

ESA Présentation des alertes d'expiration de certificat de liste d'autorité de certification personnalisée

Contenu

[Introduction](#)

[Components Used](#)

[Informations générales](#)

[Problème](#)

[Solution](#)

[Informations connexes](#)

Introduction

Ce document décrit les alertes d'expiration de certificat de l'autorité de certification personnalisée (CA) sur une passerelle de messagerie sécurisée Cisco (ESA) après la mise à niveau vers Async OS 14.x, ainsi qu'une solution de contournement.


Components Used

Les informations de ce document sont basées sur l'ESA exécutant Async OS 14.0 ou version ultérieure.

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

Au cours du processus de mise à niveau vers Async OS 14.x, les clients sont invités à confirmer s'ils souhaitent ajouter des certificats système plus anciens à la liste d'autorités de certification personnalisée. Ceci est également documenté dans les notes de version 14.0, comme le montre la capture d'écran ci-dessous, des notes de version complètes sont disponibles [ici](#).

<p>Certificate Authority Configuration Changes</p>	<p>The Certificate Authority (CA) configuration changes are applicable in any one of the following scenarios:</p> <ul style="list-style-type: none"> • Upgrade from a lower AsyncOS version to AsyncOS 14.0 version and later. • Install AsyncOS 14.0 for Cisco Secure Email Gateway for the first time. <p>The following changes are made to the Certificate Authorities list:</p> <ul style="list-style-type: none"> • You can view the count and details of custom and system CA certificates in your email gateway. Use the Managed Trusted Root Certificates option in Network > Certificates > page to view the custom or system CA certificate details. • You can upload, delete, or append the custom CA certificate in your email gateway. • You will not be able to upload duplicate custom CA certificates to your email gateway. • [Applicable for new AsyncOS install only]: You can update the existing system CA certificate bundle to the latest available version. Use the Update Now option in Network > Certificates page in the web interface or the <code>updatenow</code> CLI command to update the existing system CA certificate bundle. • [Applicable for AsyncOS upgrade only]: <ul style="list-style-type: none"> – During upgrade, you can choose to append the valid CA certificates from the system CA bundle (of the current AsyncOS build) to the custom CA bundle of the upgraded AsyncOS build. <p> Note The backup of the current system CA bundle is stored in the following location -</p> <pre data-bbox="726 1288 1316 1332">/data/pub/systemca.old/trustedca.old.pem</pre> <ul style="list-style-type: none"> – After upgrade, the system CA certificate bundle of the current AsyncOS build is updated to the latest version automatically.
--	---

Problème

Après la mise à niveau vers 14.x, les certificats système plus anciens ajoutés à la liste personnalisée peuvent expirer et entraîner des alertes telles que ci-dessous.

26 juin 2021 11:27:29 -0400 Votre certificat « CA : Root CA Generalitat Valenciana » expirera dans 5 jours (s).

Ces alertes indiquent l'expiration des anciens certificats système qui ont été ajoutés à la liste personnalisée au moment de la mise à niveau ou à un certificat personnalisé précédemment utilisé qui approche de l'expiration.

Solution

Veillez noter que les alertes relatives aux anciens certificats système de la liste personnalisée sont informatives et que vous pouvez choisir de les supprimer de la liste personnalisée ou de les laisser expirer.

Il s'agit d'un impact non lié au service, mais pour certains, une alerte indésirable doit être reçue.

Si vous voyez des alertes pour un certificat d'autorité de certification personnalisé requis par votre organisation et qui ne fait pas actuellement partie de la liste système, vous pouvez contacter l'autorité de certification en question pour obtenir un certificat mis à jour et le remplacer comme indiqué dans les guides de l'utilisateur final [ici](#).

L'offre groupée de certificats de l'autorité de certification système est mise à jour automatiquement après la mise à niveau et périodiquement, l'expiration des certificats dans la liste personnalisée n'a pas d'incidence sur le fonctionnement des certificats dans la liste système.

Pour vérifier si la liste système et la liste personnalisée sont toutes deux activées, accédez à Réseau -> Certificats -> Autorités de certification : Modifier les paramètres

Vous pouvez également exporter les listes système et personnalisées à partir du même menu de navigation ou utiliser les commandes CLI certconfig -> certauthority pour consulter manuellement les certificats dans les deux listes, si nécessaire.

Si vous souhaitez supprimer le certificat générant des alertes dans la liste d'autorités de certification personnalisée, voici les étapes qu'un administrateur peut effectuer à l'aide de SSH sur l'appliance.

Note: Veuillez vérifier le nom/la position du certificat dans la liste personnalisée en fonction de l'alerte vue car elle peut différer de l'exemple de sortie vu ci-dessous.

```
example.com> certconfig
```

```
Choose the operation you want to perform:
```

- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists

```
[> certauthority
```

```
Certificate Authority Summary
```

```
Custom List: Enabled
```

```
System List: Enabled Choose the operation you want to perform:
```

- CUSTOM - Manage Custom Certificate Authorities
- SYSTEM - Manage System Certificate Authorities

```
[> custom
```

```
Choose the operation you want to perform:
```

- DISABLE - Disable the custom certificate authorities list
- IMPORT - Import the list of custom certificate authorities
- EXPORT - Export the list of custom certificate authorities
- DELETE - Remove a certificate from the custom certificate authority list
- PRINT - Print the list of custom certificate authorities
- CHECK_CA_FLAG - Check CA flag in uploaded custom CA certs

```
[> delete
```

```
You must enter a value from 1 to 104.
```

1. [AAA Certificate Services]
2. [ANCERT Certificados CGN]


```
66. [Serasa Certificate Authority III]
67. [Serasa Certificate Authority II]
68. [Serasa Certificate Authority I]
69. [Starfield Services Root Certificate Authority]
70. [SwissSign Gold CA - G2]
71. [SwissSign Platinum CA - G2]
72. [SwissSign Silver CA - G2]
73. [Swisscom Root CA 1]
74. [TC TrustCenter Class 2 CA II]
75. [TC TrustCenter Class 3 CA II]
76. [TC TrustCenter Class 4 CA II]
77. [TC TrustCenter Universal CA II]
78. [TC TrustCenter Universal CA I]
79. [TDC OCES CA]
80. [Trusted Certificate Services]
81. [UCA Global Root]
82. [UCA Root]
83. [USERTrust RSA Certification Authority]
84. [VAS Latvijas Pasts SSI(RCA)]
85. [VRK Gov. Root CA]
86. [VeriSign Class 3 Public Primary Certification Authority - G5]
87. [VeriSign Universal Root Certification Authority]
88. [Visa Information Delivery Root CA]
89. [Visa eCommerce Root]
90. [WellsSecure Public Root Certificate Authority]
91. [XRamp Global Certification Authority]
92. [thawte Primary Root CA - G3]
93. [thawte Primary Root CA] Select the custom ca certificate you wish to delete
[]> 59
```

```
Are you sure you want to delete "Root CA Generalitat Valenciana"? [N]> Y
Custom ca certificate "Root CA Generalitat Valenciana" removed
```

Choose the operation you want to perform:

```
- DISABLE - Disable the custom certificate authorities list
- IMPORT - Import the list of custom certificate authorities
- EXPORT - Export the list of custom certificate authorities
- DELETE - Remove a certificate from the custom certificate authority list
- PRINT - Print the list of custom certificate authorities
- CHECK_CA_FLAG - Check CA flag in uploaded custom CA certs
[]> [ENTER]
```

Certificate Authority Summary

Custom List: Enabled

System List: Enabled Choose the operation you want to perform:

```
- CUSTOM - Manage Custom Certificate Authorities
- SYSTEM - Manage System Certificate Authorities
[]> [ENTER]
```

Choose the operation you want to perform:

```
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]> [ENTER]
```

```
example.com> commit
```

Please be sure to commit the change at the end.

Informations connexes

- [Notes de version de Cisco Secure Email Gateway](#)

- [Guides de l'utilisateur final de la passerelle de messagerie sécurisée Cisco](#)