: Message finished MID 5444 done
```

debug level mail_logs:

```
Thu Sep 26 15:23:39 2024 Debug: DNS query: Q(_mta-sts.domain.com, 'TXT')
Thu Sep 26 15:23:39 2024 Debug: DNS query: QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent
Thu Sep 26 15:23:39 2024 Debug: DNS query: QIP (_mta-sts.domain.com,'TXT','10.10.5.61',15)
Thu Sep 26 15:23:39 2024 Debug: DNS encache (_mta-sts.domain.com, TXT, [(131794459543073830L, 0, 'insec
Thu Sep 26 15:23:39 2024 Info: Successfully fetched MTA-STS TXT record for domain(domain.com)
Thu Sep 26 15:23:39 2024 Debug: Valid cache entry found for the domain (domain.com).Thu Sep 26 15:23:39
Thu Sep 26 15:23:39 2024 Debug: DNS query: QIP (domain.com,'MX','10.10.5.61',15)
Thu Sep 26 15:23:39 2024 Info: Applying MTA-STS policy for the domain (domain.com)
Thu Sep 26 15:23:40 2024 Info: New SMTP DCID 834833 interface 10.1.1.2 address 10.1.1.3 port 25
Thu Sep 26 15:23:41 2024 Debug: DNS query: Q(domain.com, 'MX')
Thu Sep 26 15:23:41 2024 Info: DCID 834833 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384 s
Thu Sep 26 15:23:41 2024 Info: MTA-STS policy for the domain (domain.com) Successful.
```

```
Thu Sep 26 15:23:41 2024 Info: Delivery start DCID 834833 MID 5444 to RID [0]
Thu Sep 26 15:23:44 2024 Info: Message finished MID 5444 done
```

Door SEG ondersteunde TLS v1.3 ontvangen:

```
Wed Jan 17 21:09:12 2024 Info: ICID 1020089 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

Di Sep 24 09:13:52 2024 Debug: DNS-query: Q(_mta-sts.domain.com, 'TXT')
Di Sep 24 09:13:52 2024 Debug: DNS-query: QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent')
Di Sep 24 09:13:52 2024 Debug: DNS-query: QIP (_mta-sts.domain.com, 'TXT', '10.10.5.61',15)
Di Sep 24 09:13:52 2024 Debug: DNS-encache (_mta-sts.domain.com, TXT, [(131366525701580508L, 0, 'insecure', ('v=STSv1; id=12345678598Z;",)])
Tue Sep 24 09:13:52 2024 Info: Met succes gehaalde MTA-STS TXT-record voor domein(domain.com)
Di Sep 24 09:13:52 2024 Debug: Fetch MTA-STS beleid voor het domein(domain.com)
Di Sep 24 09:13:52 2024 Debug: MTA-STS-beleidsophalen via proxy aanvragen
Di Sep 24 09:13:52 2024 Debug: Verzoek om het STS-beleid te halen is mislukt vanwege een verbindingsonderbreking., voor het domein domain.com
Tue Sep 24 09:13:52 2024 Info: Falen aangetroffen tijdens het halen van MTA-STS-beleid voor het domein(domain.com)

---

19 sep. 13:04:50 2024 Info: Met succes gehaalde MTA-STS TXT-record voor domein(domain.com)
19 sep. 13:04:50 2024 Debug: Fetch MTA-STS beleid voor het domein(domain.com)
19 sep. 13:04:50 2024 Debug: MTA-STS-beleidsophalen via proxy aanvragen
19 sep. 13:04:50 2024 Debug: Verzoek om het STS-beleid te halen is mislukt vanwege een verbindingsonderbreking., voor het domein domain.com
19 sep. 13:04:50 2024 Info: Falen aangetroffen tijdens het halen van MTA-STS-beleid voor het domein(domain.com)

19 sep. 13:04:50 2024 Info: MID 5411 in wachtrij voor levering

# Problemen oplossen

1. Als SEG niet kan leveren met de fout "peer cert niet past bij domain.com".

Dit geeft aan dat de bestemming een gehoste service is, zoals G Suite of M365. Wijzig de doelcontrolesprofielinstelling TLS > TLS Vereist - Controleer gehoste domeinen:

```
Tue Sep 24 10:02:52 2024 Info: DCID 831556 TLS deferring: verify error: peer cert does not match domain
```

```
Tue Sep 24 10:02:52 2024 Info: DCID 831556 TLS was required but could not be successfully negotiated
```

2. Communicatie mislukt als de verzendende of ontvangende certificaten niet correct zijn geconfigureerd of verlopen.

3. De SEG moet controleren of de juiste tussencertificaten en basiscertificaten in de lijst van certificeringsinstanties staan.

4. Eenvoudige Telnet-tests van de SEG-client om de DNS-txt-record en een basistests op de beleidswebserver te verifiëren.

- DNS-query van cli > dig _mta-sts.domain.com txt:

; DEEL ANTWOORD:
_mta-sts.domain.com. 0 IN TXT "v=STSv1; id=12345678598Z;"

- Telnet om de basis bereikbaarheid van een webserver van client > Telnet mta-sts.domain.com 443 te verifiëren:
- Gebruik een reguliere webbrowser om het MTA-STS-beleid te bekijken.
  - https://mta-sts.domain.com/.well-known/mta-sts.txt

```
version: STSv1
mode: enforce
mx: *.mail123.domain.com
max_age: 604800
```

## Gerelateerde informatie

- Cisco Secure Email Gateway-startpagina voor ondersteuningshandleidingen

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.