Troubleshoot Custom CA List Certificate Expiration Alerts on ESA

Contents

[Introduction](#)

[Overview](#)

[Components Used](#)

[Background Information](#)

[Problem](#)

[Solution](#)

[Related Information](#)

Introduction

This document describes custom CA certificate expiration alerts on a Secure Email Gateway (ESA) after an upgrade to AsyncOS 14.x.

Overview

The symptom is expiration alerts for certificates that were appended to the Custom Certificate Authority (CA) list during the upgrade. The impact is limited to informational alerts because expiration of certificates in the custom list does not affect certificates in the system list. The resolution is to verify the certificate source and either replace the required custom CA certificate or remove the expired certificate from the custom list.

Components Used

This document is based on Cisco Secure Email Gateway running AsyncOS 14.0 or later.

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 AsyncOS 14.x, customers are prompted to confirm whether they want to append older system certificates to the custom CA list. This behavior is also documented in the AsyncOS 14.0 release notes, as shown in Image 1. See the Cisco Secure Email Gateway Release Notes for AsyncOS 14.0.

Image 1. Release notes excerpt that shows the upgrade prompt to append older system certificates to the custom CA list.

Certificate Authority Configuration Changes	The Certificate Authority (CA) configuration changes are applicable in any one of the following scenarios: • 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. The following changes are made to the Certificate Authorities list: • 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 `updatenow` CLI command to update the existing system CA certificate bundle. • [**Applicable for AsyncOS upgrade only**]: – 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. **Note** The backup of the current system CA bundle is stored in the following location - `/data/pub/systemca.old/trustedca.old.pem` – After upgrade, the system CA certificate bundle of the current AsyncOS build is updated to the latest version automatically.

Problem

After an upgrade to AsyncOS 14.x, older system certificates that were appended to the custom list can expire over time and generate alerts such as this example.

26 Jun 2021 11:27:29 -0400 Your certificate CA:Root CA Generalitat Valenciana expires 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

The alerts for older system certificates in the custom list are informational, and you can choose to remove them from the custom list or allow them to expire.

This condition does not affect service, but the alert can be undesirable.

If you see alerts for a custom CA certificate that is required by your organization and is not currently part of the system list, contact the CA for an updated certificate and replace it as described in the Cisco Secure Email Gateway Admin Guide certificate management procedure.

The system CA certificate bundle is updated automatically after an upgrade and periodically thereafter. Expiration of certificates in the custom list does not affect certificates in the system list.

To verify that the system list and custom list are both enabled, navigate to **Network > Certificates > Certificate Authorities > Edit Settings**.

You can also export the system and custom lists from the same menu, or use the CLI commands **certconfig** and **certauthority** to review certificates in both lists as needed.

If you want to remove the certificate that generates alerts in the custom CA list, complete these steps as an administrator over SSH to the appliance.

1. Run **certconfig**.
2. Enter **certauthority**, then enter **custom**.
3. Enter **delete** and select the certificate that matches the alert.
4. Confirm the deletion and then run **commit** to save the change.

This CLI example shows the workflow.

Note: Verify the name and position of the certificate in the custom list based on the alert because it can differ from the sample output shown in this example.

```
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 authorties
- EXPORT - Export the list of custom certificate authorties
- DELETE - Remove a certificate from the custom certificate authorty list
- PRINT - Print the list of custom certificate authorties
- CHECK_CA_FLAG - Check CA flag in uploaded custom CA certs
[]> delete

You must enter a value from 1 to 104.
...
59. [Root CA Generalitat Valenciana] <<< Select this certificate based on the sample alert in this exam
...
93. [thawte Primary Root CA]

Select the custom CA certificate you want 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 authorties
- EXPORT - Export the list of custom certificate authorties
- DELETE - Remove a certificate from the custom certificate authorty list
- PRINT - Print the list of custom certificate authorties
- 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
```

Ensure that you run **commit** at the end.

Related Information

- Cisco Secure Email Gateway release notes
- Cisco Secure Email Gateway user guides