Secure Endpoint - Private Cloud Root CA Certificate Expiration

Contents

Introduction

This document describes the required information around the License Regeneration and around this announcement with version 3.9.0 and above. Refer Private Cloud Release Notes: https://docs.amp.cisco.com/Private%20Cloud%20Release%20Notes.pdf

IMPORTANT! A Secure Endpoint Private Cloud root certificate will expire on September 3, 2023. Your license will expire at the same time as a result. Contact support to obtain a new license file and maintain normal operation.

Technical Details

Affected Version: All Supported Cisco Secure Endpoint Private Cloud License generated before April 11th, 2023.

Current Root CA Certificate which is used as the Internal Root CA certificate for our certificate chain would expire as of September 3, 2023. This is a snippet of the Certificate which is located at this path: **/opt/fire/etc/ssl/certs** (You would be able to browse to this path on the appliance only if you have SSH Access Enabled on the Appliance)

[root@fireamp certs]# /usr/bin/openssl x509 -text -noout -in /opt/fire/etc/ssl/certs/root.fireamp.crt Certificate: Issuer: C=US, O=Sourcefire, O=Immunet, OU=PrivateCloud Appliance, CN=FireAMP Private Cloud ROOT CA Validity Not Before: Sep 4 17:32:46 2013 GMT Not After : Sep 2 17:32:46 2023 GMT Subject: C=US, O=Sourcefire, O=Immunet, OU=PrivateCloud Appliance, CN=FireAMP Private Cloud ROOT CA

License regeneration would be required to renew this certificate and the related certificate chain. it is mandatory to get a new license generated and applied on the private cloud appliance to ensure that the device remains functional.

With the License regeneration, these certificates would be renewed:

- ca_intermediate.crt: This is the Intermediate certificate used internally for signing the certificate chain

- ca_signing.crt: This is the certificate used for signing the connectors policies

- chained.fireamp.crt: This is used for certificate validation for internal services

IMPORTANT: root.fireamp.crt would not be renewed as part of the license renewal or with the upgrade to the **3.9.0 release**. This certificate would be renewed as part of the Appliance Version Release **4.0.1**.

Impact

If the new licenses are not installed on the appliance and the CA Cert expires, it would cause **policy sync failures** on the connectors when the policy edits are made from the Portal. So, it is critical that the license is updated before the expiration on **September 3, 2023**

License Regeneration

You would have to contact Secure Endpoint Licensing Team to request your licenses to be regenerated with the updated certificates.

To obtain a new license file please open a support case online in **Support Case Manager:** https://mycase.cloudapps.cisco.com/case

Step 1: Once, you login into the Cisco Support Portal with your Cisco ID, click on "**Open New Case**"

Step 2: Select **Software Licensing â€">Security Related Licensing** -> **FireAMP/ThreatGrid**.

Step 3: Please fill out this information in the "**Problem Description**"

Cisco.com ID:

Product Name: Cisco Secure Endpoint Private Cloud

Issue/Request Details: Private Cloud License with new Root CA

Cisco SO# and/or Web Order ID #:

Business Name:

Full Name:

Email:

Device ID:

IMPORTANT!!

Step 4: We request you to add a screenshot of **License** page from **Administration Portal** (Under **Configuration-> License**)

Step 5: Once, the request is received, we will re-generate a new license. New Licenses would be sent via Email by our Secure Endpoint Provisioning Teams

Replace License

For instructions on how to use the new license which was received from the Cisco Licensing Team, please refer to the Secure Endpoint Private Cloud Administration Portal Guide here: https://docs.amp.cisco.com/SecureEndpointPCAdminGuide.pdf

Refer to the "**License**" Section on Page 28

Once, you replace the license, please reconfigure the appliance for the new license to take effect.

Verification

IMPORTANT: For the appliance on 3.9.0 and above, The Notification on the Private Cloud Appliance Administration Portal would still be present even after the new license is applied and can be safely ignored. This will be fixed on Appliance release 4.1.0 and to validate that the issue has been fixed on earlier releases, we can follow this process.

To ensure that the certificates were renewed correctly, please use the steps as follows:

[root@fireamp certs]# /usr/bin/openssl x509 -text -noout -in /opt/fire/etc/ssl/certs/ca_intermediate.crt Certificate: Data: Version: 3 (0x2) Serial Number: 2 (0x2) Signature Algorithm: sha256WithRSAEncryption Issuer: C=US, O=Sourcefire, O=Immunet, OU=PrivateCloud Appliance, CN=FireAMP Private Cloud ROOT CA Validity Not Before: Mar 2 04:10:43 2023 GMT Not After : Feb 29 04:10:43 2028 GMT

[root@fireamp certs]# /usr/bin/openssl x509 -text -noout -in /opt/fire/etc/ssl/certs/ca_signing.crt Certificate: Data: Version: 3 (0x2) Serial Number: 7330 (0x1ca2) Signature Algorithm: sha256WithRSAEncryption Issuer: C=US, O=Sourcefire, O=Immunet, OU=PrivateCloud Appliance, CN=FireAMP Private Cloud Intermediate CA/emailAddress=private-cloud-licensing@sourcefire.com Validity Not Before: Apr 11 12:42:45 2023 GMT Not After : Apr 9 12:42:45 2028 GMT [root@fireamp certs]# /usr/bin/openssl x509 -text -noout -in /opt/fire/etc/ssl/certs/chained.fireamp.crt Certificate: Data: Version: 3 (0x2) Serial Number: 2 (0x2) Signature Algorithm: sha256WithRSAEncryption Issuer: C=US, O=Sourcefire, O=Immunet, OU=PrivateCloud Appliance, CN=FireAMP Private Cloud ROOT CA Validity Not Before: Mar 2 04:10:43 2023 GMT Not After : Feb 29 04:10:43 2028 GMT