



Boot Integrity Visibility

- [Information About Boot Integrity Visibility, on page 1](#)
- [Verifying the Software Image and Hardware, on page 1](#)
- [Verifying Platform Identity and Software Integrity, on page 2](#)
- [Additional References for Boot Integrity Visibility, on page 5](#)
- [Feature History for Boot Integrity Visibility, on page 5](#)

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.

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	show platform sudi certificate [sign [nonce]] Example: Device# show platform sudi certificate sign nonce 123	Displays checksum record for the specific SUDI. <ul style="list-style-type: none"> • (Optional) sign - Show signature • (Optional) nonce - Enter a nonce value
Step 2	show platform integrity [sign [nonce]] Example: Device# show platform integrity sign nonce 123	Displays checksum record for boot stages. <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
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRywFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaxNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwrmrmp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOamaHBKeN8hF570YQXJ
FcjPfto1YYmUQ6iEqDGYeJu5Tm8sUxJsZR2tKys7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFU14FlpyXOWWqCZe+36ufijXWLBvLdT6ZeYpzPEApk0E5tziVMW/VgpSdh
jWn0f84bcn5wGyDwbs2mAag8EtKpP6BrXruOIIt6ke01a06g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBc11HP7R2RQgYcUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlqX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwdQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFbi71R803UXHOjgkxkLtv5MOhmBvrbW7hmW
Yqpao2TB9k5UM8Z3/sUcuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJdTsD9i7rp77rMKSsH0T8lasz
Bvt9YaretIpsjYp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEbfJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hs27PKSb3TkL4Eq1ZKR4OCXPDJJoBYVL0fdX41Id
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPCCAySgAWIBAgIKYQlufQAAAAAADANBgkqhkiG9w0BAQUFADA1MRywFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaxNjbyBSb290IENBIDIwNDgw
HhcNMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDAxNj
```

```

bzEVMBMGA1UEAxMMQUNUMiBTvURJiENBmIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAOm5l3THixA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYvt/zEbs1Zq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPUx+a6tHF/gRuOiJ44mdeDYzo3qPCpxzprWJDPclM4iYKHUMQMqmgmg+
xghHIOoWS80BOcdiynEbeP5rZ7qRuewKmpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdgJ13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sX1XtEOjSXJ
URyMEj53Rdd9tJwHky8neapszS+r+kdvQIDAQABo4IBWjCCAVYwCwYDVROPAQAQD
AgHGMB0GA1UdDgQWBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHM6aAgkWrSugiWbf2nsvqjBDBgNVHR8EPDA6MDIqNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZW50cm10eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNgh0dHA6Ly93d3cuY2l2Y28uY29tL3N1Y3Vy
aXR5L3BraS9jZXJ0cy9jcmNmMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEAAQKV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2l2Y28uY29tL3N1Y3VyYXR5
L3BraS9wb2xpY2l1cy9pbmRleC5odG1sMBIGAlUdEwEB/wQIMAYBAf8CAQAQDQYJ
KoZlThvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbmSjbi
ZHc/CcC101Ju0a9zTXA9w47H9/t61eduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQ04QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOwryAK4dVo8hcKjkEku3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKN
hy147d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdI1plR1nH7KND15618yFVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgIEAUODPjANBgkqhkiG9w0BAQsFADANMQ4wDAYDVQQKEwVD
aXNjbjEVMbMGA1UEAxMMQUNUMiBTvURJiENBmB4XDTE3MDExMDE2NDUyOVV0XDTI3
MDExMDE2NDUyOVV0YyTEjMCEGAlUEBRMaUElEOLdTLVhTVVAgU046SkFFMjA1MDA3
MzAxZjAMBgNVBAoTBUNpc2NvMRgwFgYDVQQLew9BQ1QtmIbMaXRlIFNVREkxEDAO
BgNVBAMTb1dTLVhTVVAgwEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDH
gbjvf7kfaYRtHwLCoLWS0Cb/eXXJlxZ1ardp4EwXq0QaGhBES8B4oMPdZkPob/e4
TGy4f9qMrr9wDXikDh0hw10Cuf2Towm201RILHkftD1k9joWH+0oQKkU/rTQ/6n
tMOelSRNFaL0LPC9msNTSX4Gtdud+u9YQMN561SG/w0D2ywo9f08T+cAb3xUqkx
BDhcApdBWXNGdRWFJRaoSfoSUD8U7/hJxmThYOZz5Mkm8d2cuF2qgVTvvsx94rIA
dXH6881L85EkdG0rMrOCxtblytdo4MfEDwIxxGG0+Dx/HABuo8Gr/tYvzanPos8pz
dgCW0/LX85uB8WxR8HfjAgMBAAGjBzBtMA4GA1UdDwEB/wQEAwIF4DAMBgNVHRMB
Af8EAjAAME0GA1UdEQRMESgQgYJKwYBBAEJFQIDoDUTM0NoaXBJRD1VWUpOVTFj
eUNRR2NWSFZsSUU5amRDQX10eUF4T0RveE1Ub3hPU0FVVVhNPTANBgkqhkiG9w0B
AQsFAAOCAQEAAu6FDk+d1ubG6g+WyhKHHhuwu3U8730ieh0QfODYe7Ew5RmA2b8BE
o5vD7TDjUGOXgKEkw71anfrSQIPVQhasnGGseLMC1pdxiq8Zw77j9c1rU1xLiZ
vMqMChSmYhR1G41tHkpzrsD8dFJohg+AwBQwLmyplmYidW9hojiwoVp+3CV2674I
WAQDi7rbqdhMHQz+Lkbsnjsebl/6gkFSH3UEVGC0HEIhE6uEEH2V3Z0jfkPzWQH
y39DnXwNSgRIilFQMia11+i6CmkC4uyHRDYm7tDxxeDqxdALSHefFwPgrIuuQSj0
UdQ5vdQXm0ao7DCw5dv0mCA9stGQUS1MWw==
-----END CERTIFICATE-----

```

Signature version: 1
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:WS-XC7R SN:FDO1946BG05/O=Cisco/OU=ACT-2 Lite SUDI/CN=WS-XC7R

```

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 Cisco-provided reference values. An option to sign the output gives a verifier the ability to ensure the output is genuine and is not altered. A nonce can be provided to protect against replay attacks.



Note Boot integrity hashes are not MD5 hashes. For example, if you run `verify /md5 cat9k_iosxe.16.10.01.SPA.bin` command for the bundle file, the hash will not match.

The following is a sample output of the `show platform integrity sign nonce 123` command in install mode. This output includes measurements of each installed package file.

```
Device# show platform integrity sign nonce 123
Platform: WS-XC7R
Boot 0 Version: MA1004R06.1604052017
Boot 0 Hash: A99EF9F31CE3F3F8533055407F1C88C62176E667E4E1DA0649EAA7A1282F205E0A
Boot Loader Version: System Bootstrap, Version 16.8.0.7, DEVELOPMENT SOFTWARE
Boot Loader Hash:
942C2511D0EB10C8F5EC8E3ED529A5F2D210C4154434C6A591BF5553B06CBBE2039DADD949C05722CABBE1429C41737CFC2C593A814FC87F6FBA0E9A0ADB09B
OS Version: 16.10.01
OS Hashes:
cat9k-cc_srdriver.16.10.01.SPA.pkg :
D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0
cat9k-espbases.16.10.01.SPA.pkg :
3EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEF43
cat9k-guestshell.16.10.01.SPA.pkg :
B0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03E
cat9k-rpbases.16.10.01.SPA.pkg :
4057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C6
cat9k-rpboot.16.10.01.SPA.pkg :
AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057
cat9k-sipbases.16.10.01.SPA.pkg :
9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A
cat9k-sipspas.16.10.01.SPA.pkg :
E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673
cat9k-srdriver.16.10.01.SPA.pkg :
4FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E211
cat9k-webui.16.10.01.SPA.pkg :
CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7
cat9k-wlc.16.10.01.SPA.pkg :
AA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAA
PCR0: A32CFED4F960494BC1311F7A31B52D5DE90FF501932670CD43AE6DBAD8735052
PCR8: D2F8474CD82072464C11D7F7A3D5C37D078A8AA832D94B1B12E01BF400E0BBB4
Signature version: 1
Signature:
A32CFED4F960494BC1311F7A31B52D5DE90FF501932670CD43AE6DBAD8735052
D2F8474CD82072464C11D7F7A3D5C37D078A8AA832D94B1B12E01BF400E0BBB4
A32CFED4F960494BC1311F7A31B52D5DE90FF501932670CD43AE6DBAD8735052
D2F8474CD82072464C11D7F7A3D5C37D078A8AA832D94B1B12E01BF400E0BBB4
```

The following is a sample output of the `show platform integrity sign nonce 123` command in bundle mode. This output includes measurements of the bundle file and each installed package.

```
Device# show platform integrity sign nonce 123
Platform: WS-XC7R
Boot 0 Version: MA1004R06.1604052017
Boot 0 Hash: A99EF9F31CE3F3F8533055407F1C88C62176E667E4E1DA0649EAA7A1282F205E0A
Boot Loader Version: System Bootstrap, Version 16.8.0.7, DEVELOPMENT SOFTWARE
Boot Loader Hash:
942C2511D0EB10C8F5EC8E3ED529A5F2D210C4154434C6A591BF5553B06CBBE2039DADD949C05722CABBE1429C41737CFC2C593A814FC87F6FBA0E9A0ADB09B
OS Version: 16.10.01
```


Release	Feature	Feature Information
Cisco IOS XE Fuji 16.8.1a	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. Support for this feature was introduced only on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models of the Cisco Catalyst 9500 Series Switches.
Cisco IOS XE Fuji 16.9.1	Boot Integrity Visibility	Support for this feature was introduced only on the C9500-32C, C9500-32QC, C9500-48Y4C, and C9500-24Y4C models of the Cisco Catalyst 9500 Series Switches.

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>.