

ESA Understanding Custom CA List Certificate Expiration Alerts

Contents

[Introduction](#)

[Components Used](#)

[Background Information](#)

[Problem](#)

[Solution](#)

[Related Information](#)

Introduction

This document describes Custom Certificate Authority (CA) Certificate Expiration alerts on an Cisco Secure Email Gateway (ESA) after upgrade to Async OS 14.x, along with a workaround solution.


Components Used

The information in this document is based on ESA running Async OS 14.0 or above.

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

During the upgrade process to Async OS 14.x, customers are requested to confirm if they wish to append older system certificates to the custom CA list. This is also documented in the 14.0 release notes as shown in the screenshot below, complete release notes are available [here](#).

Certificate Authority Configuration Changes	<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 - <code>/data/pub/systemca.old/trustedca.old.pem</code></p> <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.
---	---

Problem

After upgrading to 14.x, over time older system certificates appended in the custom list may expire resulting in alerts such as below.

26 Jun 2021 11:27:29 -0400 Your certificate "CA:Root CA Generalitat Valenciana" will expire in 5 days (s).

These alerts are indicative of either older system certificates expiring which were appended to the custom list at the time of upgrade or a custom certificate previously used nearing expiration.

Solution

Please be advised that the alerts for older system certificates in the custom list are informational and you could choose to remove them from the custom list or let them expire out.

It is non-service impacting, yet for some an undesirable alert to receive.

If you see alerts for a custom CA certificate that is required by your Organization and currently not part of system list, you could reach out to the CA in question for an updated certificate and replace it as outlined in the end user guides [here](#).

The system CA certificate bundle is updated automatically after upgrade and periodically, expiration of certificates in the custom list do not impact the working of certificates in the system list.

To validate if system list and custom list are both enabled, please navigate to Network -> Certificates -> Certificate Authorities: Edit Settings

You can also export the system and custom lists from the same navigation menu or use the CLI certconfig -> certauthority commands to manually review certificates in both list as required.

If you wish to remove the certificate generating alerts in the custom CA list, below are the steps that can be performed by an admin using SSH to the appliance.

Note: Please verify the name/position of the certificate in the custom list based on the alert seen as it may differ from the sample output sighted below.

```
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.

Related Information

- [Cisco Secure Email Gateway Release Notes](#)
- [Cisco Secure Email Gateway End User Guides](#)