

Trustworthy Systems Commands

This module describes the commands related to trustworthy systems on Cisco IOS XR7 software.

For detailed information about the key components that form the trustworthy security systems, see the *Implementing Trustworthy Systems* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series RoutersSystem Security Configuration Guide for Cisco 8000 Series Routers*.

- platform security device-ownership, on page 2
- platform security variable customer, on page 3
- show platform security boot mode, on page 5
- show platform security integrity log, on page 7
- show platform security variable customer, on page 8
- show platform security tpm , on page 10
- show platform security tpm integrity log boot, on page 12
- show platform security tpm info ECC-sudi-certs, on page 14
- show platform security tpm attest certificate , on page 17

platform security device-ownership

To configure secure device ownership for the router, use the **platform security device-ownership** command in EXEC modeXR EXEC mode.

platform security device-ownership *ownership-voucher-path* **location** { *location* | **all** }

Syntax Description

ownership-voucher-path	Path to the .tar file containing the Ownership Vouchers (OV) and Authenticated Variable (AV) to securely transfer device ownership
location { *location* | **all** }	Applies AV to a specific location or all locations

Command Default

None

Command Modes

EXECXR EXEC

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

A power cycle of the node is required for the extended ownership transfer to take affect.

Task ID

Task ID	Operations
system	read, write

Examples

This example shows how to configure the device ownership on the router:

```
Router#platform security device-ownership /harddisk:/multiple-ov.tar.gz location all
Thu Feb 23 16:42:19.207 UTC
Successfully applied ownership voucher in node0_RP0_CPU0.
Successfully applied ownership voucher in node0_1_CPU0
Power-cycle of the node is required for the dual ownership transfer to take affect.
```

platform security variable customer

To configure the secure variable for certificate storage of customer variables, use the **platform security variable customer** command in EXEC modeXR EXEC mode.

platform security variable customer { **zeroize** *authenticated-variable-file-path* **GUID** *av-customer-guid* | **append** *key authenticated-variable-file-path* | **update** *key authenticated-variable-file-path* } **location** { *location* | **all** }

Syntax Description

zeroize	Clears the entire certificate store using Authenticated Variable (AV). Use this variable with caution
append *key*	Appends certificates or hashes to Extensible Firmware Interface (EFI) to one of the following keys: • KEKCustomer—Key Exchange Key Customer • PKCustomer—Platform Key Customer • dbCustomer—Signature and key database Customer • dbxCustomer—Forbidden signature and key database Customer
update *key*	Removes or replace certificates or hashes in EFI for one of the following keys: • KEKCustomer—Key Exchange Key Customer • PKCustomer—Platform Key Customer • dbCustomer—Signature and key database Customer • dbxCustomer—Forbidden signature and key database Customer
authenticated-variable-file-path	Path to the AV file
GUID *av-customer-guid*	Cisco-provided Global Unique Identification number (GUID)
location { *location* | **all** }	Applies AV to a specific location or all locations

Command Default

None

Command Modes

EXECXR EXEC

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

Use the zeroize command with caution as the entire certificate store using authenticated variable can be cleared. After you use the command, a reboot is required immediately for the changes to take effect.

Task ID

Task ID	Operations
system	read, write

Examples

This example shows how to update the KEKCustomer key for all nodes on the router using a sample `sonic-kek-release-update.auth` file that is created and stored in the harddisk: of the router:

```
Router#platform security variable customer update KEKCustomer
/harddisk:/sonic-kek-release-update.auth location all
Fri Feb 24 05:15:35.765 UTC
Performing operation on all nodes..
=========================
Location : 0/RP0/CPU0
=========================
Successfully applied AV /harddisk:/sonic-kek-release-update.auth for KEKCustomer
* WARNING *: Immediate reboot is recommended to avoid system instability!
=========================
Location : 0/1/CPU0
=========================
Successfully applied AV /harddisk:/sonic-kek-release-update.auth for KEKCustomer
* WARNING *: Immediate reboot is recommended to avoid system instability!
```

show platform security boot mode

To display the security boot mode for the router, use the **show platform security boot mode** command in EXEC modeXR EXEC mode.

show platform security boot mode location { *location* | **all** }

Syntax Description

location { *location* | **all** }	Specifies a specific location or all locations

Command Default

None

Command Modes

EXECXR EXEC

Command History

Release	Modification
Release 7.10.1	This command was introduced.

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
system	read, write

Examples

This example shows how to view the secure boot mode of the router. In this example, the mode is `Generic Mode`:

```
Router#show platform security boot mode location all
Tue Feb 21 16:40:16.207 UTC
Performing operation on all nodes...
=========================
Location  :  0/RP0/CPU0
=========================
Aikido mode: Generic Mode
Aikido mode value: 43

=========================
Location  :  0/1/CPU0
=========================
Aikido mode: Generic Mode
Aikido mode value: 43
```

This example shows the mode in `Customer Mode`:

```
Router#show platform  security boot mode location all
Tue Feb 21 16:40:16.207 UTC
Performing operation on all nodes..
=========================
Location : 0/RP0/CPU0
```

```
=========================

Aikido mode: Customer Mode
Aikido mode value: 127
=========================
Location : 0/2/CPU0
=========================

Aikido mode: Customer Mode
Aikido mode value: 127
=========================
Location : 0/1/CPU0
=========================

Aikido mode: Customer Mode
Aikido mode value: 127
```

show platform security integrity log

To display the security integrity logs for the router, use the **show platform security integrity log** command in EXEC modeXR EXEC mode.

show platform security integrity log { **boot location** *location-name* | **runtime** *file-location* | **secure-boot status location** *location-name* }

Syntax Description

boot	Displays boot integrity logs
runtime	Displays integrity measurement architecture (IMA) logs
secure-boot	Displays information related to secure boot

Command Default

None

Command Modes

EXECXR EXEC

Command History

Release	Modification
Release 7.10.1	The command was modified to include the secure boot status.
Release 7.0.12	This command was introduced.

Usage Guidelines

If the router does not support this secure boot verification functionality, then the status is displayed as *Not Supported*.

Task ID

Task ID	Operations
system	read, write

Examples

This example shows how to verify the secure boot status of the router:

```
Router#show  platform security integrity log secure-boot status
Wed Aug 10 15:39:17.871 UTC

+-------------------------------------+
   Node location: node0_RP0_CPU0
+-------------------------------------+
Secure Boot Status: Enabled
Router#
```

show platform security variable customer

To verify that the customer key certificate is active and registered for PKCustomer, KEKCustomer, dbCustomer and dbxCustomer variables, use the **show platform security variable customer** command in EXEC modeXR EXEC mode.

show platform security variable customer *key* **[detail] location** { *location* | **all** }

Syntax Description

key	Specifies the type of variable to which the customer key certificate is added—PKCustomer, KEKCustomer, dbCustomer and dbxCustomer
detail	Displays full certificate details for a specific location or all nodes
location *location-name*	Specifies a specific location or all locations

Command Default

None

Command Modes

EXECXR EXEC

Command History

Release	Modification
Release 7.10.1	This command was introduced.

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
system	read, write

Examples

This example shows how to view the secure variables for KEKCustomer certificate for all the locations on the router:

```
Router#show platform security variable customer KEKCustomer location all
Fri Feb 24 05:16:56.365 UTC
Performing operation on all nodes..
=========================
Location : 0/RP0/CPU0
=========================

Variable : KEKCustomer
+--------------------

Signature List # 0
 GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
 Extension type : X509

 Entry # 0
 Owner GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
 Size : 1211
```

```
  Serial Number  : BA:5C:D4:5E:F3:D4:D0:4C
  Subject:
        O=Cisco,OU=RELEASE,CN=IOSXR-WHITEBOX-KEK
  Issued By      :
        O=Cisco,OU=RELEASE,CN=IOSXR-WHITEBOX-KEK
  Validity Start : 10:03:18 UTC Wed Feb 23 2022
  Validity End   : 10:03:18 UTC Tue Feb 18 2042

  CRL Distribution Point
        http://www.cisco.com/security/pki/crl/crcakekdtxr.crl
  SHA1 Fingerprint:
         AE4DFD35EB8486FC5707609C93A5C44CDB579126

Total Signature Lists # 1
Total Certificates # 1
=========================
Location : 0/1/CPU0
=========================

Variable : KEKCustomer
+--------------------

Signature List # 0
 GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
 Extension type : X509

 Entry # 0
 Owner GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
 Size : 1211

  Serial Number  : BA:5C:D4:5E:F3:D4:D0:4C
  Subject:
        O=Cisco,OU=RELEASE,CN=IOSXR-WHITEBOX-KEK
  Issued By      :
        O=Cisco,OU=RELEASE,CN=IOSXR-WHITEBOX-KEK
  Validity Start : 10:03:18 UTC Wed Feb 23 2022
  Validity End   : 10:03:18 UTC Tue Feb 18 2042

  CRL Distribution Point
        http://www.cisco.com/security/pki/crl/crcakekdtxr.crl
  SHA1 Fingerprint:
         AE4DFD35EB8486FC5707609C93A5C44CDB579126

Total Signature Lists # 1
Total Certificates # 1
```

show platform security tpm

To display the status and key details of the Trusted Platform Module (TPM) on the router, use the **show platform security tpm** command in EXEC modeXR EXEC mode XR EXEC mode.

show platform security tpm { PCR attest hardware info integrity location { *location* | **all** } **}** [**nonce**]

Syntax Description

PCR	Specifies the PCR quotes and value. The PCR value can be from 0 to 7 or all 0-7 separated by commas. The PCR bank is based on SHA384.
attest	Specifies the TPM attest information.
hardware	Specifies the TPM system hardware integrity PCR15.
info	Specifies the generic TPM device information.
integrity	Specifies the TPM integrity.
nonce	Specifies the Nonce value to fetch the PCR quotes.
location { *location* | **all** }	Specifies the location of TPM certificates.

Command Default

None

Command Modes

EXECXR EXEC

XR EXEC

Command History

Release	Modification
Release 25.4.1	This command was introduced.

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
system	read, write

Examples

This example shows how to view the status and key details of TPM.

```
Router#show  platform security tpm pcr 0,1,2,3,4,5,6,7 location 0/rp0/CPU0

+--------------------------------------+
   Node location: node0_RP0_CPU0
+--------------------------------------+
Uptime: 503957
pcr-index       pcr-value
```

```
  0     jkkHIFe0ce11YQouajSuN0jharqmSlK8dIr4j9TxXDb0PNVE9DjqO8vAh4tqHrl2
  1     wqoQkOVvOepm0+UwHGMmZwOYQl+B1R3TAaCnM3N5spA47EMWEI8cJDv77BvU02Ep
  2     UYkjsPlV0I2gd8lqq6Uiud7O3mHFmc6mxBiJz76krk1QUp2W/k0a/a+2Xn+VvyPE
  3     UYkjsPlV0I2gd8lqq6Uiud7O3mHFmc6mxBiJz76krk1QUp2W/k0a/a+2Xn+VvyPE
  4     lPFWW2vHNA6NX8Iv0J8wWWaT3rAXnNZeRKLtc7LAoEjjNNgX7IxPdyn6WjKBkVP1
  5     TLhFkU36DYM3c75lQ6xSF3C60ebOb4fFGpbaDUuO796OhhJ8dCM69rwNeGxGvGhO
  6     UYkjsPlV0I2gd8lqq6Uiud7O3mHFmc6mxBiJz76krk1QUp2W/k0a/a+2Xn+VvyPE
  7     OoL7f6vUtdwPenkABQg01O0wmynHogAEhtV/YkxizN4Po0CZrfkQfXJf9P6C6h+Y

Router#show platform security tpm PCR 0,1,2,3,4,5,6,7 nonce 1234
Nonce: 1234

+--------------------------------------+
   Node location: node0_RP1_CPU0
+--------------------------------------+
Uptime: 157296
pcr-quote:
/1RRAAIANxXbvZplEA7+zS6IoWG/1He9m2IqRgBe+C3eQqkZAEjQAACHgAAAAAQAgAAAAAAAQAMvSAAAi2XSDRt29z6KQnG+vxCsdbbxDE5Eg+45DIGtzAsIadGbMK
pcr-quote-signature:
MGUCMQCUm63VUeXe25MSYerwr4CHIBnNqKqiBAN15fbl1dMbAOXoiBusdapVSUIIclODxQIM2c2pbgSocdR6SDri1repdEGl7uH6P8CtEWjX3MQnxg5ZNqpvgZBMBhogz9HVUQ==
pcr-index       pcr-value
  0     jkkHIFe0ce11YQouajSuN0jharqmSlK8dIr4j9TxXDb0PNVE9DjqO8vAh4tqHrl2
  1     wqoQkOVvOepm0+UwHGMmZwOYQl+B1R3TAaCnM3N5spA47EMWEI8cJDv77BvU02Ep
  2     UYkjsPlV0I2gd8lqq6Uiud7O3mHFmc6mxBiJz76krk1QUp2W/k0a/a+2Xn+VvyPE
  3     UYkjsPlV0I2gd8lqq6Uiud7O3mHFmc6mxBiJz76krk1QUp2W/k0a/a+2Xn+VvyPE
  4     cvkl6qjwrCJmgoEcSrEWyQuFLd4giBVxhsg8jrcziIEASKrF+2h+gT7EUso4ShIA
  5     d4Juh3B7g1fdaNbZdwNb9IqbKnzhgiYfSwLDQ8OQiYimampUpSljF7l5Siiwz6Xr
  6     UYkjsPlV0I2gd8lqq6Uiud7O3mHFmc6mxBiJz76krk1QUp2W/k0a/a+2Xn+VvyPE
  7     Et0OflnmhA4GmraclrDLfPcEgrYSlbAkwRNdyt3D1V+yVarLcowJNcvEzYdFwLBl
```

show platform security tpm integrity log boot

To display the boot chain integrity measurements recorded by the Trusted Platform Module (TPM) status, use the **show platform security tpm integrity log boot location** command in EXEC modeXR EXEC mode XR EXEC mode.

show platform security tpm integrity log boot location { *location* | **all** }

Syntax Description

location { *location* | **all** }	Specifies the location of TPM certificates.

Command Default

None

Command Modes

EXECXR EXEC

XR EXEC

Command History

Release	Modification
Release 25.4.1	This command was introduced.

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
system	read, write

Examples

This example shows how to view the boot chain integrity measurements. This command output is truncated.

```
Router#show  platform security tpm integrity log boot location 0/rp0/CPU0

+-------------------------------------+
   Node location: node0_RP0_CPU0
+-------------------------------------+
Uptime: 504480
Event Number: 1
Event Type: 03
PCR Index: 0
Event Digest Hash Algorithm: SHA1
Event Digest: AAAAAAAAAAAAAAAAAAAAAAAAAAA=
Event Data: U3BlYyBJRCBFdmVudDAzAAAAAAAAAgACAgAAAAsAIAAMADAAAA==
Event Number: 2
Event Type: 80000008
PCR Index: 0
Event Digest Hash Algorithm: SHA256
Event Digest: 8emdTrXnHLbHk7wXjWIMkF3/rKTUx7aJ7bFbqw5IEv4=
Event Digest Hash Algorithm: SHA384
Event Digest: 6OuqsUTGphX/NRZc82MBOefq1uLmac7i+kCjzmF5emFth2Fvd8NIAY4JruOOQMLM
Event Data: MrVWeEdXauXu7dTksv0FWh/3qy9lCrxrKWRy/2iR+xc=
Event Number: 3
```

```
Event Type: 80000008
PCR Index: 0
Event Digest Hash Algorithm: SHA256
Event Digest: mlrPXdkLmp++U11lPwBJZpnJ/qjOpVTxQljh8548Qxs=
Event Digest Hash Algorithm: SHA384
Event Digest: ioW380j8Ujk+EbQCX2Rz3OpJrjkh0ICSOCaJcm6cPdp0m05yma6tAqOk9FXCH145
Event Data: AEtoSI8ICqnAz53G1/XMD4qHH1qkuXmEAhLEUpw5ON4=
Event Number: 4
Event Type: 08
PCR Index: 0
Event Digest Hash Algorithm: SHA256
Event Digest: rvGvo1fKHlIH/+KxV/Oosl297rYw33B7xe15WCBHRPw=
Event Digest Hash Algorithm: SHA384
Event Digest: CTU1UADrh7g0egQYiVCMieVnJZisoH8WOt3pDGxY/LZK1QR815nPseDpodOQlQw0
Event Data: MQAtADQAMQAtADAALQBnAGIAYwAyADAAMwA3ADQAMQAtAHQAcABtAC0AcwAAAA==
Event Number: 5
Event Type: 80000008
PCR Index: 0
Event Digest Hash Algorithm: SHA256
Event Digest: mKowzTwX6/EzLO7DBKYmrcbdtqHYt4QMKWPzQk7YdC8=
Event Digest Hash Algorithm: SHA384
Event Digest: cV1V2ZmKahY+nYQ9wzt3oQgDELBN2PgTU7xaH0/yGpJYjKtK4eJlPvk9WnZS6kp4
Event Data: AFBTZgAAAAAAABYAAAAAAA==
```

show platform security tpm info ECC-sudi-certs

To display the information about the Cisco Secure Unique Device Identifier (SUDI) certificates stored in the Trusted Platform Module (TPM) at a specified location, use the **show platform security tpm info ECC-sudi-certs location** command in EXEC modeXR EXEC mode XR EXEC.

show platform security tpm info ECC-sudi-certs location { *location* | **all** }

Syntax Description

location { *location* | **all** }	Specifies the location of TPM certificates.

Command Default

None

Command Modes

EXECXR EXEC

XR EXEC

Command History

Release	Modification
Release 25.4.1	This command was introduced.

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
system	read, write

Examples

This example displays the information about the Cisco Secure IDevID certificates stored in the Trusted Platform Module (TPM) at a specified location.

```
Router#show platform security tpm info ECC-sudi-certs location 0/rp0/CPU0
-------------------------------------------
Node - 0/RP0/CPU0
-------------------------------------------

HA Sudi Root Cert:
-------------------------------------------
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: O=Cisco, CN=Cisco ECC Root CA
        Validity
            Not Before: Apr  4 08:15:44 2013 GMT
            Not After : Sep  7 16:24:07 2099 GMT
        Subject: O=Cisco, CN=Cisco ECC Root CA
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
```

```
                    04:7e:c0:c3:bc:d8:1b:c6:f3:67:91:4d:d6:78:8c:
                    e6:b5:75:39:04:7f:2f:fe:60:d0:ac:77:2a:d3:6d:
                    02:41:45:54:67:b0:58:b7:19:bf:cc:bd:4b:36:5c:
                    7b:5b:83:38:ec:a6:d7:4d:30:26:61:b3:4b:8b:ab:
                    5e:0e:15:26:3b:4c:88:ab:02:70:c9:22:37:02:50:
                    75:c0:d5:d4:48:34:c7:bf:58:53:fe:ae:cb:8f:73:
                    20:f5:06:5b:12:87:ca
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                A4:45:B6:2F:A3:31:B1:76:15:B0:0A:18:33:CA:F6:AD:4F:3D:28:04
    Signature Algorithm: ecdsa-with-SHA384
    Signature Value:
        30:65:02:31:00:f0:9b:71:dc:7b:40:56:9f:ff:61:a9:3a:ba:
        6d:f1:19:10:44:4f:88:f9:80:ff:a5:86:6f:13:89:c8:19:75:
        39:9e:0e:b6:e8:85:bb:9f:06:0d:07:31:11:ba:80:57:2b:02:
        30:08:b9:e0:52:29:8f:89:14:84:28:c7:27:80:1d:98:73:ea:
        97:2c:6b:31:e3:84:b7:ac:48:b1:d6:54:d5:49:35:54:ca:66:
        27:8f:7a:f6:e2:b1:1e:38:ab:8a:a5:f3:86

HA Sudi Sub CA Cert:
-------------------------------------------
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 5 (0x5)
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: O=Cisco, CN=Cisco ECC Root CA
        Validity
            Not Before: Apr  4 08:26:13 2013 GMT
            Not After : Sep  7 16:24:06 2099 GMT
        Subject: O=Cisco, CN=ACT2 ECC SUDI CA
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:8c:61:dc:fa:79:d2:31:0a:f8:ce:e0:11:cc:3c:
                    47:17:a4:c3:8b:de:df:ed:e1:aa:49:d0:ca:e6:68:
                    ac:56:9a:01:3f:43:70:c1:c9:9a:ce:cf:86:4e:24:
                    fe:52:ce:76:fc:12:ae:a3:82:65:69:9e:f8:72:79:
                    73:cc:12:27:90:fc:2d:b9:a8:36:6d:74:82:79:85:
                    49:85:c0:77:b1:5b:95:bd:88:92:29:51:22:d4:e2:
                    20:c7:ce:5d:b5:77:70
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            Authority Information Access:
                CA Issuers - URI:http://www.cisco.com/security/pki/certs/eccroot.cer
                OCSP - URI:http://pkicvs.cisco.com/pki/ocsp
            X509v3 Authority Key Identifier:
                A4:45:B6:2F:A3:31:B1:76:15:B0:0A:18:33:CA:F6:AD:4F:3D:28:04
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.9.21.1.19.0
                  CPS: http://www.cisco.com/security/pki/policies/index.html
            X509v3 CRL Distribution Points:
```

```
                Full Name:
                  URI:http://www.cisco.com/security/pki/crl/eccroot.crl
            X509v3 Subject Key Identifier:
                96:87:3A:D8:89:81:91:41:15:33:BF:E0:34:8F:20:8F:C2:BB:C3:96
    Signature Algorithm: ecdsa-with-SHA384
    Signature Value:
        30:66:02:31:00:cf:27:bd:bf:58:79:9b:fd:5b:01:44:94:d0:
        c4:30:4a:10:c3:09:12:47:5e:c7:3e:d5:3b:5b:a8:e2:51:d5:
        c6:4c:9a:1b:08:cc:d3:72:fc:0b:24:90:1a:08:80:d3:6d:02:
        31:00:93:70:c0:2b:19:01:c7:70:d8:c9:94:b8:53:3d:c1:e7:
        43:29:6e:b6:70:a7:13:d3:50:2a:96:9b:ba:84:c4:23:3b:9b:
        51:63:22:0f:7c:96:d7:dd:96:d3:c7:82:a3:ff

HA Sudi Cert:
--------------------------------------------
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            07:75:52:19:47:14:30:41:41:69
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: O=Cisco, CN=ACT2 ECC SUDI CA
        Validity
            Not Before: May 23 16:32:22 2025 GMT
            Not After : Sep  7 16:24:05 2099 GMT
       Subject: serialNumber=PID:8800-RP2-S SN:FOC2845N1BJ, O=Cisco, OU=TPM SUDI, CN=Cisco
 8800 Route Processor 2 (sZTP default) MAC:c4ab4dff83c0-0008800-RP2-S
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:0d:72:79:12:08:e2:b2:ea:15:17:d3:a6:aa:67:
                    4f:91:d4:83:86:6e:3c:6f:0a:9c:b2:7b:f8:61:bf:
                    8b:4c:70:c4:b3:ce:0c:76:3e:38:6b:55:48:29:41:
                    19:c9:56:8c:7a:63:42:bb:f2:1d:3b:b4:e0:35:c2:
                    e8:8b:30:ae:95:be:01:c6:25:48:ba:5b:f8:a1:e2:
                    f6:92:1d:b7:4b:12:b5:05:f5:b9:23:91:68:c6:42:
                    f3:e1:01:ab:f5:f4:f1
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Authority Key Identifier:
                96:87:3A:D8:89:81:91:41:15:33:BF:E0:34:8F:20:8F:C2:BB:C3:96
            X509v3 Certificate Policies:
                Policy: 2.23.133.11.1.1
                Policy: 2.23.133.11.1.2
            X509v3 Subject Alternative Name:
                othername: 1.3.6.1.5.5.7.8.4::<unsupported>, othername: Permanent
Identifier::<unsupported>
            X509v3 Subject Key Identifier:
                45:15:D3:60:67:89:0C:5F:89:14:DD:41:5C:E0:7E:36:61:D1:A0:FF
    Signature Algorithm: ecdsa-with-SHA384
    Signature Value:
        30:65:02:31:00:b6:dd:d7:f6:bc:c5:4b:f4:9d:b4:5b:6d:8d:
        cd:e7:81:26:f5:36:f9:ac:1c:23:5d:24:7d:c6:58:4a:bf:92:
        2c:0f:81:4c:75:3f:88:bc:94:21:ab:59:a6:a7:2f:63:b5:02:
        30:0d:f1:72:1b:93:eb:a2:0f:35:f9:2b:8d:9a:0f:49:00:11:
        50:fd:37:ef:a7:62:af:13:a2:15:2c:1c:79:d5:06:54:3c:73:
        33:13:9b:19:bd:cb:87:af:07:86:90:6d:40
```

show platform security tpm attest certificate

To display the cryptographic certificates used by the Trusted Platform Module (TPM) use the **show platform security tpm attest certificate** command in EXEC modeXR EXEC mode XR EXEC mode.

show platform security tpm integrity attest certificate CiscoECCIAK | CiscoECCSUDI location { *location* | **all** } [**nonce**]

Syntax Description

CiscoECCIAK	Displays the Cisco Attestation Identity Key (AIK) certificates stored in the TPM at specified location.
CiscoECCSUDI	Displays the Cisco Secure Unique Device Identifier (SUDI) certificates stored in the TPM at specified location.
location { *location* | **all** }	Specifies the location of TPM certificates.
nonce	Specifies the Nonce value to Hex String Format

Command Default

None

Command Modes

EXECXR EXEC

XR EXEC

Command History

Release	Modification
Release 25.4.1	This command was introduced.

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
system	read, write

Examples

This example shows how to display the Cisco Secure Unique Device Identifier (SUDI) certificates stored in the Trusted Platform Module (TPM) .

```
Router#show  platform security tpm attest certificate CiscoECCSUDI location 0/rp0/CPU0 nonce
 1234

+-------------------------------------+
   Node location: node0_RP0_CPU0
+-------------------------------------+
Nonce: 1234
Certificate name: Cisco ECC SUDI Root
-----BEGIN CERTIFICATE-----
MIIByDCCAU6gAwIBAgIBAzAKBggqhkjOPQQDAzAsMQ4wDAYDVQQKEwVDaXNjbzEa
MBgGA1UEAxMRQ2lzY28gRUNDIFJvb3QgQ0EwIBcNMTMwNDA0MDgxNTQ0WhgPMjA5
```

```
OTA5MDcxNjI0MDdaMCwxDjAMBgNVBAoTBUNpc2NvMRowGAYDVQQDExFDaXNjbyBF
Q0MgUm9vdCBDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABH7Aw7zYG8bzZ5FN1niM
5rV1OQR/L/5g0Kx3KtNtAkFFVGewWLcZv8y9SzZce1uDOOym100wJmGzS4urXg4V
JjtMiKsCcMkiNwJQdcDV1Eg0x79YU/6uy49zIPUGWxKHyqNCMEAwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFKRFti+jMbF2FbAKGDPK
9q1PPSgEMAoGCCqGSM49BAMDA2gAMGUCMQDwm3Hce0BWn/9hqTq6bfEZEERPiPmA
/6WGbxOJyBl1OZ4OtuiFu58GDQcxEbqAVysCMAi54FIpj4kUhCjHJ4AdmHPq1yxr
MeOEt6xIsdZU1Uk1VMpmJ4969uKxHjiriqXzhg==
-----END CERTIFICATE-----

Certificate name: Cisco ECC SUDI CA
-----BEGIN CERTIFICATE-----
MIIDETCCApagAwIBAgIBBTAKBggqhkjOPQQDAzAsMQ4wDAYDVQQKEwVDaXNjbzEa
MBgGA1UEAxMRQ2lzY28gRUNDIFJvb3QgQ0EwIBcNMTMwNDA0MDgyNjEzWhgPMjA5
OTA5MDcxNjI0MDZaMCsxDjAMBgNVBAoTBUNpc2NvMRkwFwYDVQQDExBBQ1QyIEVD
QyBTVURJIENBMHYwEAYHKoZIzj0CAQYFK4EEACIDYgAEjGHc+nnSMQr4zuARzDxH
F6TDi97f7eGqSdDK5misVpoBP0Nwwcmazs+GTiT+Us52/BKuo4JlaZ74cnlzzBIn
kPwtuag2bXSCeYVJhcB3sVuVvYiSKVEi1OIgx85dtXdwo4IBiTCCAYUwDgYDVR0P
AQH/BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwfQYIKwYBBQUHAQEEcTBvMD8G
CCsGAQUFBzAChjNodHRwOi8vd3d3LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY2Vy
dHMvZWNjcm9vdC5jZXIwLAYIKwYBBQUHMAGGIGh0dHA6Ly9wa2ljdnMuY2lzY28u
Y29tL3BraS9vY3NwMB8GA1UdIwQYMBaAFKRFti+jMbF2FbAKGDPK9q1PPSgEMFwG
A1UdIARVMFMwUQYKKwYBBAEJFQETADBDMEEGCCsGAQUFBwIBFjVodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvcG9saWNpZXMvaW5kZXguaHRtbDBCBgNV
HR8EOzA5MDegNaAzhjFodHRwOi8vd3d3LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kv
Y3JsL2VjY3Jvb3QuY3JsMB0GA1UdDgQWBBSWhzrYiYGRQRUzv+A0jyCPwrvDljAK
BggqhkjOPQQDAwNpADBmAjEAzye9v1h5m/1bAUSU0MQwShDDCRJHXsc+1TtbqOJR
1cZMmhsIzNNy/AskkBoIgNNtAjEAk3DAKxkBx3DYyZS4Uz3B50MpbrZwpxPTUCqW
m7qExCM7m1FjIg98ltfdltPHgqP/
-----END CERTIFICATE-----

Certificate name: Cisco ECC SUDI
-----BEGIN CERTIFICATE-----
MIIDYDCCAuagAwIBAgIKB3VSGUcUMEFBaTAKBggqhkjOPQQDAzArMQ4wDAYDVQQK
EwVDaXNjbzEZMBcGA1UEAxMQQUNUMiBFQ0MgU1VESSBDQTAgFw0yNTA1MjMxNjMy
MjJaGA8yMDk5MDkwNzE2MjQwNVowgaAxJjAkBgNVBAUTHVBJRDo4ODAwLVJQMi1T
IFNOOkZPQzI4NDVOMUJKMQ4wDAYDVQQKEwVDaXNjbzERMA8GA1UECxMIVFBNIFNV
REkxUzBRBgNVBAMTSkNpc2NvIDg4MDAgUm91dGUgUHJvY2Vzc29yIDIgKHNaVFAg
ZGVmYXVsdCkgTUFDOmM0YWI0ZGZmODNjMC0wMDA4ODAwLVJQMi1TMHYwEAYHKoZI
zj0CAQYFK4EEACIDYgAEDXJ5EgjisuoVF9OmqmdPkdSDhm48bwqcsnv4Yb+LTHDE
s84Mdj44a1VIKUEZyVaMemNCu/IdO7TgNcLoizCulb4BxiVIulv4oeL2kh23SxK1
BfW5I5FoxkLz4QGr9fTxo4IBWzCCAVcwDgYDVR0PAQH/BAQDAgXgMAwGA1UdEwEB
/wQCMAAwHwYDVR0jBBgwFoAULoc62ImBkUEVM7/gNI8gj8K7w5YwHQYDVR0gBBYw
FDAIBgZngQULAQEwCAYGZ4EFCwECMIHXBgNVHREEgc8wgcygcQYIKwYBBQUHCASg
ZTBjBgVngQUBAgRaNTM1NDREMjA6NTNkZWM1MmE0YjgwYTczYzViOWJjMDY5ZWM0
MDc5MTZiZjNiMzM4MDoxNmI5ZjllYTIxMTQxZmY4NWMwMjAzY2ZhODEwYzg5NzEw
YjRiOWQ0oFcGCCsGAQUFBwgDoEswSQxAODc5ZWYwMjUxNTlkYTVlMzUzZWEyZTNi
MDhjZGM0MjAzZDUyNzAxNTJjMThlYmRlYjA4Yjc5MzMxYTA3ODQ0ZAYFZ4EFDAEw
HQYDVR0OBBYEFEUV02BniQxfiRTdQVzgfjZh0aD/MAoGCCqGSM49BAMDA2gAMGUC
MQC23df2vMVL9J20W22NzeeBJvU2+awcI10kfcZYSr+SLA+BTHU/iLyUIatZpqcv
Y7UCMA3xchuT66IPNfkrjZoPSQARUP0376dirxOiFSwcedUGVDxzMxObGb3Lh68H
hpBtQA==
-----END CERTIFICATE-----
```