



Boot Integrity Visibility

- [Overview of Boot Integrity Visibility, on page 1](#)
- [Verifying Software Image and Hardware, on page 1](#)
- [Verifying Platform Identity and Software Integrity, on page 2](#)

Overview of Boot Integrity Visibility

Boot Integrity Visibility allows the Cisco 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 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
	Example: Device# show platform sudi certificate sign nonce 123	<ul style="list-style-type: none"> • (Optional) sign - Show signature. • (Optional) nonce - Enter a nonce value.
Step 2	show platform integrity [sign [nonce 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.



Important All the CLI outputs provided here are intended only for reference. The output differs based on the configuration of the device.

```
Device# show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KctU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRSwGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRSwGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAYv8CrLqUccda8bnuoqrpu0hWISEwdovyD0My5jOAmAHBKeN8hF570YQXJ
FcjPFto1YmUQ6iEqdGYeJu5Tm8sUxJsZr2tKys7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFU14F1pyXOWWQCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMM/VgPsdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6ke01a06g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdFHbBc11HP7R2RQgYCUtOG/rksc35LtLgXfAgED
o1EwtzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBI71R803UXHOjgkxhLtv5M0hmBvRbW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpxYgyC81WhJDtSd9i7rp77rMKsSH0T8lasz
Bvt9YArEtIpsjYp8qS5UwGH0GikJ3+r/+n6yUA4iGe00caEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPJDJoBYVL0fdX41Id
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPCCAySgAwIBAgIKYQlufQAAAAAADANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRSwGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTcwNjMwMTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEw1DaXNj
bzEvMVBMBG1UEA/MMQUNUMiBTVURJIENBMTIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAM5l3THIx9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYvt/zEbs1Zq3+LR6qrqKQVv6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuoiJ44medDYz03qPCpxzprWJDPc1M4iYKHUMQMqmgmg+
```

```
xghHiooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sX1XtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWbf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZW50cm10eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNgh0dHA6Ly93d3cuY2l2Y28uY29tL3N1Y3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZlIwXAYDVR0GgBFUwUzBRBgorBgEAAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2l2Y28uY29tL3N1Y3VyXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwdQYJ
KoZlIhvcNAQEFBQADggEBAGhlqclr9tx4hzWgDERm37lyeuEmqcIfi9b9+GbmSjbi
ZHc/CcC10lJu0a9zTXA9w47H9/t61eduGxb4WeLxcwCiUgvFtCa51Iklt8NbcKY
/4dwllex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEzku3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2PlAs8YyjoNpK/urSRI14WdIlplRlnH7KND15618yFVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIEAwQD7zANBgkqhkiG9w0BAQsFADANMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGA1UEAxMMQUNUMiBTVURJENBMB4XDTE4MDk5MzIyMjYwMDUxMDUx
MDUxNDIwMjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0
MzZMMFESMjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0
MRQwEgYDQVQDEwTODOTYwMCI1TVVATMTCCASlWdQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBANsh0jcvgh1pd0jP9KnfDnDc/zEHDzbcTWPJi2FZcsaSE5jvq6CUBQc4
MYpNAZU2Jym7NSD8iQbMXwnCtoL64QtXQeFhRymc4d5o933M7GwpEH0I7HUSbO/
Fxy7JbMGPgAkY7rKsYENiNK2hiR7Q2O7X2BidOKknEuofWdJMNyMaZgLYLOHbJ
5oXaORxhUy3VRaxN16qI7kYxuugg2LcAbZ539sRXe8JtHyK811URNsGmiQ0S17pS
idGmrJJ0pEHA0EUVTZqEny3z+NW9uxLVSzu6+hEJYlqfI+Yef0DbVZly1cy5r/jF
yNdGuGKvd5agvgCly8aYMza3P+D5S8sCAwEAAANvMG0wDgYDVR0PAAQH/BAQDAgXg
MAwGA1UdEwEB/wQCMAAwTQYDVR0REBEYwRKBCBgkrBgEAAQkVAgOgNRMzQ2hpcE1E
PVUxUk5TVE13TVRjd05qSTFBQUFwZndBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQU
CSqGSIB3DQEBcWUAA4IBAQCpHo/CUyk5Hs/asIcYw0ep8KocSkbN8qamyd4oWD
e/MGJW9Bs5f09IEbILWpdytCCS21SyJbxz2HvVDzdxQdxjDwUNiWuu3dWMXN/i67
yuCGM+lA1AAG5dT6lNgWYHh+YzsZm9eoq1+4NM+JuMXWsnzAK8rSy+dSpBxqFsBq
E00lPsaK7y2h8gs+XrV9x+D48OZQkTRXpxhJfiWvs+EbdgsAM/vBxTAoTJFPvMXWN
Cmcj9X52X13i4MdOUXocZLO2kh6JSGOYgkFeZifJ0iDvMfAf0cJ6+cEF6bSxAqBL
veel+8LmeiE/209h6qGHPPDacCaXA2oJCDHveAt8iPTG
-----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 sudi_id.pem -subject -noout
subject= /serialNumber=PID:C9600-SUP-1 SN:CAT2239L06B/CN=C9600-SUP-1-70b3171eaa00
```

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. This output includes measurements of each installed package file.

```
Device# show platform integrity sign nonce 123
Platform: C9800-L-F-K9
Boot 0 Version: R04.1173930452019-06-11
Boot 0 Hash: A6C92C44976FC77DD42234444FFD87798FB9036A2762FAA4999A190A0258B18C
Boot Loader Version: 16.12(1r)
Boot Loader Hash:
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
OS Version: 2020-03-19_20.26
OS Hashes:
C9800-L-universalk9_wlc.2020-03-19_20.26.SSA.bin:
53E2DF1A1A082E36EA4CAB817C1794EC9D69AC0E90BCBFEFC9BCD0BCA9385AA9E9372AEF7431E4A08FC5E5B9670131C09D158E5B8A7B457501FE77AB9F1C26D
C9800-L-mono-universalk9_wlc.2020-03-19_20.26.SSA.pkg:
1D3279D53B0311CE42C669824DF86FB5596CD7CA45CA8D7FDC3D10657B8C9A48F4B0508D7BCFFD645CB6571AC1E674A57A82414E3D6E1666BE64E6132F707671
PCR0: EE14A2D5099DA343B3941C54A429C4AC1D3EE8E9B609F1AC00049768A470734E
PCR8: 78794D0F5667F8FA4E425E3CA2AF3CD99B90B219FD90222D622B3D563416BBAA
```



Note Only OS and package hashes are supported.
