Boot Integrity Visibility

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.

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	**show platform sudi certificate** [**sign** [**nonce** *nonce*]] **Example:** `Device# show platform sudi certificate sign nonce 123`	Displays checksum record for the specific SUDI. • (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. • (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
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUl4F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1aO6g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
olEwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
```

```
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQMqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcCl0lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KNDl5618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDeTCCAmGgAwIBAgIEAYF/rTANBgkqhkiG9w0BAQsFADAnMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMB4XDTE3MDQyODEwNTU1NVoXDTI3
MDQyODEwNTU1NVowZTElMCMGA1UEBRMcUElEOkM5NTAwLTE2WCBTTjpGQ1cyMTE3
QTU2TTEOMAwGA1UEChMFQ2lzY28xGDAWBgNVBAsTD0FDVC0yIExpdGUgU1VESTES
MBAGA1UEAxMJQzk1MDAtMTZYMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAsenmrNybW0gLru4Y3UakblbFjmHvIwIdEro2HZPewrv/S014tPOAuXSfFdJh
SRAGwhB4ji71P4R9AqoQfrpybq3fJEaJCmakkdP5VBmPLm+QdJwGc7GGiUuXr6/R
PTjzdfVTJ0uvEi/holnTrYuHiu0JT3vsXi1bKkl1HJFeGspMCSZRRcoAxIZ8GRFt
+Y5f3QgV7b1Ce4zLSxJqTqiEDUNRuoeGwb+YtQOtep53hnwVoU6bjNaQXjq9pgcJ
dMyhh+zRtaRREpes4B7IZaFSMGeUbGvfVE6R+40mIM+T26fnZa2k4bQvrcm/1Vbe
/6Fy4rniHAXwzGCCgIHfIJMrSwIDAQABo28wbTAOBgNVHQ8BAf8EBAMCBeAwDAYD
VR0TAQH/BAIwADBNBgNVHREERjBEoEIGCSsGAQQBCRUCA6A1EzNDaGlwSUQ9VVlK
T1NqSk1Cd2dhVFc5dUlFOWpkQ0F4TUNBeE1qbzFORG96T0NENE9hQT0wDQYJKoZI
hvcNAQELBQADggEBADxO7Ks4AlSb8WnEq0OMoq+3tiXHLDYVdJUgH0w5FsUoE13f
yxn867saiJVMYrT7+/wTsexxdDJySGAJH5mPdwPPmEfLHw9/D6/l/d6Fsc1M/LeB
q+Q2a6L6oZd1rJJheNQyCN/jOCYuM0dK9JyDjLda9jSa3AL7UsOcr9aciBQ/CjZ6
8bV3x8LzAyPDs++qy6fHgB4OpP8vOJtQdnYGDZAtOun4Jlz3PyXjSJy9XWoWflG+
2nGXg9PCig8l1ppPjDg1prZ60lt+scEEJzqZmoHGn/lelOH4s+mJTVAxbgBudcA3
0XpdeHqOD0OdkG8JkXPYcUQ5in4R6zgwXEnqMzY=
-----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:C9500-16X SN:FDO1946BG05/O=Cisco/OU=ACT-2 Lite SUDI/CN=C9500-16X
```

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. 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 in install mode. This output includes measurements of each installed package file.

```
Device# show platform integrity sign nonce 123
Platform: C9500-16X
Boot 0 Version: MA0081R06.1307262016
Boot 0 Hash: A99EF9F31CE3F3F8533055407F1C88C62176E667E4E1DA0649EAA7A1282F205E0A
Boot Loader Version: System Bootstrap, Version 16.8.0.3, RELEASE SOFTWARE (P)
Boot Loader Hash:
F82826514658055C3993AB95F53512341BF20F3CC7D4083C980450EA6CD84608EE636B5B15D13414203CED35603F01974B8676C6AC6F9DC45B25CD1039E686C40A
OS Version: 16.10.01
OS Hashes:
cat9k-cc_srdriver.16.10.01.SPA.pkg :
D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0
cat9k-espbase.16.10.01.SPA.pkg :
3EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEF43
cat9k-guestshell.16.10.01.SPA.pkg :
B0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03E
cat9k-rpbase.16.10.01.SPA.pkg :
4057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C6
cat9k-rpboot.16.10.01.SPA.pkg :
AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057
cat9k-sipbase.16.10.01.SPA.pkg :
9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A
cat9k-sipspa.16.10.01.SPA.pkg :
E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673
cat9k-srdriver.16.10.01.SPA.pkg :
4FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E211
cat9k-webui.16.10.01.SPA.pkg :
CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7
cat9k-wlc.16.10.01.SPA.pkg :
AA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCCA
PCR0: 9745B571B66D79F0936F4D292B5672B50F50FD1E56E74248D48A33582E992574
PCR8: 1CC295C233DA41BD3530A6F09C21991E8406BFFC88249D7778CA4BB0B9E71EB7
Signature version: 1
Signature:
[redacted]
```

The following is a sample output of the **show platform integrity sign nonce 123** command in bundle mode. This output includes measurements of the bundle file and each installed package.

```
Device# show platform integrity sign nonce 123
Platform: C9500-16X
Boot 0 Version: MA0081R06.1307262016
Boot 0 Hash: A99EF9F31CE3F3F8533055407F1C88C62176E667E4E1DA0649EAA7A1282F205E0A
```

```
Boot Loader Version: System Bootstrap, Version 16.8.0.3, RELEASE SOFTWARE (P)
Boot Loader Hash:
F8282651465805 5C3993AB95F53512341BF20F3CC7D4083C980450FA6CD84608EE636B5B15D13414203CED35603F01974B8676C6AC6F9DC45B25CD1039E686C40A
OS Version: 16.10.01
OS Hashes:
cat9k_iosxe.16.10.01.SPA.bin :
F4CAD08BE1EF841C3A2E3ED8540829F08F3CBA9336F38E45669D4D8B15AD15E365B922AC8B4DC0D5B63E2806D6A1BDAB7839DD9DC8CD7E366A49ED648C113440
cat9k-cc_srdriver.16.10.01.SPA.pkg :
D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0
cat9k-espbase.16.10.01.SPA.pkg :
3EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEF43
cat9k-guestshell.16.10.01.SPA.pkg :
B0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03E
cat9k-rpbase.16.10.01.SPA.pkg :
4057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C6
cat9k-rpboot.16.10.01.SPA.pkg :
AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057
cat9k-sipbase.16.10.01.SPA.pkg :
9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A
cat9k-sipspa.16.10.01.SPA.pkg :
E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673
cat9k-srdriver.16.10.01.SPA.pkg :
4FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E211
cat9k-webui.16.10.01.SPA.pkg :
CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7
cat9k-wlc.16.10.01.SPA.pkg :
AA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCCA
PCR0: 9745B571B66D79F0936F4D292B5672B50F50FD1E56E74248D48A33582E992574
PCR8: 1CC295C233DA41BD3530A6F09C21991E8406BFFC88249D7778CA4BB0B9E71EB7
Signature version: 1
Signature:
[redacted]
```

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.	*Command Reference (Catalyst 9500 Series Switches)*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	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 16.8.1a	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. Support for this feature was introduced only on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models of the Cisco Catalyst 9500 Series Switches.
Cisco IOS XE Fuji 16.9.1	Boot Integrity Visibility	Support for this feature was introduced only on the C9500-32C, C9500-32QC, C9500-48Y4C, and C9500-24Y4C models of the Cisco Catalyst 9500 Series Switches.

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.