



ブート整合性の可視性

- [ブート整合性の可視性について \(1 ページ\)](#)
- [ソフトウェアイメージとハードウェアの確認 \(1 ページ\)](#)
- [プラットフォーム ID とソフトウェア整合性の確認 \(2 ページ\)](#)
- [ブート整合性の可視性に関する追加情報 \(6 ページ\)](#)
- [ブート整合性の可視性の機能履歴 \(6 ページ\)](#)

ブート整合性の可視性について

ブート整合性の可視性によって、シスコのプラットフォーム ID とソフトウェアの整合性情報が可視化され、実用可能になります。プラットフォーム ID は、プラットフォームの製造元でインストールされた ID を提供します。ソフトウェアの整合性ではブート整合性の測定値が明らかになり、それを使用してプラットフォームが信頼できるコードを起動しているかどうかを評価できます。

ブートプロセス中に、ソフトウェアはブートローダーアクティビティの各ステージのチェックサムレコードを作成します。

このレコードを取得して、シスコ認定レコードと比較し、ソフトウェアイメージが正規かどうかを確認できます。チェックサム値が一致していない場合は、シスコによって認定されていない、または未承認パーティによって改ざんされているソフトウェアイメージを実行している可能性があります。

ソフトウェアイメージとハードウェアの確認

このタスクでは、スイッチの起動時に作成されたチェックサムレコードを取得する方法について説明します。特権 EXEC モードで次のコマンドを入力します。



(注) 次のコマンドを実行した後で、メッセージ **% Please Try After Few Seconds** が CLI に表示されることがあります。これは CLI の障害を示すものではありませんが、必要な出力を取得するために必要な基盤となるインフラストラクチャの設定を示します。数分間待機して、コマンドを再度試すことをお勧めします。

メッセージ **% Error retrieving SUDI certificate** および **% Error retrieving integrity data** は、実際の CLI 障害を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	show platform sudi certificate [sign [nonce nonce]] 例： Device# show platform sudi certificate sign nonce 123	特定の SUDI のチェックサム レコードを表示します。 <ul style="list-style-type: none"> • (オプション) sign : 署名を示します • (オプション) nonce : ナンス値を入力します
ステップ 2	show platform integrity [sign [nonce nonce]] 例： Device# show platform integrity sign nonce 123	ブート段階のチェックサム レコードを表示します。 <ul style="list-style-type: none"> • (オプション) sign : 署名を示します • (オプション) nonce : ナンス値を入力します

プラットフォーム ID とソフトウェア整合性の確認

プラットフォーム ID の確認

次に、PEM 形式でセキュアな固有デバイス識別子 (SUDI) チェーンを表示する例を示します。SUDI にエンコードされるのは、個々のデバイスの製品 ID とシリアル番号であり、何千ものデバイスからなるネットワーク上でデバイスを一意に識別できます。最初の証明書は Cisco Root CA 2048 で、2 番目はシスコの下位 CA (ACT2 SUDI CA) です。どちらの証明書も、<https://www.cisco.com/security/pki/> で公開されているものと一致しているかを確認できます。3 番目は SUDI 証明書です。

```
Device# show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KctU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTenX0ZW1zMRswGQYDVQQDEsJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
```

```

Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQDExJDaXNjbyBSb290IENBIDIwNDgwgEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwgEIAoIBAQCwmrmp68Kd6f1cba0ZmKUEIhH
xmJVhEAYv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5j0AmaHBKeN8hf570YQXJ
FcjPFto1YmUQ61EqDGYeJu5Tm8sUxJsZr2tKyS7McQr/4NEb7Y9JhcJ6r8qqB9q
VvYgDxFUL4F1pyXOWWqCZe+36ufijXWlBvLdT6ZeYpzPEApk0E5tzivMW/VgpSdh
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6ke01a06g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYUCUOG/rksc35LgLfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFbi71R803UXHOjgxxkLtv5M0hmEVRBW7hmW
Yqpao2TB9k5UM8Z3/sUcuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cb7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJdTsd9i7rp77rMKSSh0T8lasz
Bvt9YaretIpsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGeOcaEblfJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJqkOXuPL1hS27PKSb3TkL4Eq1ZKR4OCXPdJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

```

```

MIIEPDCCAySgAwIBAgIKYQlufQAAAAAADANBgkqhkiG9w0BAQUFADA1MRYwFAyD
VQKKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQDExJDaXNjbyBSb290IENBIDIwNDgW
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQKKEwVDAxNj
bzEVMBMGALUEAxMMQUNUMiBTVURJENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBGgKCAQEA0m513THIXA9tN/hs5qR/6UZRpdd+9aE2JbFknjht6gfHKd477AkS
5XAtUs5oxDYvt/zEbs1Zq3+LR6qrqKQVu6JYvH05UYLBqCj38s76Nlk53905Wzp
9pRcmRCPUx+a6tHF/qRuOiJ4mdedYz03qPCpxzprWJDPclM4iYKHuMqMgmq+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXDgJ130veF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sX1XtEoJSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdvQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GALUdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVhm6aAgkWrSugiWBF2nsqvjBDBGNVHR8EPDA6MDiGnQa0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZW10eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBGRgRgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNh0dHA6Ly93d3cuY21zY28uY29tL3N1Y3Vy
aXR5L3BraS9jZXJ0cy9jcmNmMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEAAQkV
AQwAMEMwQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY21zY28uY29tL3N1Y3VyXAR5
L3BraS9wb2xpY21lcY9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAgh1qclr9tx4hzWgDERm371yeuEmqcIffi9b9+GbMSJbi
ZHc/Cc101Ju0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Ik1t8nNbcKY
/4dwlEx+7amATUQ04QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimbSv6TEci
i5jUhOWryAK4dVo8hcJkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djfKn
hyl47d7cZR4DY4LlUfM2P1As8YyjzoNpK/urSRI14wdI1plRlnH7KND15618yfvFP
0IFJZBGrooCRBjOSwFv8cpWcbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

```

```

MIIDgTCCAmgAwIBAgIEAp4UYzANBgkqhkiG9w0BAQsFADANMQ4wDAYDVQKKEwVDA
xNjbyzEVMBMGALUEAxMMQUNUMiBTVURJENBMB4XDTE4MDYwNTAzNDUwNVoXDTI5
MDUxNDIwMjU0MVowbTEpMCCGALUEBRMgUELEOKM5MjAwTC0yNFQtnEcGU046S1BH
MjIwMjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0
REkxYjAwQTAwQTAwQTAwQTAwQTAwQTAwQTAwQTAwQTAwQTAwQTAwQTAwQTAwQTAw
DwAwgEKAoIBAQBm2Dg0GWQ18wLTKxeCt87DL8K1Rbx8Db1IigHjzebbXMPx7Ja
6Cp+kwRrIwGi5AmNmV7jZ2ZLj+vFVzBQ9eGM+6LdNg18c6nqmSnnuXMerD1UEMMK
bkFl4ydn1EIMoWpCARbgz+/zaLM2A5bpQXVndiKq1v0NA2Pgvqdxbm+8AELdDG/D
3SQ1anOja+yH5vu3NjyMjftjzk+n/ILp9iZMWzcA+O6E8K5FclR2cfvWlQvoFM
ZEWmHdhHPTsnN+4hhmDeurgeM0S+xIvzZqOH7PxS0k4vYQ9xWQEwawJAL44k0uY
JxKP6bdNssSLZ2s4/20BSODjyBhb0GwrOAHdAgMBAAGjBzBtMA4GA1UdDwEB/wQE
AwIF4DAMBGNVHRMBAf8EAJAAME0GALUdeEQRGMESgQYJKwYBBAEJFQIDoDUTM0No
aXBjRD1RRGx6T0FZUHQwRTJJRVFFQUFjQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
PTANBgkqhkiG9w0BAQsFAAOCAQEAgLUxZfNmrXZ6ZMGX69dDPkmvp9cFqXR538LF
PdypCRuSk20GF80eDUOSuIi4mbB87JSOWvLomdBtXdnxzRu4kPZNFz/7pjAVRT3R
gWMMyiEnDWQsvy7e4SZmyVgej55e3hTW/LTeU8lCE0KRoYGDce5Phv2zdHtIsXrV
XsY+Erropfntt1FV9qqDskDWcKf0bos6VsyWUpSCEGqF7LfnNBTKYvXUUmKXHKf/d
W5HgrYt6bQ/h/+0EP+MY2wpAiWMCfX6F+xW20vZfK8NzNesieB38IvuTkgefHz2s
yGCOavAxqGd0j7atcRpdRjt9+KM9Vwuy4VJZgK/tlfmTL4cawQ==
-----END CERTIFICATE-----

```

Signature version: 1

Signature:

```
-----BEGIN RSA SIGNATURE-----
```

オプションの RSA 2048 署名は、3つの証明書、署名のバージョンおよびユーザにより提供されるナンスに対するものです。

```
RSA PKCS#1v1.5 Sign {<Nonce (UINT64)> || <Signature Version (UINT32)> || <Cisco Root CA
 2048 cert (DER)> ||
<Cisco subordinate CA (DER)> || <SUDI certificate (DER)> }
```

シスコの管理ソリューションには、上記の出力を解釈する機能が装備されています。しかし、OpenSSL コマンドを使用した簡単なスクリプトを使用してプラットフォームの ID を表示して署名を確認することもでき、それによってシスコの一意のデバイス ID を確保できます。

```
[linux-host:~]openssl x509 -in sudicert.pem -subject -noout
subject= /serialNumber=PID:C9200L-24T-4G SN:FD01946BG05/O=Cisco/OU=ACT-2 Lite
SUDI/CN=C9200L-24T-4G
```

ソフトウェア整合性の確認

次に、ブート段階のチェックサムレコードを表示する例を示します。ハッシュ測定値は、連続してブートされたソフトウェアの3つの段階それぞれについて表示されます。これらのハッシュをシスコが提供する基準値と比較できます。出力に署名するオプションを使用すると、出力は正規であり改ざんされていないことを保証する機能が検証ツールに付与されます。リプレイ攻撃から保護するために、ナンスを提供できます。



- (注) ブート整合性ハッシュは MD5 ハッシュではありません。たとえば、バンドルファイルに対して `verify/md5 cat9k_iosxe.16.10.01.SPA.bin` コマンドを実行すると、ハッシュは一致しません。

次に、インストールモードでの `show platform integrity sign nonce 123` コマンドの出力例を示します。この出力には、インストールされている各パッケージファイルの測定値が含まれます。

```
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:
922087E7A153A79E9AE37311A1FE2313C9996E21032F8A1E7EF4935D3E742765E40DE53E7B3C50E84121C00B2D5567864FE15D30A9F67F63E1A6B
OS Version: 16.10.01
OS Hashes:
cat9k_lite-rpbase.16.10.01.SPA.pkg :
DD15C1DEFB03B0C6057AD6A9673E2114FA7CCAA7ED0AE935CB0B84E0DD15C1DEFB03B0C6057AD6A9673E2114FA7CCAA7ED0AE935CB0B84E0
cat9k_lite-rpboot.16.10.01.SPA.pkg :
AD6A9673E2114FA7CCAA7ED0AE935CB0B84E0DD15C1DEFB03B0C6057AD6A9673E2114FA7CCAA7ED0AE935CB0B84E0DD15C1DEFB03B0C6057
cat9k_lite-srdriver.16.10.01.SPA.pkg :
4FA7CCAA7ED0AE935CB0B84E0DD15C1DEFB03B0C6057AD6A9673E2114FA7CCAA7ED0AE935CB0B84E0DD15C1DEFB03B0C6057AD6A9673E211
cat9k_lite-webui.16.10.01.SPA.pkg :
```


ブート整合性の可視性に関する追加情報

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9200 Series Switches)</i>

ブート整合性の可視性の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	ブート整合性の可視性	ブート整合性の可視性によって、シスコのプラットフォームIDとソフトウェアの整合性情報が可視化され、実用可能になります。プラットフォームIDは、プラットフォームの製造元でインストールされたIDを提供します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。