

カスタムCAリスト証明書の期限切れアラートについて

内容

[概要](#)

[使用するコンポーネント](#)

[背景説明](#)

[問題](#)

[解決方法](#)

[関連情報](#)

概要

このドキュメントでは、Async OS 14.xへのアップグレード後のCisco Secure Email Gateway(ESA)のカスタム認証局(CA)証明書の期限切れアラートと、回避策のソリューションについて説明します。


使用するコンポーネント

このドキュメントの情報は、Async OS 14.0以降を実行するESAに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Async OS 14.xへのアップグレードプロセス中、お客様は古いシステム証明書をカスタムCAリストに追加するかどうかを確認する必要があります。これは、次のスクリーンショットに示すように、14.0リリースノートにも記載されています。完全なリリースノートはこちらから入手[できま](#)
[す](#)。

<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 - <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.
--	---

問題

14.xにアップグレードした後、カスタムリストに追加された古いシステム証明書の有効期限が切れ、次のようなアラートが表示されることがあります。

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

これらのアラートは、アップグレード時にカスタムリストに追加された古いシステム証明書または期限切れ間近に使用されたカスタム証明書のいずれかを示します。

解決方法

カスタムリスト内の古いシステム証明書のアラートは情報であり、カスタムリストから削除するか、期限切れにするかを選択できます。

これはサービスに影響しませんが、一部の望ましくないアラートが受信されます。

組織で必要で、現在システムリストに含まれていないカスタムCA証明書のアラートが表示された場合は、問題のCAに連絡して更新された証明書を検索し、ここに示すエンドユーザガイドに示すように置き換えることができます。

システムCA証明書バンドルは、アップグレード後に自動的に更新され、定期的にカスタムリストの証明書の有効期限は、システムリストの証明書の動作に影響しません。

システムリストとカスタムリストの両方が有効になっているかどうかを確認するには、[Network] -> [Certificates] -> [Certificate Authorities]に移動します。設定の編集

同じナビゲーションメニューからシステムおよびカスタムリストをエクスポートするか、CLI `certconfig -> certauthority`コマンドを使用して、必要に応じて両方のリストの証明書を手動で確認することもできます。

カスタムCAリストで証明書を生成するアラートを削除する場合は、管理者がアプライアンスにSSHを使用して実行できる手順を次に示します。

注：次に示す出力例とは異なる場合があるため、カスタムリストの証明書の名前と位置を確認してください。

```
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.

関連情報

- [Cisco Secure Eメールゲートウェイリリースノート](#)
- [Cisco Secure Eメールゲートウェイエンドユーザガイド](#)