



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	<p>show platform sudi certificate [sign [nonce]]</p> <p>Example:</p> <pre>Device# show platform sudi certificate sign nonce 123</pre>	<p>Displays checksum record for the specific SUDI.</p> <ul style="list-style-type: none"> • (Optional) sign - Show signature • (Optional) nonce - Enter a nonce value
Step 2	<p>show platform integrity [sign [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
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjAlMRywFAYDVQQK
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
Bvt9YAreTIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEbfJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hs27PKSb3TkL4Eq1ZKR4OCXPDJJoBYVL0fdX41Id
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPCCAySgAWIBAgIKYQlufQAAAAAADANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaxNjbyBSb290IENBIDIwNDgw
HhcNMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDAxNj
```

```

bzEVMBMGA1UEAxMMQUNUMiBTvURJiENBmIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAOm5l3THiXA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYvt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPUx+a6tHF/qRuOiJ44mdeDYzo3qPCpxzprWJDPclM4iYKHUMQMqmgmg+
xghHIOoWS80BOcdiyEbeP5rZ7qRuewKmpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdgJ13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URyMEj53Rdd9tJwHky8neapszS+r+kdvQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWbf2nsvqjBDBgNVHR8EPDA6MDIqNqA0hjJodHRWoi8vd3d3
LmNpc2NvLmNvbS9zZWN1cm10eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNgh0dHA6Ly93d3cuY2l2Y28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNmMjA0OC5jZXIwXAYDVR0GBFUwUzBRBgorBgEEAQKv
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2l2Y28uY29tL3NlY3VyYXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGAlUdEwEB/wQIMAYBAf8CAQAQDQYJ
KoZlThvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbmSjbi
ZHc/CcC101Ju0a9zTXA9w47H9/t61eduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dwlEX+7amATUQ04QggIE67wVlPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hcKjkEku3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKN
hy147d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KND15618yFVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDgTCCAmmgAwIBAgIEAp4UYzANBgkqhkiG9w0BAQsFADANMQ4wDAYDVQQKEwVd
aXNjbjEzEVMBMGA1UEAxMMQUNUMiBTvURJiENBmB4XDTE4MDYwNTAzNDUwNVoXDTE5
MDUxNDIwMjU0MjUwVowbTEpMCCGA1UEBRMgUe1EOKM5MjAwTC0yNFQ0tNEcgU046S1BH
MjIwMjAwQ0TgxDjAMBGNVBAOTBUNpc2NvMRgwFgYDVoQLEw9BQ1QtMiBMAxRlIFNV
REkxXjAUBGNVBAMTDUM5MjAwTC0yNFQ0tNEcgwGgEiMAOGCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQBDBm2Dg0GWQ18wLTKxeCt87DL8K1Rbx8Db1IigHjzebBXmpx7Ja
6Cp+kwRrIWGi5AmNmV7jZ2ZLj+vFVzBQ9eGM+6LdNg18c6nqmSmnuXMerD1UEMMK
bkFl4ydn1EIMoWpCARbgz+/zaLM2A5bpQXVndiKq1v0NA2Pgvqdxbm+8AELdDG/D
3SQ1anOja+yH5vu3NjyMjftjzk+n/ILp9iZMWzCA+O6E8KC5FclR2cfvWlQvoFM
ZEWmHdhHptsnN+4hhdDeurgeM0S+xIvZq0H7PxS0kT4vYQ9xWQEWavJAL44k0uY
JxKP6bDNssSLZ2s4/2OBSODjyBhb0GwrOAHdAgMBAAGjBzBtMA4GA1UdDwEB/wQE
AwIF4DAMBGNVHRMBAf8EAjAAME0GA1UdEQRGMEsgQyJKwYBBAEFQIDoDUTM0No
aXBjRD1RRGx6T0FZUHQRtJjRVFFQUFjQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
PTANBgkqhkiG9w0BAQsFAAOCAQEAgLUxZfnmrXZ6ZMGX69dDPkmvp9cFqXR538LF
PdyPCrUsk20GF80eDU0suIi4mbB87JSOWvLomdBtXdnxzRu4kPZNFz/7pjAVRT3R
gWMyiEnDWQsvy7e4SZmyVgej55e3hTW/LTeU8lCE0KR0YGDce5Phv2zdHtIsXrV
XsY+FrpfnTt1FV9qgDskDwCkF0bos6VsyWUpSCEGqF7LfnNBTKYvXUUmKXHKf/d
W5HgrYt6bQ/h/+0EP+MY2wpAiWMCfX6F+xW20vZfK8NzNesieB38IvuTkgefHz2s
yGCOavAxqGd0j7atcRpdRjt9+KM9Vwuy4VJZgK/t1fmTL4cawQ==
-----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:C9200L-24T-4G SN:FDO1946BG05/O=Cisco/OU=ACT-2 Lite
SUDI/CN=C9200L-24T-4G

```


