



# Boot Integrity Visibility

Boot integrity visibility allows Cisco's platform identity and software integrity information to be visible and actionable.

- [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](#)
- [Feature Information for Boot Integrity Visibility, on page 4](#)

## Information About Boot Integrity Visibility

Platform identity provides the platform's manufacturing installed identity, and 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 boot loader 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 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. It is recommended to wait for few minutes and then try the command again.

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

### SUMMARY STEPS

1. `show platform sudi certificate [sign [nonce nonce]]`

## 2. show platform integrity [sign [nonce nonce]]

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>show platform sudi certificate [sign [nonce nonce]]</b> <b>Example:</b> <pre># show platform sudi certificate sign nonce 123</pre>	Displays checksum record for the specific SUDI. <ul style="list-style-type: none"> <li>• (Optional) <b>sign</b> - Show signature</li> <li>• (Optional) <b>nonce</b> - Enter a nonce value</li> </ul>
Step 2	<b>show platform integrity [sign [nonce nonce]]</b> <b>Example:</b> <pre># show platform integrity sign nonce 123</pre>	Displays checksum record for boot stages. <ul style="list-style-type: none"> <li>• (Optional) <b>sign</b> - Show signature</li> <li>• (Optional) <b>nonce</b> - Enter a nonce value</li> </ul>

# Verifying Platform Identity and Software Integrity

## Verifying Platform Identity

The following example displays the Secure Unique Device Identity (SUDI) chain in PEM format. 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/h7KctU3I1CoxWlaMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwGwEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCWmrmrp68Kd6ficba0ZmKueIhH
xmJVhEAYv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmahBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJsZr2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFU14F1pyXOWWqCZe+36ufijXWlLvLdT6ZeYpzPEApk0E5tziVMMW/VgpSdh
jWn0f84bcN5wGyDwbs2mAag8EtKpP6BrXruOIIt6ke01a06g58QBdKhTCytKmg9l
Eg6CTy5j/e/rmxrbU6YTYK/CfdHbBc11HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwtzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQa18dwy3U8pORFbi71R803UXH0jgkxhLtv5MOhmBvrbW7hmW
Yqpa02TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFpliQRe6lJT37mjpXYgyc8lWhJDtSd9i7rp77rMKSSh0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe00caEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPLlHs27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX41Id
kxpUnwVvwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPCCAySgAWIBAgIKYQlufQAAAAAADANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTcwNjMwMTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTvURJIEENBMTIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
```

```

MIIBCgKCAQEAA0m5l3THixA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AKs
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKQVU6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQmqmgmg+
xghHIooWS80BocdiynEbeP5rZ7qRuewKmp1l1TiI3WdBNjZjnpfjg66F+P4SaDkGb
EXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfQXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdvQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVhm6aAgkWrSugiWbF2nsqvjBDBgNVHR8EPDA6MDigNqA0hjJodHRWoi8vd3d3
LmNpc2NvLmNvbS9zZW51cm10eS9wa2kvY3JsL2NyY2EyMDQ4LmNybdBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNgh0dHA6Ly93d3cuY2l2Y28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2l2Y28uY29tL3NlY3VyYXR5
L3BraS9wb2xpY2llcy9pbmRleC50dG1sMIBGAlUdEwEB/wQIMAYBAf8CAQAwdQYJ
KoZlHvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm37lyeuEmqCIfi9b9+GbMSJbi
ZHc/Cc101Ju0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgVfTca51Iklt8nNbcKY
/4dwllex+7amATUQO4QggIE67wVlPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjKjEkz3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djfKn
hy147d7cZR4DY4LIuFM2PlAs8YyjoNpK/urSRI14WdI1plR1nH7KND15618yFV
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDhzCCAm+gAwIBAgIEAJT3DDANBgkqhkiG9w0BAQsFADANMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGAlUEAxMMQUNUMiBTvURJIENBMB4XDTE1MTEwNDA5MzZmZmZmZmZmZm
MTEwNDA5MzZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
RkRPMtKONkjhMDUxDjAMBGNVBAoTBUNpc2NvMRgwFgYDVQQLLW9BQ1Q1MjBMAxRl
IFNVREkxGTAXBGNVBAMTEFdlUMzNjUwLTYyY2E5MDQ4VVEwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDWAwwgEKAoIBAQC6SARWYImWrRV/x7XQogAE+02WmzKki+4arMVBv19o
GgvJfkoJDDaHOROSUKEE3qXtd8N3lFky3TZ+jtHD85m2aGz6+IRx/e/lLsQzi6d1
WIB+N94pgecFBONPR9wJriox1IGD3B43b0hMLkmro4R5Zrs8XFkDo9k1tBU7F207
GEzb/Wk05NLeznezf2Niglx9fCDL0HC27BbsR5+03p8jhG0+mvrp8M9du1HKiGin
ZIV4XgTmP1/k/TVaIepEGZuWM3hxdUZjkNGG1clm+oB8vLX3U1SL76sDBBoiaprD
rjXBgBIOzyFW8tTjh50jMDG84hKD5s3liFoE4KpqEcnVAgMBAAGjBzBtMA4GA1Ud
DwEB/wQEAwIF4DAMBgNVHRMBAf8EAJAAME0GA1UdEQRMESgQgYJKwYBBAEJFQID
oDUTM0NoaXBjRD1VWUpOTLZJMENBUkhVM1Z1SUVSbF15QXlPQ0F4TXpvek5U331N
U0EwS0NnPTANBgkqhkiG9w0BAQsFAAOCAQEADjtm8vd1f+plWKSXK1C1qQ4aEnD5
p8T5e4iTer7Y1fbCrHIEEm3mnip+568j299z0H8V7PDp1l1juLHYMFTC+945F9RfA
eAuVWVb5A9dnGL8MsBJe2LVSnZwrWkT1EIdxLrTiPAQhtl16CN77S4u/f71oYE
tzPE5AGfyGw7ro1MEPVGffaQmYUDAwKFNH1uI7c2S1qlwk4WWZ6xxci+1haQnIG
pWzapaiaYL1XrcBz4KwFc1ZzPQT6hHw24jzYaYimvCo+/kSKuA9xNdtSu18ycox0
zKnXQ17s6aChMMt7Y8Nh4iz9BDejoOF6/b3sM0wRi+2/4j+6/GhcMRs0Og==
-----END CERTIFICATE-----

```

```

Signature version: 1
Signature:
405C770D802B73947EDBF8DD0D2C8180F10D4B3EF9699444514219C579D2ED52F7D5
83E0F4408133FC4E9F549B2EB1C21725F7CB1C79F98271E47E780E703E674723880F
B52D4963E1D1FB9787B38E28B8E696570A180B7A2F1311B1F174EAA79F55DB4765DF
67386126D899E07EDF6C26E0A81272EAA114437DD03F26992937082756AE1F1BFAFB
BFACD6BE9CF9C84C961FACE9FA0FEE64D85AE4FA0086969D0702C536ABDB8FBFDC47
C14C17D02FEBF4F7F5BB24D2932FA876F56B4C07816270AA0B4195C53D9758B5AEAE
3A74F2DBF293F52423ECB7B8539667080A9C57DA3E4B08B2B2CA623B2CBFA7080A0A
EB09B222E5B756970A3AA27E0F1D17C8A243

```

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-C3650-12X48UQ SN:FDO1946BG05/O=Cisco/OU=ACT-2 Lite
SUDI/CN=WS-C3650-12X48UQ
```

### 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.

```
Device #show platform integrity sign nonce 456
```

```
Platform: WS-C3650-12X48UQ
Boot Loader Version: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.16, engineering
software (D)
Boot Loader Hash: DB5A686E9F4CE358481DE3AF8B9C762F0A604E3B4764DF2A351F176E3D7
D3C60EB85C02906BD8CF28228C0DFC2AA8960CAFE6675D696E4ABA0CD687C0609E7E2
Boot 0 Version: F01062R15.0508d68fa2015-09-15
Boot 0 Hash: 6EF15CD54D3C66A8B64419A67B7ED57044C8C2E0EECB69736A7FFEC1F6D0EAD
OS Version: 2016-10-18_10.57_mundru
OS Hash: 4C85AECC88DAA49D940BBF65B1F17269F55C8D98DEFB4140F981923AA961140293E1
3B3E6E68CE3F8ED7F596CD858ACDD4BEF6538F59C1E243C351353026E6CD
PCR0: 90214167AAF35C06B2AC97292596E5669EAB72578FCDAD0B91746683BAA7B2B0
PCR8: FC2CE1BAC397F97008936DF372A2218BB16A798222B8FF55A7B6AEDA8018EDF5
Signature version: 1
Signature:
632A724F1AB6ADE134F6B0E8724D2052B3157F45B47E547763EE224A848E807CD737600587FF68
2526A8FE354A116CC9EDEBD9C659B9927336542EE4295084368327D01BD22AB4849BB3C007B6EB
B67708685FD6BC85DD045431E19A389FEB358894D4FBCF7C0FC960AC9133B61099DFD507F316C1
BF82F7F98687C7E7E8F99355DC1A95BD511B0B8DCB0CA909828F9EFBDF18847930392A8E3D072D
F3D90536880BAE9B7D7CF0E301D3F5AF16E7517FC2700E2F75911B836D6559A18E15B4CF452555
91656DF22DFF73392F777AEB796BCF9AC046C581ADEF19CA48A98F620BB58A79B32DA8B3BFB1CF
8399468A096E2F0C54B8B3ECD15EE3FE2C5ABDB5A029
```

The optional RSA 2048 signature is produced with the SUDI private key and can be verified with the SUDI public key contained in the SUDI certificate. The signature across PCR values, the signature version and the user-provided nonce is displayed.

```
RSA PKCS# 1 v1.5 Sign { <Nonce (UINT64)> || <Signature Version (UINT32)> || <PCR0 (32 bytes)>
|| <PCR8 (32 bytes)> }
```

Cisco management solutions are equipped with the ability to interpret the above output, compare the results against published Cisco values, and to verify the signature.

## Feature Information for Boot Integrity Visibility

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1: Feature Information for Open Plug-n-Play Agent**

Feature Name	Releases	Feature Information
Management and Control: Boot Integrity Visibility	Cisco IOS XE Everest 16.5.1	<p>The Boot Integrity Visibility feature allows Cisco's platform identity and software integrity information to be visible and actionable. Platform identity provides the platform's manufacturing installed identity, and software integrity exposes boot integrity measurements that can be used to assess whether the platform has booted trusted code.</p> <p>In Cisco IOS XE Everest 16.5.1, support was added for Cisco ASR 1000 Aggregation Series Routers.</p> <p>No commands were introduced or modified for this release.</p>

