Regenerate the Default Certificate in Intersight Managed Mode

Contents

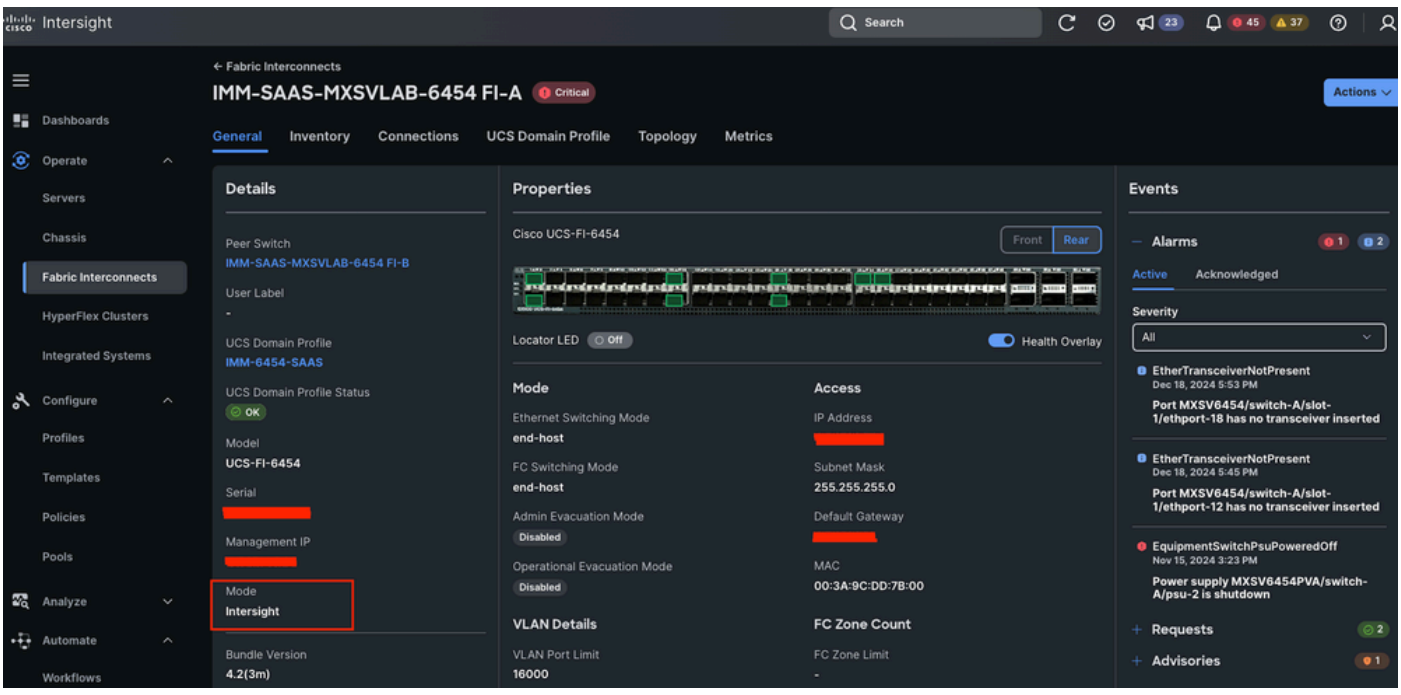
Introduction

This document describes the process to renew a Fabric Interconnect self-signed certificate in Intersight environments (SAAS or Appliance).

Prerequisites

Requirements

UCS domain in Intersight Managed Mode.



UCS Domain Intersight Managed Mode

Components Used

- Fabric Interconnect 6454
- Version: 4.2(3m)

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.

Generate Self-Signed Certificate

Cisco recommends using CA-signed certificates to access the appliance, as modern browsers can restrict access if self-signed certificates are used. The Intersight Virtual Appliance allows you to generate a self-signed certificate to extend its validity if the Cisco-provided certificate expires.

When generating a new self-signed certificate, the existing SSL certificate is replaced, potentially logging you out of the current browser session. If you are not logged out, refresh your **browser** to apply the new certificate. To confirm the update, click the **lock** or **warning** icon next to the URL in your browser's address bar. After refreshing, you are directed to the **Settings > Certificates** page without needing to log in again.

The Device Console User Interface (UI) uses a self-signed certificate with the Common Name (CN) set to switch. This certificate is generated the first time the Fabric Interconnect (FI) is powered on and configured. The self-signed certificate is valid for 365 days, meaning that any FI running for over a year has an expired certificate.

Some customers use automated monitoring tools to scrape the device's IP or hostname over HTTPS and validate the certificate's expiration date. When the certificate expires, these tools can trigger alarms, leading to observability and security teams to flag it as a potential issue.

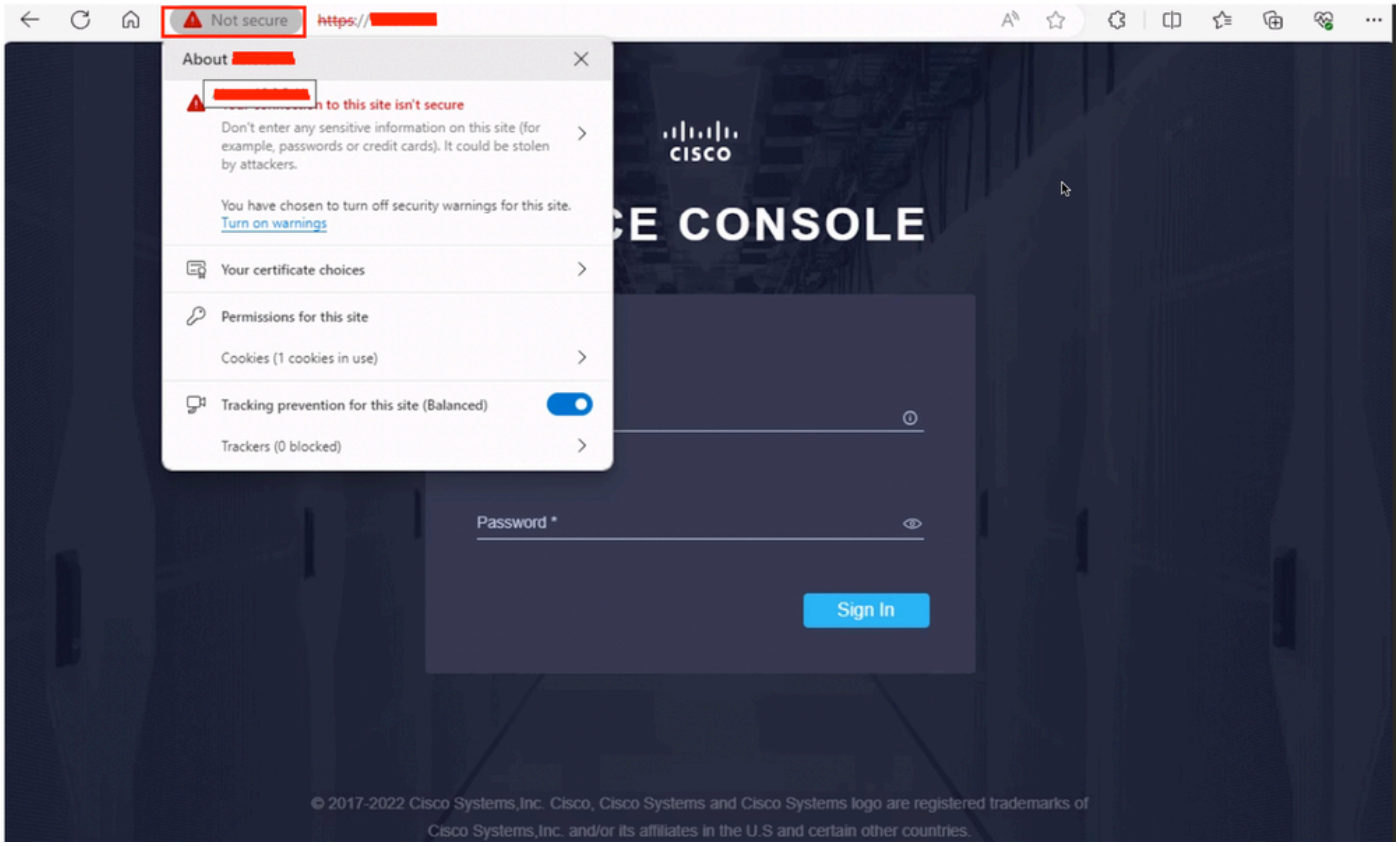
Additionally, because the certificate is self-signed, web browsers do display a Not Secure warning. This warning can also appear if the certificate is expired, potentially causing further security concerns.

To prevent these issues, it is recommended to renew or replace the certificate proactively.

Problem/Symptom

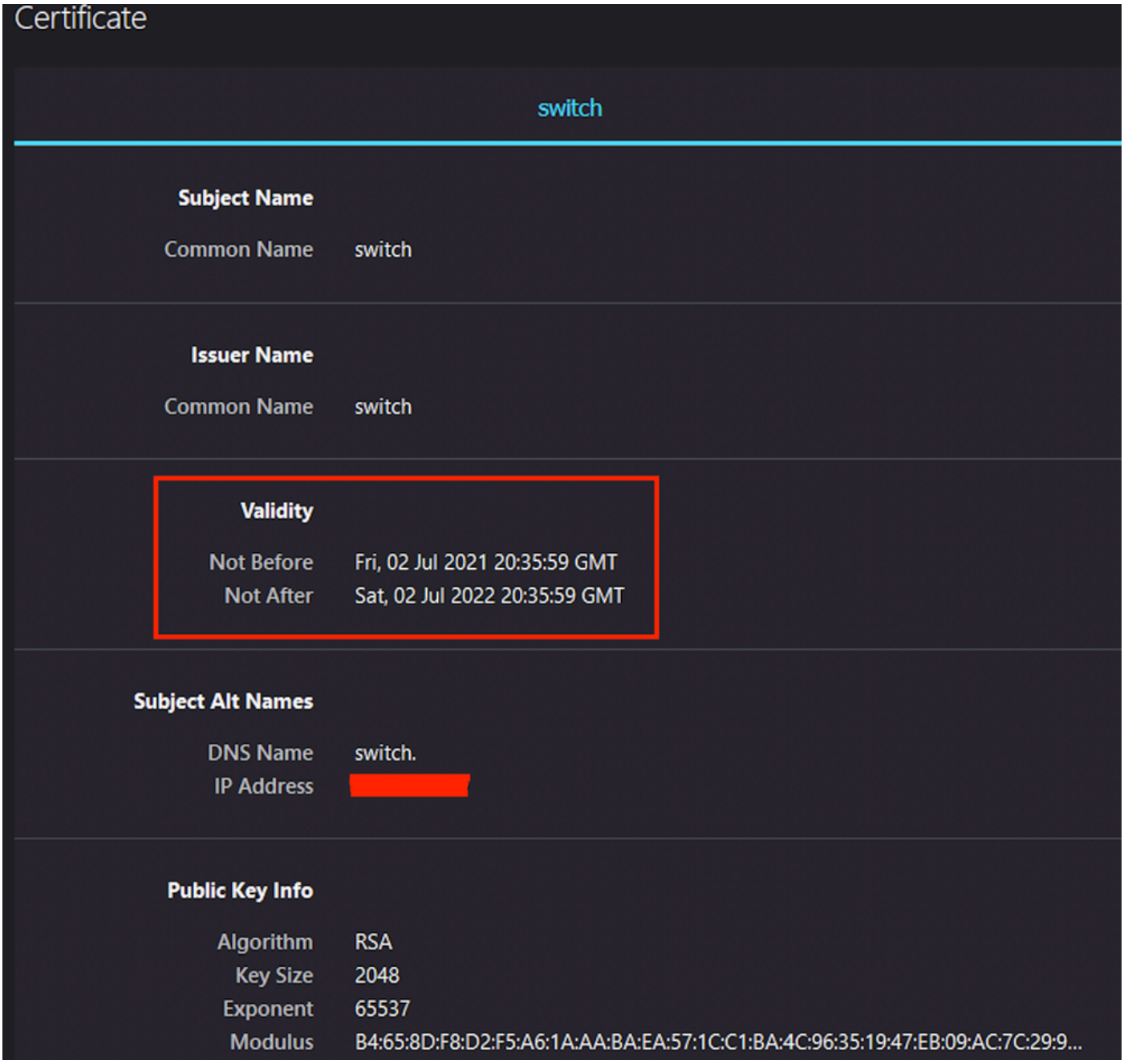
You see the site is not secure when you access the device console.

Note: For device console access, you need the IP address of the Fabric Interconnect.



Certificate Error

When you click the **certificate information**, you see the certification expiration date.



Certificate Expiration Date

Regenerate the Certificate

To renew the default certificate in Intersight, you need to restart the **device console** or reboot the **Fabric Interconnect** (not recommended).

Use these steps to manually regenerate the default certificate in Intersight:

1. Open an **SSH session** using the IP address of one Fabric Interconnect.
2. Run the command:

```
UCS# generate-self-signed-certificate
```

If the certificate generated successfully, you see:

```
hostname is IMM-FI6454
Successfully generated the self-signed-certificates
Successfully restarted the web-server
```

To check the actual certificate and confirm it changed, use this command:

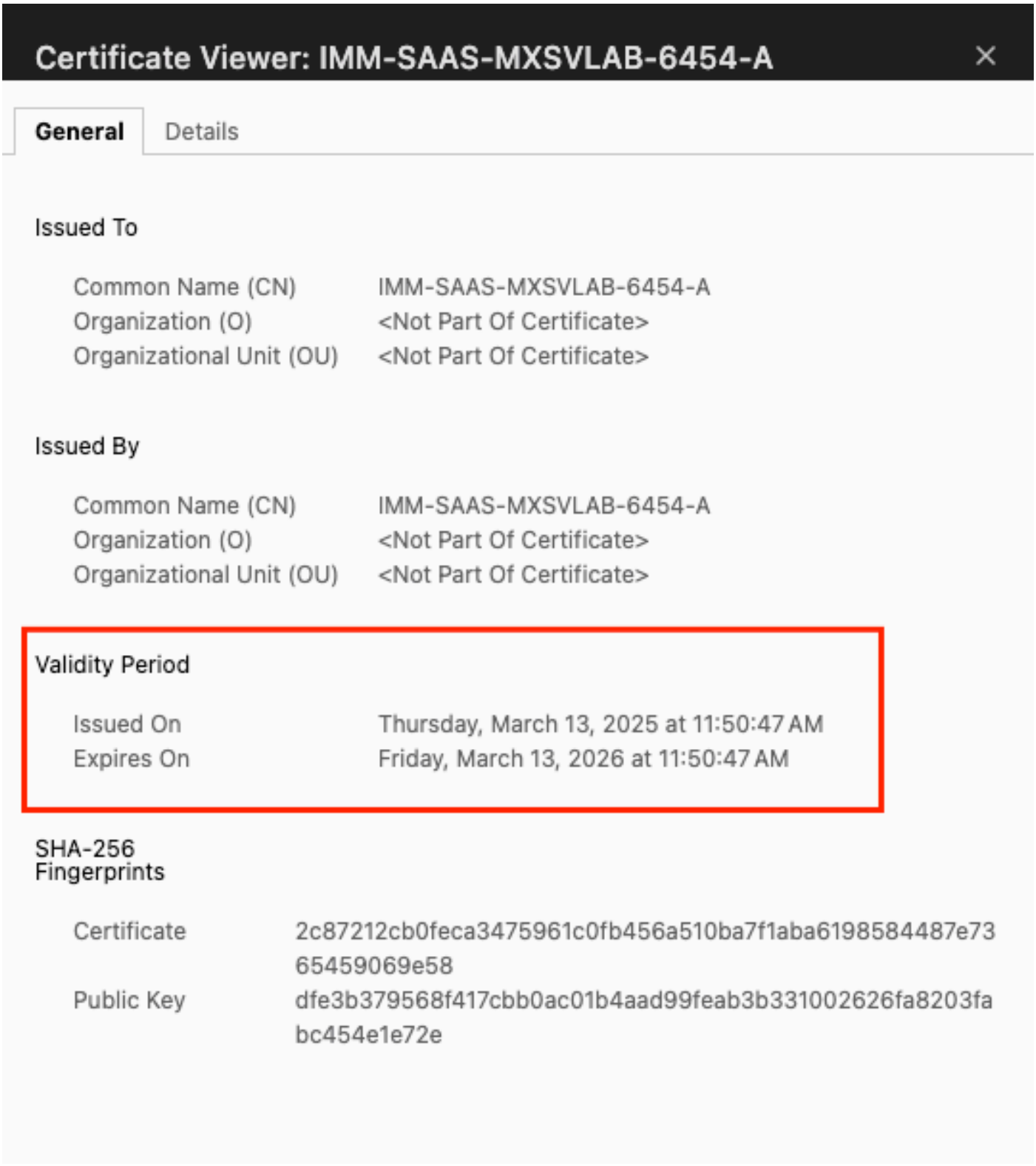
```
UCS# show self-signed-certificate
```

Example output:

```
-----BEGIN CERTIFICATE-----
MIIC+DCCAeCgAwIBAgICBnowDQYJKoZIhvcNAQELBQAwIjEgMB4GA1UEAxMXSU1N
LVNBQVMtTVhTVkxBQi02NDU0LUEwHhcNMjUwMzEyMjI1MTM4WhcNMjYwMzEyMjI1
MTM4WjAiMSAwHgYDVQQDExdJTU0tU0FBUy1NWFNWTEFCLTY0NTQtQTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAK+Q9oAU2rHxtV5stg9vfCeKQ+9+n5Ke
oz6IKOeEDufeRcBYepaJlEhffvdLp/uOh/NnyphT4mVLiJxh6dTTIhW58G8LaGNV
hIRtNAX984eLCs1nSG3o3tzJ3+e5tO4G6klAcj43HiKY+oRCEs+oiUsQlYpBjHoy
FGxMT8wpnNMIg59mKVTuUeC4r6ACnyy1CRNp8qD8Rf4lIBU/jTI/jPdzE2//9rAo
G85qhZ46vIOdLu1jv/ySszQkATFA15KHFETnyTkptdlJH8mcO33edJ1Xq9plebMp
dtn18zj+2qxQq8ErZ6doFdkOuyuq3N6Q0dbfdefKKuiFvkCGv4GwRG8CAwEAAaM4
MDYwDgYDVR0PAQH/BAQDAgKkMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA8GA1UdEQQI
MAaHBH8AAAEwDQYJKoZIhvcNAQELBQADggEBAFn+v4ehwLFi/mcHWA4ld03JBkvI
RIlbFPHjOykzmAN8E1XoJlLciCxA3gHUzPP6lT+2VpeAXAoWzIlgUlm2GwPzZbCQ
nz2v7NpGHchaXAEi756IMmCm2IJ2jOuS9p9v3AAX3gLUp43SeCQN+C2nNOcZgmZr
/K1CoNkIUXdVI8nxEDCMFPezL1SXdNa2c4AB699teolCNc65tnnNDjsxkLkL7bTx
P5euETVi5CizQQpjcZzXEMHv3XdvXtkzyAATjRmvUS8lxyXxiisMjMl7f8zXkLnG
n7ZKR746BXgXufmSOzITtbpvgI9+6PnauoWOh3EH7rGmJyZnn5L62/oaoy4=
-----END CERTIFICATE-----
```

Note: If you check the certificate before renewal, ensure that it changes after the renewal process.

Finally, the certificate should look like this:



Certificate Validation

Related Information

[Certificates in Intersight Virtual Appliance](#)