



Boot Integrity Visibility

- [Information About Boot Integrity Visibility, on page 1](#)
- [Verifying the Software Image and Hardware, on page 2](#)
- [Verifying Platform Identity and Software Integrity, on page 3](#)
- [Verifying Image Signing, on page 6](#)
- [Additional References for Boot Integrity Visibility, on page 7](#)
- [Feature History for Boot Integrity Visibility, on page 7](#)

Information About Boot Integrity Visibility

Boot Integrity Visibility allows Cisco's platform identity and software integrity information to be visible and actionable. Platform identity provides the platform's manufacturing installed identity. Software integrity exposes boot integrity measurements that can be used to assess whether the platform has booted trusted code.

During the boot process, the software creates a checksum record of each stage of the bootloader activities.

You can retrieve this record and compare it with a Cisco-certified record to verify if your software image is genuine. If the checksum values do not match, you may be running a software image that is either not certified by Cisco or has been altered by an unauthorized party.

Image Signing and Bootup

The Cisco build servers generate the Cisco IOS XE images. Cisco IOS XE images use the Abraxas image signing system to sign these images securely with the Cisco private RSA keys.

When you copy the Cisco IOS XE image onto a Catalyst 9000 Series Switch, Cisco's ROMMON Boot ROM verifies the image using Cisco release keys. These keys are public keys that correspond to the Cisco release private key that is stored securely on the Abraxas servers. The release key is stored in the ROMMON.

Catalyst 9000 Series Switches support boot integrity visibility feature. Boot integrity visibility serves as a hardware trust anchor which validates the ROMMON software to ensure that the ROMMON software is not tampered with.

The Cisco IOS XE image is digitally signed during the build time. An SHA-512 hash is generated over the entire binary image file, and then the hash is encrypted with a Cisco RSA 2048-bit private key. The ROMMON verifies the signature using the Cisco public key. If the software is not generated by a Cisco build system, the signature verification fails. The device ROMMON rejects the image and stops booting. If the signature verification is successfully, the device boots the image to the Cisco IOS XE runtime environment.

The ROMMON follows these steps when it verifies a signed Cisco IOS XE image during the bootup:

1. Loads the Cisco IOS XE image into the CPU memory.
2. Examines the Cisco IOS XE package header.
3. Runs a non-secure integrity check on the image to ensure that there is no unintentional file corruption from the disk or TFTP. This is performed using a non-secure SHA-1 hash.
4. Copies the Cisco's RSA 2048-bit public release key from the ROMMON storage and validates that the Cisco's RSA 2048-bit public release key is not tampered.
5. Extracts the Code Signing signature (SHA-512 hash) from the package header and verifies it using Cisco's RSA 2048-bit public release key.
6. Performs the Code Signing validation by calculating the SHA-512 hash of the Cisco IOS XE package and compares it with the Code Signing signature. The Signed package is now validated.
7. Examines the Cisco IOS XE package header to validate the platform type and CPU architecture for compatibility.
8. Extracts the Cisco IOS XE software from the Cisco IOS XE package and boots it.



Note In above process, step 3 is a non-secure check of the image which is intended to confirm the image against inadvertent corruption due to disk errors, file transfer errors, or copying errors. This is not part of the image code signing. This check is not intended to detect deliberate image tampering.

Image Code Signing validation occurs in step 4, 5, and 6. This is a secure code signing check of the image using an SHA-512 hash that is encrypted with a 2048-bit RSA key. This check is intended to detect deliberate image tampering.

Verifying the Software Image and Hardware

This task describes how to retrieve the checksum record that was created during a switch bootup. Enter the following commands in privileged EXEC mode.



Note On executing the following commands, you might see the message **% Please Try After Few Seconds** displayed on the CLI. This does not indicate a CLI failure, but indicates setting up of underlying infrastructure required to get the required output. We recommend waiting for a few minutes and then try the command again.

The messages **% Error retrieving SUDI certificate** and **% Error retrieving integrity data** signify a real CLI failure.

Procedure

	Command or Action	Purpose
Step 1	<code>show platform sudi certificate [sign [nonce nonce]]</code>	Displays checksum record for the specific SUDI.

	Command or Action	Purpose
	<p>Example:</p> <pre>Device# show platform sudi certificate sign nonce 123</pre>	<ul style="list-style-type: none"> • (Optional) sign - Show signature • (Optional) nonce - Enter a nonce value
Step 2	<p>show platform integrity [sign [nonce nonce]]</p> <p>Example:</p> <pre>Device# show platform integrity sign nonce 123</pre>	<p>Displays checksum record for boot stages.</p> <ul style="list-style-type: none"> • (Optional) sign - Show signature • (Optional) nonce - Enter a nonce value

Verifying Platform Identity and Software Integrity

Verifying Platform Identity

The following example displays the Secure Unique Device Identity (SUDI) chain in PEM format. Encoded into the SUDI is the Product ID and Serial Number of each individual device such that the device can be uniquely identified on a network of thousands of devices. The first certificate is the Cisco Root CA 2048 and the second is the Cisco subordinate CA (ACT2 SUDI CA). Both certificates can be verified to match those published on <https://www.cisco.com/security/pki/>. The third is the SUDI certificate.

```
Device# show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiuGAWIBAgIQX/h7KctU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDwNDGwHhcNMjQwNTE0MjAxNzEyWncNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDwNDGwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmmrmp68Kd6f1cba0ZmkUeIhH
xmJVhEAYv8CrLqUccda8bnuoqrpu0hWISewdovyD0My5j0AmaHBKeN8hF570YXJ
FcyjPfto1YYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JhcJ6r8qqB9q
VvYgDxFU14F1pyXOWWqCZe+36ufijXWLBvLdT6ZeYpzPEApk0E5tzivMW/VgpdH
jWn0f84bcN5wGyDws2mAg8EtKpP6BrXruOIIt6ke01a06g58QBdKhTcyTKmg9l
Eg6CTy5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LTLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAAQh/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFbi71R803UXHOjgXkhLtv5MOhmBvrbW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe61JT37mjpXYgyC81WhJdTsD9i7rp77rMKSsH0T81asZ
Bvt9YaretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe00caEblfJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hs27PKSb3TkL4Eq1ZKR4OCXPDJoBYVVL0fdX41Id
kxpUnwVwEpxYB5DC2Ae/qPOgrnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAWIBAgIKYQ1ufQAAAAAADANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDwNDGw
HhcNMTEwNjMwMTc1NjU3WncNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDAxNj
bzEVMBMGA1UEAxMMQUNUMiBTvURJIENBMBIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAOm5l3THiXA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHkD477AkS
5XAtUs5oxDYvt/zEbs1Zq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYzo3qPCpxzprWJDPc1M4iYKHUMQMqmgmg+
xghHIOoWS80BOcdiyEbeP5rZ7qRuewKmpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXDgJ13oVeF+EyFwLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sX1XtEOjSXJ
```

```

URsyMEj53Rdd9tJwHky8neapszS+r+kdvQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GAlUdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVhm6aAgkWrSugiWbf2nsvqjBDBGNVHR8EPDA6MDigNgA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cm10eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNH0dHA6Ly93d3cuY2l2Y28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEAAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2l2Y28uY29tL3NlY3VyXR5
L3BraS9wb2xpY2llcy9pbmRleC50dG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIHvcNAQEFBQADggEBAGh1qc1r9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcC10lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dwlex+7amATUQ04QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOwryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hy147d7cZR4DY4LIuFM2P1As8YjzozNpK/urSRI14WdIlp1r1nH7KND15618yFVP
0IFZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=

```

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

```

MIIDgTCCAmmgAwIBAgIEAp4UYzANBgkqhkiG9w0BAQsFADANMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGAlUEAxMMQUNUMiBTvURJIENBMB4XDTE4MDYwNTAzNDUwNV0xDTI5
MDUxNDIwMjU0MVowbTEpMCCGAlUEBRMgUe1EOkM5MjAwTC0yNFQtNEcgU0046S1BH
MjIwMjAwQWQgTgxdjAMBGNVBAoTBUNpc2NvMRgwFgYDVQQLew9BQ1Q1tMiBMAXRlIFNV
REkxZjAUBG9NVBAMTDUM5MjAwTC0yNFQtNEcgwGgEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDBm2Dg0GwQ18wLTKxeCt87DL8K1Rbx8Db1IigHjzebBXMpx7Ja
6Cp+kwRrIWGi5AmNmV7jZ2ZLj+vFVzBQ9eGM+6LdNg18c6nqmSmnuXMerD1UEMMK
bkFl4ydn1EIMoWpCARbgz+/zaLM2A5bpQXVndiKq1v0NA2Pgvqdxbm+8AELdDG/D
3SQ1anOja+yH5vu3NjyMjftjzkn/ILp9iZMwzcA+06E8KC5FclR2cfvWlQvoFM
ZEWmHdhHptsnN+4hhdDeurgeM0S+xIvzZq0H7PxS0kt4vYQ9xWQEWavJAL44k0uY
JxKP6bDNssSLZ2s4/2OBsODjyBhb0GwrOAHdAgMBAAGjBzBtMA4GAlUdDWEB/wQE
AwIF4DAMBGNVHRMBAf8EAJAAME0GAlUdEQRGMESgQgYJKwYBBAEFJFQIDoDUTM0No
aXBjRD1RRGx6T0FZUHqWRTJJRVFFQUFjQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
PTANBgkqhkiG9w0BAQsFAAOCAQEAgLUxZfnMrXZ6ZMGX69dDPkmpv9cFqXR538LF
PdypCRuSk20GF8OeDU0suTi4mbB87JSOWvLomdBtXdnxzRu4kP2NFz/7pjAVRT3R
gwMMyiEnDwQsvy7e4S2myVgej55e3hTW/LTeU81CE0KR0yGDce5Phv2zdHtIsXrV
XsY+Propfntt1FV9qqDsKdWcKf0bos6VsYwUpSCEGqF7LfnNBTkYvXUUmKXHKf/d
W5HgrYt6bQ/h/+0EP+MY2wpAiWMCfX6F+xW20vzfK8NzNesieB38IvuTkgefzh2s
yGCOavAxxGd0j7atcRpdRjT9+KM9Vwuy4VJZgK/tlfmTL4cawQ==

```

-----END CERTIFICATE-----

Signature version: 1

Signature:

```

-----BEGIN RSA SIGNATURE-----
MIIDgTCCAmmgAwIBAgIEAp4UYzANBgkqhkiG9w0BAQsFADANMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGAlUEAxMMQUNUMiBTvURJIENBMB4XDTE4MDYwNTAzNDUwNV0xDTI5
MDUxNDIwMjU0MVowbTEpMCCGAlUEBRMgUe1EOkM5MjAwTC0yNFQtNEcgU0046S1BH
MjIwMjAwQWQgTgxdjAMBGNVBAoTBUNpc2NvMRgwFgYDVQQLew9BQ1Q1tMiBMAXRlIFNV
REkxZjAUBG9NVBAMTDUM5MjAwTC0yNFQtNEcgwGgEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDBm2Dg0GwQ18wLTKxeCt87DL8K1Rbx8Db1IigHjzebBXMpx7Ja
6Cp+kwRrIWGi5AmNmV7jZ2ZLj+vFVzBQ9eGM+6LdNg18c6nqmSmnuXMerD1UEMMK
bkFl4ydn1EIMoWpCARbgz+/zaLM2A5bpQXVndiKq1v0NA2Pgvqdxbm+8AELdDG/D
3SQ1anOja+yH5vu3NjyMjftjzkn/ILp9iZMwzcA+06E8KC5FclR2cfvWlQvoFM
ZEWmHdhHptsnN+4hhdDeurgeM0S+xIvzZq0H7PxS0kt4vYQ9xWQEWavJAL44k0uY
JxKP6bDNssSLZ2s4/2OBsODjyBhb0GwrOAHdAgMBAAGjBzBtMA4GAlUdDWEB/wQE
AwIF4DAMBGNVHRMBAf8EAJAAME0GAlUdEQRGMESgQgYJKwYBBAEFJFQIDoDUTM0No
aXBjRD1RRGx6T0FZUHqWRTJJRVFFQUFjQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
PTANBgkqhkiG9w0BAQsFAAOCAQEAgLUxZfnMrXZ6ZMGX69dDPkmpv9cFqXR538LF
PdypCRuSk20GF8OeDU0suTi4mbB87JSOWvLomdBtXdnxzRu4kP2NFz/7pjAVRT3R
gwMMyiEnDwQsvy7e4S2myVgej55e3hTW/LTeU81CE0KR0yGDce5Phv2zdHtIsXrV
XsY+Propfntt1FV9qqDsKdWcKf0bos6VsYwUpSCEGqF7LfnNBTkYvXUUmKXHKf/d
W5HgrYt6bQ/h/+0EP+MY2wpAiWMCfX6F+xW20vzfK8NzNesieB38IvuTkgefzh2s
yGCOavAxxGd0j7atcRpdRjT9+KM9Vwuy4VJZgK/tlfmTL4cawQ==
-----END RSA SIGNATURE-----

```

The optional RSA 2048 signature is across the three certificates, the signature version and the user-provided nonce.

```

RSA PKCS#1v1.5 Sign {<Nonce (UINT64)> || <Signature Version (UINT32)> || <Cisco Root CA
2048 cert (DER)> ||
<Cisco subordinate CA (DER)> || <SUDI certificate (DER)> }

```

Cisco management solutions are equipped with the ability to interpret the above output. However, a simple script using OpenSSL commands can also be used to display the identity of the platform and to verify the signature, thereby ensuring its Cisco unique device identity.

```

[linux-host:~]openssl x509 -in sudicert.pem -subject -noout
subject= /serialNumber=PID:C9200L-24T-4G SN:FDO1946BG05/O=Cisco/OU=ACT-2 Lite
SUDI/CN=C9200L-24T-4G

```

Verifying Software Integrity

The following example displays the checksum record for the boot stages. The hash measurements are displayed for each of the three stages of software successively booted. These hashes can be compared against


```

cat9k_lite-rpbase.16.10.01.SPA.pkg :
D0D155C1DEFB03EB064057AD6A9673E2114FA7CCAA7EDAE935CB0B84E0DD155C1DEFB03EB064057AD6A9673E2114FA7CCAA7EDAE935CB0B84E0
cat9k_lite-rpboot.16.10.01.SPA.pkg :
AD6A9673E2114FA7CCAA7EDAE935CB0B84E0DD155C1DEFB03EB064057AD6A9673E2114FA7CCAA7EDAE935CB0B84E0DD155C1DEFB03EB064057
cat9k_lite-srdriver.16.10.01.SPA.pkg :
4FA7CCAA7EDAE935CB0B84E0DD155C1DEFB03EB064057AD6A9673E2114FA7CCAA7EDAE935CB0B84E0DD155C1DEFB03EB064057AD6A9673E211
cat9k_lite-webui.16.10.01.SPA.pkg :
CCAA7EDAE935CB0B84E0DD155C1DEFB03EB064057AD6A9673E2114FA7CCAA7EDAE935CB0B84E0DD155C1DEFB03EB064057AD6A9673E2114FA7
cat9k-wlc.16.10.01.SPA.pkg :
AA7EDAE935CB0B84E0DD155C1DEFB03EB064057AD6A9673E2114FA7CCAA7EDAE935CB0B84E0DD155C1DEFB03EB064057AD6A9673E2114FA7CCA
PCR0: 750E5D2EDAE6E3A68050638E0BFD8619BE4EA13066025D39DF79408719F5177E
PCR8: EB6E739A63F53E703B6CDAF3F6188833CEF6D32E2F726006B9AA34E1E73048C4
Signature version: 1
Signature:

```

Verifying Image Signing

The following example displays the secure code signing check of the image during bootup using an SHA-512 hash.

```

switch:boot flash:packages.conf
boot: attempting to boot from [flash:packages.conf]
boot: reading file packages.conf
#
Performing Integrity Check ...
boot: parsed image from conf file: cat9k-rpboot.17.02.01.SSA.pkg

```

Loading image in Verbose mode: 1

```

Image Base is: 0x100099000
Image Size is: 0x2C83487
Package header rev 3 structure detected
Package type:30001, flags:0x0
IsoSize = 0
Parsing package TLV info:
000: 0000000900000001D4B45595F544C565F - KEY_TLV_
010: 5041434B4147455F434F4D5041544942 - PACKAGE_COMPATIB
020: 494C495459000000000000090000000B - ILITY
030: 4652555F52505F545950450000000009 - FRU_RP_TYPE
040: 000000184B45595F544C565F5041434B - KEY_TLV_PACK
050: 4147455F424F4F544152434800000009 - AGE_BOOTARCH
060: 0000000E415243485F693638365F5459 - ARCH_i686_TY
070: 5045000000000009000000144B45595F - PE KEY_
080: 544C565F424F4152445F434F4D504154 - TLV_BOARD_COMPAT
090: 0000000900000010424F4152445F6361 - BOARD_ca
0A0: 74396B5F545950450000000900000018 - t9k_TYPE
0B0: 4B45595F544C565F43525950544F5F4B - KEY_TLV_CRYPTOK
0C0: 4559535452494E470000000900000004 - EYSTRING

```

```

TLV: T=9, L=29, V=KEY_TLV_PACKAGE_COMPATIBILITY
TLV: T=9, L=11, V=FRU_RP_TYPE

```

```

TLV: T=9, L=24, V=KEY_TLV_PACKAGE_BOOTARCH
TLV: T=9, L=14, V=ARCH_i686_TYPE
TLV: T=9, L=20, V=KEY_TLV_BOARD_COMPAT
TLV: T=9, L=16, V=BOARD_cat9k_TYPE
TLV: T=9, L=24, V=KEY_TLV_CRYPTO_KEYSTRING
TLV: T=9, L=4, V=none
TLV: T=9, L=11, V=CW_BEGIN=$$
TLV: T=9, L=17, V=CW_FAMILY=$cat9k$
TLV: T=9, L=74, V=CW_IMAGE=$cat9k-rpboot.17.02.01.SSA.pkg$
TLV: T=9, L=20, V=CW_VERSION=$17.2.01$
IOS version is 17.2.1
TLV: T=9, L=53, V=CW_FULL_VERSION=$17.2.01.0.869.1580816579..Amsterdam$
TLV: T=9, L=52, V=CW_DESCRIPTION=$Cisco IOS Software, IOS-XE Software$
TLV: T=9, L=9, V=CW_END=$$
Found DIGISIGN TLV type 12 length = 392
RSA Self Test Passed

Expected hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F

Obtained hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F
Sha512 Self Test Passed
Found package arch type ARCH_i686_TYPE
Found package FRU type FRU_RP_TYPE
Performing Integrity Check ...

RSA Signed DEVELOPMENT Image Signature Verification Successful.
    
```

Additional References for Boot Integrity Visibility

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	<i>Command Reference (Catalyst 9200 Series Switches)</i>

Feature History for Boot Integrity Visibility

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Fuji 16.9.2	Boot Integrity Visibility	Boot Integrity Visibility allows Cisco's platform identity and software integrity information to be visible and actionable. Platform identity provides the platform's manufacturing installed identity.
Cisco IOS XE Cupertino 17.9.1	Boot Integrity Visibility	This feature was implemented on C9200CX-12P-2X2G, C9200CX-8P-2X2G, and C9200CX-12T-2X2G models of the Cisco Catalyst 9200CX Series Switches, which were introduced in this release.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.