



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.



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

```
Device# show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCTU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaxNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaxNjbyBSb290IENBIDIwNDgwHhcN
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUEIhH
xmJVhEAYv8CrLqUccda8bnuoqrpu0hWtSEWdovyD0My5jOamaHBKeN8hF570YQXJ
FcjPFto1YmUQ6iEqDGYeJu5Tm8sUxJsZr2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFU14F1pyXOWWqCZe+36ufijXWlLvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6ke01a06g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmrxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFbi71R803UXH0jgkxhLtv5M0hmBvrbW7hmW
Yqao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJt37mjpXYgyc81WhJdTsD9i7rp77rMKSSh0T8lasz
Bvt9YaretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3Tkl4Eq1ZKR4OCXPDJoBYVL0fdX41Id
```

```

kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQLufQAAAAAADANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZWlzMRSwGQYDVQQDEwJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTEOMjAyNTQyWjAnMQ4wDAYDVQQKEwVDAxNj
bzEVMBMGA1UEAxMMQUNUMiBTvURJIENBMBIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAm5l3THixA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477Aks
5XAtUs5oxDYvt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYzo3qPCpxzprWJDPclM4iYKHumMQmqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKmp11TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdgj130VeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sX1XtEOjSXJ
URsYMEj53Rdd9tJwHky8neapsz+s+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVhM6aAgkWrSugiWbF2nsqvjBDBgNVHR8EPDA6MDIqNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZW50cm10eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNgh0dHA6Ly93d3cuY2l2Y28uY29tL3N1Y3VyaXR5
aXR5L3BraS9wY2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwdQYJ
KoZIHvcNAQEFBQADggEBAGhlqclr9tx4hzWgDERm37lyeuEmqCIfi9b9+GbmSjbi
ZHc/CcC10lJu0a9zTXA9w47H9/t61eduGxb4WeLxcwCiUgvFtCa51lklT8NbcKY
/4dw1ex+7amATUQ04QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECI
i5jUhoWryAK4dV08hCjkjEkzu3ufBTJapnv89g90E+H3VKM4L+/KdkUO+52djFkn
hy147d7cZR4DY4LIuFM2PlAs8YyjoNpK/urSRI14WdIlplRlnH7KND15618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIEAwQD7zANBgkqhkiG9w0BAQsFADANMQ4wDAYDVQQKEwVD
aXNjbyEVMBMGA1UEAxMMQUNUMiBTvURJIENBMB4XDTE4MDkyMzIyMzIwNDU0ZDQ1
MDUxNDIwMjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0
MzZMMFE5MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0
MRQwEgYDVQQDEwV0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0
AQoCggEBANsh0jcvgh1pdOjP9KnfDnDc/zEHDzbCTWpJi2FZcsaSE5jvq6CUqc4
MYpNAZU2Jym7NSD8iQbMXwbnCtoL64QtXQeFhRYmc4d5o933M7GwpEH0I7HUSbO/
Fxy7JbMgPPgAkY7rKsYENiNK2hiR7Q207X2BidOKknEuofWdJmNyMaZgLYLOhbJ
5oXaORxhUy3VRaxN16qI7kYxuugg2LcAbZ539sRXe8JtHyK811URNsgmiQ0S17pS
idGmrJJ0pEHA0EUVTzqEny3z+NW9uxLVSzu6+hEJYlqfI+Yef0DbVz1y1cy5r/jf
yNdGuGKvd5agvgCly8aYMza3P+d5S8sCAwEAANvMG0wDgYDVR0PAAQH/BAQDAgXg
MAwGA1UdEwEB/wQCMAAwTQYDVR0REBEYwRKBCBgkrBgEAAQkVAgOgNRMzQ2hpcELE
PVUxUk5TVE13TVRjd05qSTFBQUFwZndBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQU
CSqGSIB3DQEBcWUAA4IBAQCrpHo/CUyk5Hs/asIcYW0ep8KocSkn8h8qamyd4oWD
e/MGJW9Bs5f09IEbILWpdytCCS21SyJbxz2HvVDzdxQdxjDwUNiWuu3dWMXN/i67
yuCGM+lA1AAG5dT6lNgWYHh+YzsZm9eoq1+4NM+JuMXWsnzAK8rSy+dSpBxqFsbq
E00lPsaK7y2h8gs+XrV9x+D48OZQkTRXpxhJfiWvs+EbdgsAM/vBxTAoTJFPvMWN
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: C9606R
Boot 0 Version: MA0083R06.1810032017
Boot 0 Hash: 535AD9DC3D2A26C030D7DF6D4342FD52AB4DC6B1395DB18E7CA33F678A874B9E
Boot Loader Version: System Bootstrap, Version 16.11.1r[FC2], RELEASE SOFTWARE (P)
Boot Loader Hash:
C66199E7F63242A45FEAA0A8FCB5C17432FA13AF82FB1596D5CFF1FF1080F2107FEF8B48AC5DF88B41894AEC7AF87052717012BFF6185D34F579D9BF7184597
OS Version: BLD_V1611_THROTTLE_LATEST_20190203_030036
OS Hashes:
cat9k_iosxe.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.bin:
3F4A10066EAAA30417D7D17395ADD71FFCCED6ABA122ABA439D12A03C78EF38B8D281DEFA2D7CC15AA7FE63AA1344FEAFB68AC6409D408F89277F35DB8EE55
cat9k-wlc.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
2F0894E3F3A1332EDF2B2733EB456A4EB57E1A417BF46B53AD1323D1B02BA7688667C84AC7BD274B6B3A5DD3D19EB7EFA5DAB13E9941A37C73256C7577F3A3A1
cat9k-webui.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
ADE97B8FA0AC1C2694ECA93C96F77DCC0E96D7D36134795A4197AF60B9E2E9FE582C0535E9CE11A5EBD50542C6A94B55742E916185E333D3EF9E716D16AD0FDD
cat9k-guestshell.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
174AE72DF46F86D5ADD0A73344295A91C809CD42E6C12FEB29024215DAC89140511FE2EDFFEF85CEAD731B4276C85B3F7D5BF9386083CCEBE3E4C504E1E0400E1
cat9k-srdriver.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
64884593C2281B687374E283E14BFCF89F69D37EB4C238E7D71FA280B940FD0D11F57BAFF16788AA054AEEFB898BC689D623DDE25C743069538A7E83F146240
cat9k-sipbase.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
0AFF960435A97C9FA3522AC93E5CE1A683003C93CEBD4288A8AE481E3D9D8806451A23022AE5E810A010B6196B802CEA5D1354DDCC6B7A7120FF4A915B9ECF9
cat9k-espbase.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
6D5324CD00E578EF5C874620900ADEBFC38CD05B01E43B4E579E267D581145FE5E5FCE5ED09FE12338FDE2A162A389BED6C951AF8C394AE5FBAF4EAE4D7E9
cat9k-cc_srdriver.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
59362BDD62AB1E94297891D8BCEB467FB28261B6D75F6442610DD41A8E54D69609C94D081D32142412CC69C5C88036F26BE5F356B848ACBCEB5692A423D92F
cat9k-sippa.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
708B0D0869E841CD9220C916C566C46D07CE206FBAD294498E81A915E69F33063B9AFC0EBB5B048F250150E07EA37160AA8E5AA4CD491E402C836A6322631175
cat9k-rpbase.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
F24FB8347047A3D0930F8E353E2494EFCB6E0FB60E2A1BFE5F9C322EBC675A0A5D94CDC36195B41971F5B47383FB095BC731FB45407D42DE57BA14E3E6DEFFFE
PCR0: 7803FB049E7B111131B2FDACAF9B1918C28448E250054FE0C65D0317427A5EB1
PCR8: 0B65A1D00AA4AC815552170D11E5B4405C6D4B80453925E54F866D5BDF2B718A
Signature version: 1
Signature:
00958B89028F91726E018E9A720141F72009825330782700489206B010B597909F929A8E59C21096061066E1E4A91A5556663A20206112A0A140E2020
```

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 9600 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 Gibraltar 16.11.1	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.

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>.

