



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 4](#)
- [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.



Note Boot Integrity Visibility is supported only on the active supervisor. It does not support high availability scenarios.

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.

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	<p><code>show platform sudi certificate [sign [nonce nonce]]</code></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><code>show platform integrity [sign [nonce nonce]]</code></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. 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
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmahBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJsZR2tKys7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFU14F1pyXOWWqCZe+36ufijXWlLvLdT6ZeYpzPEApk0E5tzivMW/VgpSdh
jWn0f84bcN5wGyDwbs2mAag8EtKpP6BrXruOIIt6ke01a06g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQa18dwy3U8pORFbi71R803UXHOjgkxhLtv5MOhmBvrbW7hmW
Yqpao2TB9k5UM8Z3/sUcuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpxYgyc8lWhJdTsD9i7rp77rMKSH0T8Lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe00caEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX41Id
```

```

kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAAADANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQKQEWlDaXNjbyBTeXN0ZW1zMRswGQYDVQQDEXJDaXNjbyBSb290IENBIDwNDGw
HhcNMTEwNjMwMjE1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDAxNj
bzEVMBMGA1UEAxMMQUNUMiBTvURJIENBMBIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAOm5l3THIx9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYvt/zEbs1Zq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYzo3qPCpxzprWJDPclM4iYKHUMQmqmgmg+
xghHiooWS80BOcdiyEbeP5rZ7qRueWKmpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXGdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sX1XtEOjSXJ
URsyMEj53Rdd9tJwHky8neapsz+s+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHM6aAgkWrSugiWBF2nsvqjBDBgNVHR8EPDA6MDIqNqA0hjJodHRWoi8vd3d3
LmNpc2NvLmNvbS9zZW51cm10eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNgh0dHA6Ly93d3cuY2l2Y28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEAAQK5
AQwAMEMwQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2l2Y28uY29tL3NlY3VyYXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwdQYJ
KoZIHvcNAQEFBQADggEBAGhlqclr9tx4hzWgDERm371yeuEmqCIfi9b9+GmSjbi
ZHc/CcC10lJu0a9zTXA9w47H9/t61eduGxb4WeLxcwCiUgvFtCa51lkl8nNbcKY
/4dwlx+7amATUQ04QggIE67wVlPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECI
i5jUhoWryAK4dV08hCjkkjEkzu3ufBTJapn89g90E+H3VKM4L+/KdkUO+52djFKn
hy147d7cZR4DY4LIuFM2P1As8YyjoNpK/urSRI14WdIlplR1nH7KND15618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDgTCCAmmgAwIBAgIEAp4UYzANBgkqhkiG9w0BAQsFADANMQ4wDAYDVQQKEwVD
aXNjbyBzEVMBMGA1UEAxMMQUNUMiBTvURJIENBMB4XDTE4MDYwNTAzNDUwNVoXDTE5
MDUxNDIwMjU0MjU0VowbTEpMCCGA1UEBRMGUe1EOKM5MjAwTC0yNFQ0tNEcgU046S1BH
MjIwMjAwQWQ0TgxDjAMBGNVBAoTBUNpc2NvMRgwFgYDVQLEw9BQ1Q0tMiBMAXRlIFNV
REkxXjAUBGNVBAmtDUM5MjAwTC0yNFQ0tNEcwgEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDBm2Dg0GWQ18wLTKxeCt87DL8K1Rbx8Db1IigHjzebBXMpx7Ja
6Cp+kwRrIWGi5AmNmV7jZ2ZLj+vFVzBQ9eGM+6LdNg18c6nqmSmnuXMerD1UEMMK
bkF14ydn1EIMoWpCARbgz+/zaLM2A5bpQXVndiKq1v0NA2Pgvqdxbm+8AELdDG/D
3S1anOj+a+yH5vu3NjyMjfgtjzk+n/ILp9iZMWzcA+O6E8KC5FclR2cFvW1QvoFM
ZEWmHdhHPTsnN+4hhmDeurgeM0S+xIvzZq0H7Pxs0kT4vYQ9xWQEWavJAL44k0uY
JxKP6bDNssSLZ2s4/2OBsODjyBhb0GwrOAHdAgMBAAGjbjzBtMA4GA1UdDwEB/wQE
AwIF4DAMBGNVHRMBAF8EAjAAAME0GA1UdEQRGMEsGqYgYJKwYBBAEFQIDoDUTM0No
aXBjRD1RRGx6T0FZUHqWRTJRVFFQUFjQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
PTANBgkqhkiG9w0BAQsFAAOCAQEAgLUXzfnmrXZ6ZMGX69dDFkmp9cFqXR538LF
PdyPCRuSk20GF80eDU0suIi4mbB87JSOWvLomdBtXdnxRu4kPZNFz/7pjAVRT3R
gWMMYiEnDWQsVy7e4SZmyVgej55e3hTW/LTeU8lCE0KRoYGDce5Phv2zdHtIsXrV
XsY+Frpfn1FV9qqDskDwcKf0bos6VsyWUpSCEGqF7LfnNBTKYvXUUmKXHKf/d
W5HgrYt6bQ/h/+0EP+MY2wpAiWMCfX6F+xW20vZfK8NzNesieB38IvuTkgefHz2s
yGOavAxqGd0j7atcRpdRjt9+KM9Vwuy4VJZgK/tl1fmTL4cawQ==
-----END CERTIFICATE-----

```

```

Signature version: 1
Signature:

```

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 123
Platform: C9200L-24T-4G
Boot 0 Version: SBOOT0.v27
Boot 0 Hash:
EE98DCD0D6AEA85C8891039F649664FCC3CF709CCFC7A6F248C9D5BA8463528F
Boot Loader Version: System Bootstrap, Version 10.2, DEVELOPMENT SOFTWARE
Boot Loader Hash:
9220B7E7A153A79EB9AE37311A1FE2313C999F2103F8AE7EF4985D8E742765E4CDEF53E7B3C50E84121C00BD25567864FE155D80AFF67F63F1A69B
OS Version: 16.09.01
OS Hash:
7099B3108F5A1D9C967580DAD383457394A0909E550090ED9EB34F1D0871DE1AD56355A8F3BC19399B7136EAD7401DEA69ED65FFDCE107F11C98E0E0F5D
PCR0: 750E5D2EDAE6E3A68050638E0BFD8619BE4EA13066025D39DF79408719F5177E
PCR8: EB6E739A63F53E703B6CDAF3F6188833CEF6D32E2F726006B9AA34E1E73048C4
Signature version: 1
Signature:
    
```

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 9200 Series Switches)</i>

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

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 Fuji 16.9.2	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>.

