Upgrading Cisco IMC Supervisor From Older Versions

This chapter contains the following topics:

Upgrading to Cisco IMC Supervisor Version 2.2

To upgrade to Cisco IMC Supervisor 2.2, deploy either through VMware vSphere or Micrsoft Hyper -V and follow the upgrade path below to migrate data from the old system to the new system.

- From Release 2.2(1.3) to Release 2.2 (1.4)
- From Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.2(1.1) to Release 2.2(1.4)
- From Release 2.2(1.0) to Release 2.2(1.4)
- From Release 2.2(0.6) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.2(0.5) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.2(0.4) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.2(0.2) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.1.x.x to Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.1.x.x to Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4)

Digitally Signed Images

Cisco IMC Supervisor release 2.2(1.2) images are delivered in digitally signed zip files. These signed zip files are wrapped in a container zip file that includes the following:

- Digitally signed zip file—Contains the Cisco IMC Supervisor installation or upgrade image
- Verification program—Verifies the certificate chain and signature. During certificate chain validation, the program verifies the authenticity of the end-entity certificate using Cisco's SubCA and root CA certificates. Then, the authenticated end-entity certificate is used to verify the signature.
- Digital signature file—Contains the signature that you can verify before installation or upgrade.
- Certificate file—Enables you to verify the digital signature. This Cisco-signed x.509 end-entity certificate contains a public key that can be used to verify the signature. This certificate is chained to the Cisco root posted on http://www.cisco.com/security/pki/certs/crcam2.cer.
- ReadMe file—Provides the information and instructions required to verify the digitally signed zip file.

Verify the image offline. Once the image is verified, you can begin the installation or upgrade of Cisco IMC Supervisor.

Requirements for Verifying Digitally Signed Images

Before you verify a Cisco IMC Supervisor digitally signed image, ensure that you have the following on your local machine:

- Connectivity to https://www.cisco.com during the verification process.
- Python 3.6.8
- OpenSSL

Verifying a Digitally Signed Image

Before you begin

Download the Cisco IMC Supervisor image from Cisco.com.

Procedure

Step 1 Unzip the file you downloaded from Cisco.com and verify that it contains the following files:

- ReadMe file
- Digitally signed zip file.
- Certificate file, for example `UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer`
- Digital signature generated for the image.

- Signature verification program, for example `cisco_x509_verify_release.py3`

Step 2 Review the instructions in the ReadMe file.

Note If there are any differences between these instructions and those in the ReadMe, follow the ones in the ReadMe.

Step 3 Run the signature verification program from the directory where you have unzipped the downloaded content.

Example: Signature Verification for Upgrade Patch

```
python3 ./cisco_x509_verify_release.py3 -e UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
-i cimcs_patch_2_3_2_0_67198.zip -s cimcs_patch_2_3_2_0_67198.zip.signature -v dgst -sha512
```

Step 4 Review the output and ensure that the verification has succeeded.

Example: Expected Output for Upgrade

```
Downloading CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully downloaded and verified crcam2.cer.
Downloading SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer
...
Successfully downloaded and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully verified the signature of cimcs_patch_2_3_2_0_67198.zip using
UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
```