# Guide de configuration de création de certificats pour TLS sur ESA

## Table des matières



## Introduction

Ce document décrit comment créer un certificat pour une utilisation avec TLS, activer TLS entrant / sortant et dépanner des problèmes sur Cisco ESA.

## Conditions préalables

### Exigences

Aucune exigence spécifique n'est associée à ce document.

### Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

## Informations générales

L'implémentation TLS sur l'ESA assure la confidentialité de la transmission point à point des e-mails via le cryptage. Il permet à un administrateur d'importer un certificat et une clé privée à partir d'un service d'autorité de certification (CA) ou d'utiliser un certificat auto-signé.

Cisco AsyncOS for Email Security prend en charge l'extension *STARTTLS* au protocole SMTP (Simple Mail Transfer Protocol) (*Secure SMTP over TLS*).

> **Conseil** : pour plus d'informations sur TLS, reportez-vous à la RFC 3207.

> **Remarque** : ce document décrit comment installer des certificats au niveau du cluster à l'aide de la fonctionnalité *Gestion centralisée* sur l'ESA. Les certificats peuvent également être appliqués au niveau de l'ordinateur. Toutefois, si l'ordinateur est supprimé du cluster, puis rajouté, les certificats de niveau ordinateur sont perdus.

### Présentation fonctionnelle et exigences

Un administrateur souhaite créer un certificat auto-signé sur l'appliance pour l'une des raisons suivantes :

- Afin de chiffrer les conversations SMTP avec d'autres MTA qui utilisent TLS (les conversations entrantes et sortantes).
- Afin d'activer le service HTTPS sur l'appliance pour l'accès à l'interface utilisateur graphique via HTTPS.
- Àutiliser comme certificat client pour les protocoles LDAP (Lightweight Directory Access Protocol), si le serveur LDAP requiert un certificat client.
- Afin de permettre une communication sécurisée entre l'appliance et le Rivest-Shamir-Addleman (RSA) Enterprise Manager for Data Loss Protection (DLP).
- Afin de permettre une communication sécurisée entre l'appliance et une appliance Cisco Advanced Malware Protection (AMP) Threat Grid.

L'ESA est livré préconfiguré avec un certificat de démonstration qui peut être utilisé afin d'établir des connexions TLS.

> **Attention** : bien que le certificat de démonstration soit suffisant pour établir une connexion TLS sécurisée, sachez qu'il ne peut pas offrir une connexion vérifiable.

Cisco recommande que vous obteniez un certificat X.509, ou PEM (Privacy Enhanced Email) d'une autorité de certification. On parle également de certificat *Apache*. Le certificat d'une autorité de certification est préférable au certificat auto-signé, car un certificat auto-signé est similaire au certificat de démonstration mentionné précédemment, qui ne peut pas offrir une connexion vérifiable.

> **Remarque** : le format du certificat PEM est défini plus en détail dans les RFC 1421 à RFC 1424. Le PEM est un format de conteneur qui peut inclure uniquement le certificat public (comme avec les installations Apache et les fichiers de certificats CA */etc/ssl/certs*) ou une chaîne de certificats complète, pour inclure la clé publique, la clé privée et les certificats racine. Le nom *PEM* provient d'une méthode qui a échoué pour la messagerie sécurisée, mais le format de conteneur qu'il a utilisé est toujours actif et est une traduction en base 64 des clés ASN.1 X.509.

#### Apportez votre propre certificat

L'option d'importation de votre propre certificat est disponible sur l'ESA ; cependant, le certificat doit être au format *PKCS#12*. Ce format inclut la clé privée. Les administrateurs ne disposent pas souvent de certificats disponibles dans ce format. Pour cette raison, Cisco vous recommande de générer le certificat sur l'ESA et de le faire signer correctement par une autorité de certification.

#### Mettre à jour un certificat actuel

Si un certificat qui existe déjà a expiré, ignorez la section *Déploiement de certificats auto-signés* de ce document et resignez le certificat qui existe.

> **Conseil** : reportez-vous au document Cisco Renew a Certificate on an Email Security Appliance pour plus de détails.

# Déployer des certificats auto-signés

Cette section décrit comment générer un certificat auto-signé et une demande de signature de certificat (CSR), fournir le certificat auto-signé à une autorité de certification pour signature, télécharger le certificat signé vers l'ESA, spécifier le certificat à utiliser avec les services ESA et sauvegarder la configuration de l'appliance et le ou les certificats.

## Générer un certificat auto-signé et un CSR

Pour créer un certificat auto-signé via l'interface de ligne de commande, entrez la commande **certconfig**.

Pour créer un certificat auto-signé à partir de l'interface utilisateur graphique :

1. Accédez à **Network > Certificates > Add Certificate** à partir de l'interface utilisateur graphique de l'appliance.

2. Cliquez sur le menu déroulant **Create Self-Signed Certificate**.

   Lorsque vous créez le certificat, assurez-vous que le *Common Name* correspond au nom d'hôte de l'interface d'écoute, ou qu'il correspond au nom d'hôte de l'interface de remise. L'interface *listening* est l'interface qui est liée à l'écouteur qui est configuré sous **Network > Listeners**.L'interface *delivery* est automatiquement sélectionnée, sauf si elle est explicitement configurée à partir de l'interface de ligne de commande avec la commande **deliveryconfig**.
3. Pour une connexion entrante vérifiable, vérifiez que ces trois éléments correspondent :

   Enregistrement MX (nom d'hôte DNS (Domain Name System))

   Nom commun

   Nom d'hôte

   **Remarque** : le nom d'hôte du système n'affecte pas les connexions TLS en ce qui concerne la vérification. Le nom d'hôte du système s'affiche dans le coin supérieur droit de l'interface utilisateur graphique de l'appliance ou dans le résultat de la commande **sethostname de l'**interface de ligne de commande.

   **Attention** : n'oubliez pas d'**envoyer** et de **valider** vos modifications avant d'exporter le CSR. Si ces étapes ne sont pas terminées, le nouveau certificat n'est pas validé dans la configuration de l'appliance et le certificat signé de l'autorité de certification ne peut pas signer ou être appliqué à un certificat existant.

## Fournir le certificat auto-signé à une autorité de certification

Pour envoyer le certificat auto-signé à une autorité de certification pour signature :

1. Enregistrez le CSR sur un ordinateur local au format PEM **Réseau > Certificats > Nom du certificat > Télécharger la demande de signature de certificat**.

2. Envoyer le certificat généré à une autorité de certification reconnue pour signature.

3. Demandez un certificat formaté X.509/PEM/Apache, ainsi que le certificat intermédiaire.

L'autorité de certification génère ensuite un certificat au format PEM.

**Remarque** : pour obtenir la liste des fournisseurs d'autorité de certification, reportez-vous à l'article Wikipédia de l'autorité de certification.

## Télécharger le certificat signé sur l'ESA

Une fois que l'autorité de certification a renvoyé le certificat public approuvé signé par une clé privée, téléchargez le certificat signé vers l'ESA.

Le certificat peut ensuite être utilisé avec un écouteur public ou privé, un service HTTPS d'interface IP, l'interface LDAP ou toutes les connexions TLS sortantes aux domaines de destination.

Pour télécharger le certificat signé vers l'ESA :

1. Assurez-vous que le certificat public approuvé reçu utilise le format PEM ou un format qui peut être converti en PEM avant de le télécharger vers l'appliance. **Conseil** : Vous pouvez utiliser la boîte à outils OpenSSL, un logiciel gratuit, afin de convertir le format.
2. Téléchargez le certificat signé :

   Accédez à **Réseau > Certificats**.

   Cliquez sur le nom du certificat qui a été envoyé à l'autorité de certification pour signature.

   Entrez le chemin d'accès au fichier sur l'ordinateur local ou le volume réseau.

   **Remarque** : lorsque vous téléchargez le nouveau certificat, il remplace le certificat actuel. Un certificat intermédiaire associé au certificat auto-signé peut également être téléchargé.

   **Attention** : n'oubliez pas d'**envoyer** et de **valider** les modifications après avoir téléchargé le certificat signé.

## Spécifier le certificat à utiliser avec les services ESA

Maintenant que le certificat est créé, signé et téléchargé vers l'ESA, il peut être utilisé pour les services qui nécessitent une utilisation de certificat.

### TLS entrant

Complétez ces étapes afin d'utiliser le certificat pour les services TLS entrants :

1. Accédez à **Réseau > Écouteurs**.
2. Cliquez sur le nom du processus d'écoute.
3. Sélectionnez le nom du certificat dans le menu déroulant *Certificate*.
4. Cliquez sur Submit.
5. Répétez les étapes 1 à 4 si nécessaire pour d'autres écouteurs.
6. **Validez** les modifications.

### TLS sortant

Complétez ces étapes afin d'utiliser le certificat pour les services TLS sortants :

1. Accédez à **Politiques de messagerie > Contrôles de destination**.
2. Cliquez sur **Modifier les paramètres globaux...** dans la section *Paramètres globaux*.
3. Sélectionnez le nom du certificat dans le menu déroulant *Certificate*.
4. Cliquez sur Submit.
5. **Validez** les modifications.

### HTTPS

Complétez ces étapes afin d'utiliser le certificat pour les services HTTPS :

1. Accédez à **Network > IP Interfaces**.
2. Cliquez sur le nom de l'interface.
3. Sélectionnez le nom du certificat dans le menu déroulant *HTTPS Certificate*.
4. Cliquez sur Submit.
5. Répétez les étapes 1 à 4 si nécessaire pour toute interface supplémentaire.
6. **Validez** les modifications.

### LDAP

Complétez ces étapes afin d'utiliser le certificat pour les LDAP :

1. Accédez à **Administration système > LDAP**.
2. Cliquez sur **Modifier les paramètres...** dans la section *Paramètres globaux LDAP*.
3. Sélectionnez le nom du certificat dans le menu déroulant *Certificate*.
4. Cliquez sur Submit.
5. **Validez** les modifications.

### Filtrage des URL

Pour utiliser le certificat pour le filtrage des URL :

1. Entrez la commande **websecurityconfig** dans l'interface de ligne de commande.

2. Passez en revue les invites de commande. Assurez-vous que vous sélectionnez **Y** lorsque vous atteignez cette invite :

```
Do you want to set client certificate for Cisco Web Security Services Authentication?
```

3. Sélectionnez le numéro associé au certificat.

4. Entrez la commande **commit** afin de valider les modifications de configuration.

### Sauvegarde de la configuration de l'appliance et du ou des certificats

Assurez-vous que la configuration de l'appliance est enregistrée à ce stade. La configuration de l'appliance contient le travail de certificat terminé qui a été appliqué via les processus décrits précédemment.

Complétez ces étapes afin d'enregistrer le fichier de configuration de l'appliance :

1. Accédez à **Administration système > Fichier de configuration > Télécharger le fichier sur l'ordinateur local pour afficher ou enregistrer**.

2. Exporter le certificat :

   Accédez à **Réseau > Certificats**.

   Cliquez sur **Exporter le certificat**.

   Sélectionnez le certificat à exporter.

   Entrez le nom de fichier du certificat.

   Entrez un mot de passe pour le fichier de certificat.

   Cliquez sur **Exporter**.

   Enregistrez le fichier sur un ordinateur local ou réseau.

   Vous pouvez exporter des certificats supplémentaires à ce stade ou cliquer sur **Cancel** afin de revenir à l'emplacement **Network > Certificates**.

   **Remarque** : ce processus enregistre le certificat au format PKCS#12, qui crée et enregistre le fichier avec une protection par mot de passe.

## Activer TLS entrant

Afin d'activer TLS pour toutes les sessions entrantes, connectez-vous à l'interface utilisateur graphique Web, choisissez **Politiques de messagerie > Politiques de flux de messagerie** pour l'écouteur entrant configuré, puis complétez ces étapes :

1. Sélectionnez un écouteur pour lequel les stratégies doivent être modifiées.

2. Cliquez sur le lien correspondant au nom de la stratégie afin de la modifier.

3. Dans la section *Security Features*, choisissez l'une des options de *chiffrement et d'authentification* suivantes afin de définir le niveau de TLS qui est requis pour cet écouteur et cette stratégie de flux de messagerie :

   **Éteint** : lorsque cette option est sélectionnée, TLS n'est pas utilisé.

   **Préféré** - Lorsque cette option est sélectionnée, TLS peut négocier du MTA distant à l'ESA. Cependant, si le MTA distant ne négocie pas (avant la réception d'une réponse *220*), la transaction SMTP continue *en clair* (non chiffrée). Aucune tentative n'est effectuée pour vérifier si le certificat provient d'une autorité de certification approuvée. Si une erreur se produit après la réception de la réponse 220, la transaction SMTP ne revient pas en texte clair.

   **Obligatoire** - Lorsque cette option est sélectionnée, TLS peut être négocié du MTA distant vers l'ESA. Aucune tentative n'est effectuée pour vérifier le certificat du domaine. Si la négociation échoue, aucun e-mail n'est envoyé via la connexion. Si la négociation réussit, le message est remis via une session chiffrée.
4. Cliquez sur Submit.

5. Cliquez sur le bouton **Valider les modifications**. Vous pouvez ajouter un commentaire facultatif à ce stade, si vous le souhaitez.

6. Cliquez sur **Commit Changes** afin d'enregistrer les modifications.

La stratégie de flux de messagerie de l'écouteur est désormais mise à jour avec les paramètres TLS que vous avez choisis.

Complétez ces étapes afin d'activer TLS pour les sessions entrantes qui arrivent à partir d'un ensemble sélectionné de domaines :

1. Connectez-vous à l'interface utilisateur graphique Web et choisissez **Politiques de messagerie > Vue d'ensemble HAT**.

2. Ajoutez le nom de domaine complet/IP de l'expéditeur au groupe d'expéditeurs approprié.

3. Modifiez les paramètres TLS de la stratégie de flux de messages associée au groupe d'expéditeurs que vous avez modifié à l'étape précédente.

4. Cliquez sur Submit.

5. Cliquez sur le bouton **Valider les modifications**. Vous pouvez ajouter un commentaire facultatif à ce stade, si vous le souhaitez.

6. Cliquez sur **Commit Changes** afin d'enregistrer les modifications.

La stratégie de flux de messages du groupe d'expéditeurs est désormais mise à jour avec les

paramètres TLS que vous avez choisis.

> **Conseil** : Reportez-vous à cet article pour plus d'informations sur la façon dont l'ESA gère la vérification TLS : Quel est l'algorithme de vérification de certificat sur l'ESA ?

## Activer TLS sortant

Afin d'activer TLS pour les sessions sortantes, connectez-vous à l'interface utilisateur graphique Web, choisissez **Politiques de messagerie > Contrôles de destination**, puis complétez ces étapes :

1. Cliquez sur **Ajouter une destination...**.
2. Ajoutez le domaine de destination.
3. Dans la section *TLS Support*, cliquez sur le menu déroulant et choisissez l'une de ces options afin d'activer le type de TLS qui doit être configuré :

   **None** : lorsque cette option est sélectionnée, TLS n'est pas négocié pour les connexions sortantes de l'interface vers le MTA pour le domaine.

   **Préféré** : lorsque cette option est sélectionnée, TLS est négocié de l'interface ESA vers le ou les MTA du domaine. Cependant, si la négociation TLS échoue (avant la réception d'une réponse 220), la transaction SMTP continue *en clair* (non chiffrée). Aucune tentative n'est effectuée pour vérifier si le certificat provient d'une autorité de certification approuvée. Si une erreur se produit après la réception de la réponse 220, la transaction SMTP ne revient pas en texte clair.

   **Obligatoire** - Lorsque cette option est sélectionnée, TLS est négocié de l'interface ESA vers les MTA pour le domaine. Aucune tentative n'est effectuée pour vérifier le certificat du domaine. Si la négociation échoue, aucun e-mail n'est envoyé via la connexion. Si la négociation réussit, le message est remis via une session chiffrée.

   **Preferred-Verify** : lorsque cette option est sélectionnée, TLS est négocié de l'ESA vers le ou les MTA du domaine et l'appliance tente de vérifier le certificat de domaine. Dans ce cas, ces trois résultats sont possibles :

   Le TLS est négocié et le certificat est vérifié. Le courrier est envoyé via une session chiffrée.

   Le TLS est négocié, mais le certificat n'est pas vérifié. Le courrier est envoyé via une session chiffrée.

   Aucune connexion TLS n'est établie et le certificat n'est pas vérifié. Le message électronique est envoyé en texte brut.**Required-Verify** : lorsque cette option est sélectionnée, TLS est négocié de l'ESA vers le ou les MTA pour le domaine, et la vérification du certificat de domaine est requise. Dans ce cas, ces trois résultats sont possibles :

   Une connexion TLS est négociée et le certificat est vérifié. Le message électronique est

envoyé via une session chiffrée.

Une connexion TLS est négociée, mais le certificat n'est pas vérifié par une autorité de certification approuvée. Le courrier n'est pas remis.

Une connexion TLS n'est pas négociée, mais le courrier n'est pas remis.

4. Apportez les modifications supplémentaires nécessaires aux *contrôles* de *destination* pour le domaine de destination.

5. Cliquez sur Submit.

6. Cliquez sur le bouton **Valider les modifications**. Vous pouvez ajouter un commentaire facultatif à ce stade, si vous le souhaitez.

7. Cliquez sur **Commit Changes** afin d'enregistrer les modifications.

# Symptômes d'erreur de configuration du certificat ESA

TLS fonctionne avec un certificat auto-signé, mais si la vérification TLS est requise par l'expéditeur, un certificat signé par l'autorité de certification doit être installé.

La vérification TLS peut échouer même si un certificat signé par une autorité de certification a été installé sur l'ESA.

Dans ce cas, il est recommandé de vérifier le certificat en suivant les étapes de la section Vérifier.

# Vérifier

## Vérification de TLS avec un navigateur Web

Afin de vérifier le certificat signé par l'autorité de certification, appliquez le certificat au service HTTPS de l'interface graphique utilisateur ESA.

Accédez ensuite à l'interface graphique utilisateur de votre ESA dans votre navigateur Web. Si des avertissements s'affichent lorsque vous accédez à https://youresa, le certificat est probablement enchaîné de manière incorrecte, comme l'absence d'un certificat intermédiaire.

## Vérification de TLS avec des outils tiers

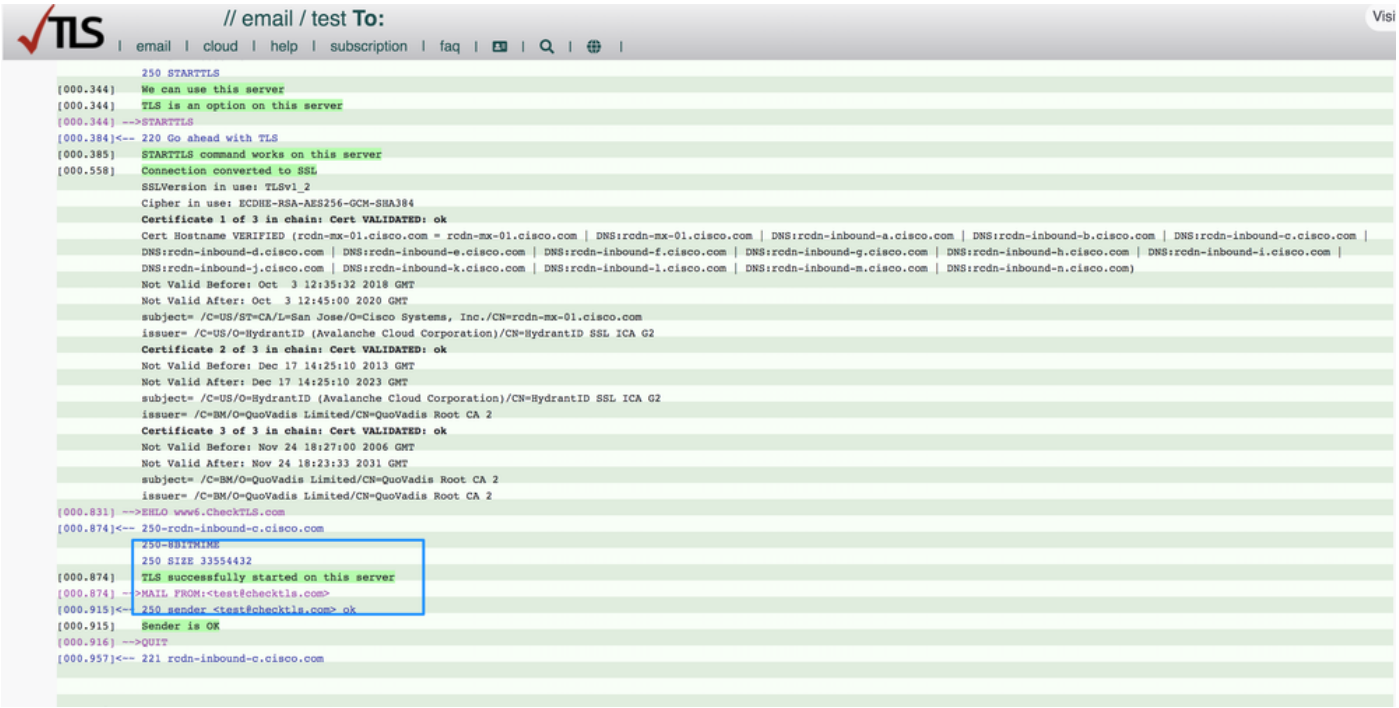
Avant le test, assurez-vous que le certificat à tester est appliqué au niveau de l'écouteur où votre appliance reçoit le courrier entrant.

Des outils tiers tels que CheckTLS.com et SSL-Tools.net peuvent être utilisés pour vérifier le chaînage approprié du certificat.

**Exemple de résultat CheckTLS.com pour la vérification TLS réussie**

## CheckTLS Confidence Factor for "postmaster@cisco.com": 100

| MX Server | Pref | Answer | Connect | HELO | TLS | Cert | Secure | From |
|---|---|---|---|---|---|---|---|---|
| alln-mx-01.cisco.com [173.37.147.230:25] | 10 | OK (41ms) | OK (422ms) | OK (50ms) | OK (48ms) | OK (450ms) | OK (58ms) | OK (41ms) |
| rcdn-mx-01.cisco.com [72.163.7.166:25] | 20 | OK (41ms) | OK (260ms) | OK (42ms) | OK (41ms) | OK (446ms) | OK (43ms) | OK (42ms) |
| aer-mx-01.cisco.com [173.38.212.150:25] | 30 | OK (80ms) | OK (484ms) | OK (81ms) | OK (79ms) | OK (548ms) | OK (80ms) | OK (81ms) |
| **Average** | | 100% | 100% | 100% | 100% | 100% | 100% | 100% |




Exemple de sortie CheckTLS.com pour l'échec de la vérification TLS

CERT Hostname NE VÉRIFIE PAS (mailC.example.com != gvsvipa006.example.com)
**Résolution**

> **Remarque :** si un certificat auto-signé est utilisé, le résultat attendu dans la colonne « Cert OK » est « FAIL ».

Si un certificat signé par une autorité de certification est en cours d'utilisation et que TLS-verify échoue toujours, vérifiez que ces éléments correspondent :

- Nom commun du certificat.
- Nom d'hôte (dans GUI > Network > Interface).
- MX record hostname : il s'agit de la colonne MX Server dans la table TestReceiver.

Si un certificat signé par une autorité de certification a été installé et que vous voyez des erreurs, passez à la section suivante pour obtenir des informations sur la façon de résoudre le problème.

# Dépannage

Cette section décrit comment dépanner les problèmes TLS de base sur l'ESA.

## Certificats intermédiaires

Recherchez des certificats intermédiaires en double, en particulier lorsque les certificats actuels sont mis à jour au lieu d'une nouvelle création de certificat. Le ou les certificats intermédiaires ont peut-être été modifiés ou chaînés de manière incorrecte, et le certificat a peut-être téléchargé plusieurs certificats intermédiaires. Cela peut entraîner des problèmes de chaînage et de vérification des certificats.

## Activer les notifications pour les échecs de connexion TLS requis

Vous pouvez configurer l'ESA afin d'envoyer une alerte si la négociation TLS échoue lorsque les messages sont remis à un domaine qui nécessite une connexion TLS. Le message d'alerte contient le nom du domaine de destination pour la négociation TLS ayant échoué. L'ESA envoie le message d'alerte à tous les destinataires configurés pour recevoir des alertes de niveau de gravité Avertissement pour les types d'alerte *Système*.

> **Remarque** : il s'agit d'un paramètre global, qui ne peut donc pas être défini par domaine.

Complétez ces étapes afin d'activer les alertes de connexion TLS :

1. Accédez à **Politiques de messagerie > Contrôles de destination**.
2. Cliquez sur **Modifier les paramètres globaux**.
3. Cochez la case **Envoyer une alerte en cas d'échec d'une connexion TLS requise**.

   **Conseil** : vous pouvez également configurer ce paramètre à l'aide de la commande

**destconfig > setup** CLI.

L'ESA consigne également les instances pour lesquelles TLS est requis pour un domaine, mais n'a pas pu être utilisé dans les journaux de messagerie de l'appliance. Cela se produit lorsque l'une de ces conditions est remplie :

- Le MTA distant ne prend pas en charge ESMTP (par exemple, il ne comprenait pas la commande *EHLO* de l'ESA).
- Le MTA distant prend en charge ESMTP, mais la commande *STARTTLS* n'était pas dans la liste des extensions qu'elle a annoncées dans sa réponse *EHLO*.
- Le MTA distant a annoncé l'extension *STARTTLS*, mais a répondu avec une erreur lorsque l'ESA a envoyé la commande *STARTTLS*.

## Localisation des sessions de communication TLS réussies dans les journaux de messagerie

Les connexions TLS sont enregistrées dans les journaux de messagerie, ainsi que d'autres actions importantes liées aux messages, telles que les actions de filtrage, les verdicts antivirus et antispam et les tentatives de remise. Si la connexion TLS est établie, une entrée de *réussite* TLS est créée dans les journaux de messagerie. De même, une connexion TLS défaillante produit une entrée TLS *défaillante*. Si aucun message n'est associé à une entrée TLS dans le fichier journal, ce message n'a pas été transmis via une connexion TLS.

> **Conseil** : pour comprendre les journaux de messagerie, reportez-vous au document Cisco ESA Message Disposition Determination.

Voici un exemple de connexion TLS réussie à partir de l'hôte distant (réception) :

```
Tue Apr 17 00:57:53 2018 Info: New SMTP ICID 590125205 interface Data 1 (192.168.1.1) address
10.0.0.1 reverse dns host mail.example.com verified yes
Tue Apr 17 00:57:53 2018 Info: ICID 590125205 ACCEPT SG SUSPECTLIST match sbrs[-1.4:2.0] SBRS -
1.1
Tue Apr 17 00:57:54 2018 Info: ICID 590125205 TLS success protocol TLSv1 cipher DHE-RSA-AES256-
SHA
Tue Apr 17 00:57:55 2018 Info: Start MID 179701980 ICID 590125205
```

Voici un exemple d'échec de connexion TLS à partir de l'hôte distant (réception) :

```
Mon Apr 16 18:59:13 2018 Info: New SMTP ICID 590052584 interface Data 1 (192.168.1.1) address
10.0.0.1 reverse dns host mail.example.com verified yes
Mon Apr 16 18:59:13 2018 Info: ICID 590052584 ACCEPT SG UNKNOWNLIST match sbrs[2.1:10.0] SBRS
2.7
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 TLS failed: (336109761, 'error:1408A0C1:SSL
routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 lost
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 close
```

Voici un exemple de connexion TLS réussie à l'hôte distant (livraison) :

```
Tue Apr 17 00:58:02 2018 Info: New SMTP DCID 41014367 interface 192.168.1.1 address 10.0.0.1
port 25
Tue Apr 17 00:58:02 2018 Info: DCID 41014367 TLS success protocol TLSv1.2 cipher ECDHE-RSA-
AES256-GCM-SHA384
Tue Apr 17 00:58:03 2018 Info: Delivery start DCID 41014367 MID 179701982 to RID [0]
```

Voici un exemple d'échec de connexion TLS à l'hôte distant (livraison) :

```
Mon Apr 16 00:01:34 2018 Info: New SMTP DCID 40986669 interface 192.168.1.1 address 10.0.0.1
port 25
Mon Apr 16 00:01:35 2018 Info: Connection Error: DCID 40986669 domain: domain IP:10.0.0.1 port:
25 details: 454-'TLS not available due to
temporary reason' interface: 192.168.1.1 reason: unexpected SMTP response
Mon Apr 16 00:01:35 2018 Info: DCID 40986669 TLS failed: STARTTLS unexpected response
```

# Informations connexes

- Appliance de sécurisation de la messagerie Cisco - Guides de l'utilisateur final
- Cisco Content Security Management Appliance - Guides d'utilisation
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.