

# Waarschuwingen voor ETA-overeenstemming met aangepaste CA-lijst

## Inhoud

[Inleiding](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Probleem](#)

[Oplossing](#)

[Gerelateerde informatie](#)

## Inleiding

In dit document wordt een beschrijving gegeven van de Aangepaste certificaataanvraag (CA) en van de certificaataanvraag voor een Cisco Secure Email Gateway (ESA) na een upgrade naar Async OS 14.x, samen met een oplossing voor tijdelijke invoer.


## Gebruikte componenten

De informatie in dit document is gebaseerd op het ESR-systeem met Async OS 14.0 of hoger.

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Achtergrondinformatie

Tijdens het upgradeproces naar Async OS 14.x, wordt de klant gevraagd te bevestigen of zij oudere systeemcertificaten aan de aangepaste CA-lijst wilt toevoegen. Dit wordt ook beschreven in de opmerkingen met 14.0 releases, zoals aangegeven in het hieronder weergegeven scherm. [Klik hier](#) om volledige opmerkingen over de release [te](#) maken.

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

## Probleem

Na een upgrade naar 14.x kunnen de meer dan tijd oudere systeemcertificaten die aan de aangepaste lijst zijn toegevoegd, verlopen, wat kan resulteren in waarschuwingen zoals hieronder.

26 jun 2021 11:27:29 -0400 Uw certificaat "CA:Root CA Generalitat Valenciana" verstrijkt in 5 dagen (s).

Deze waarschuwingen zijn kenmerkend voor oudere systeemcertificaten die verstrijken en die op het moment van de upgrade aan de aangepaste lijst zijn toegevoegd, of voor een eerder tijdens de verloopperiode gebruikt aangepast certificaat.

## Oplossing

U dient er op te worden gewezen dat de waarschuwingen voor oudere systeemcertificaten in de aangepaste lijst informatie zijn en u kunt ervoor kiezen deze te verwijderen uit de aangepaste lijst of ze te laten verlopen.

Het heeft geen invloed op het gebruik, maar voor sommigen is het een ongewenste waakzaamheid.

Als u waarschuwingen ziet voor een aangepast CA-certificaat dat door uw organisatie is vereist en momenteel geen deel uitmaakt van de systeemlijst, kunt u naar de betreffende CA gaan voor een bijgewerkt certificaat en deze vervangen zoals [hieronder](#) in de eindgebruikershandleidingen is aangegeven.

Het systeem CA-certificatiebundel wordt automatisch bijgewerkt na een upgrade en periodiek, heeft verloopdatum van certificaten in de aangepaste lijst geen invloed op de werking van certificaten in de systeemlijst.

Om te bevestigen of de systeemlijst en de aangepaste lijst beide beschikbaar zijn, navigeer dan naar Netwerk -> Certificaten -> Certificaatautoriteiten: Instellingen bewerken

U kunt het systeem en de aangepaste lijsten van het zelfde navigatiemenu ook exporteren of de CLI certificateConfiguration -> de opdrachten van de certificeringsinstantie gebruiken om certificaten in beide lijsten handmatig te bekijken zoals vereist.

Als u de waarschuwingen voor het genereren van certificaten wilt verwijderen in de aangepaste CA-lijst, worden hieronder de stappen beschreven die door een beheerder met behulp van SSH aan het apparaat kunnen worden uitgevoerd.

**Opmerking:** Controleer de naam/positie van het certificaat in de aangepaste lijst op basis van de waarschuwing aangezien deze kan afwijken van de onderstaande voorbeelduitvoer.

```
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]
3. [ANCERT Certificados Notariales]
4. [ANCERT Corporaciones de Derecho Publico]
5. [Actalis Authentication Root CA]
6. [Admin-Root-CA]
7. [Agence Nationale de Certification Electronique]
8. [Agence Nationale de Certification Electronique]
9. [America Online Root Certification Authority 1]
10. [America Online Root Certification Authority 2]
11. [Autoridad Certificadora Raiz de la Secretaria de Economia]
12. [Autoridad de Certificacion de la Abogacia]
13. [Baltimore CyberTrust Root]
14. [COMODO Certification Authority]
15. [COMODO RSA Certification Authority]
16. [Certipost E-Trust TOP Root CA]
17. [Certum CA]
18. [Chambers of Commerce Root]
19. [Cisco Root CA 2048]
20. [ComSign Advanced Security CA]
21. [ComSign CA]
22. [ComSign Secured CA]
23. [Cybertrust Global Root]
24. [D-TRUST Root Class 2 CA 2007]
25. [D-TRUST Root Class 3 CA 2007]
26. [DST Root CA X3]
27. [DigiCert Assured ID Root CA]
28. [DigiCert Baltimore CA-2 G2]
29. [DigiCert Global Root CA]
30. [DigiCert Global Root G2]
31. [DigiCert High Assurance EV Root CA]
32. [E-CERT ROOT CA]
33. [Echoworx Root CA2]
34. [Entrust Root Certification Authority - G2]
35. [Entrust Root Certification Authority]
36. [GLOBALTRUST]
37. [GeoTrust Global CA]
38. [GeoTrust Primary Certification Authority - G2]
39. [GeoTrust Primary Certification Authority - G3]
40. [GeoTrust Primary Certification Authority]
41. [GeoTrust RSA CA 2018]
42. [GeoTrust SSL CA - G2]
43. [GeoTrust Universal CA 2]
44. [GeoTrust Universal CA]
45. [Global Chambersign Root]
46. [GlobalSign PersonalSign 2 CA - SHA256 - G3]
47. [GlobalSign Root CA]
48. [GlobalSign]
49. [GlobalSign]
50. [Go Daddy Root Certificate Authority - G2]
51. [Hongkong Post Root CA 1]
52. [HydrantID SSL ICA G2]
53. [InfoNotary CSP Root]
54. [NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado]
55. [Network Solutions Certificate Authority]
56. [OISTE WISEKey Global Root GA CA]
57. [Post. Trust Root CA]
58. [QuoVadis Root CA 2]
59. [Root CA Generalitat Valenciana]  
<<<<<<<<<<<< Select this one based on sample alert above
60. [S-TRUST Authentication and Encryption Root CA 2005:PN]
61. [SSC Root CA A]
62. [SSC Root CA B]
63. [SSC Root CA C]
64. [Secure Global CA]

```
65. [SecureTrust CA]
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.

## Gerelateerde informatie

- [Cisco Secure E-gateway release](#)
- [Cisco Secure Email Gateway-eindgebruikershandleidingen](#)