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 NCS 5500 Series Routers*.

show platform security integrity log

To display the security integrity logs for the router, use the **show platform security integrity log** command in XR 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

XR 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 attest

To allow the operator to cryptographically verify the Platform Configuration Registers (PCRs) and attest with the device Attestation Identity Key (AIK) , use the **show platform security attest** command in XR EXEC mode.

show platform security attest { **pcr** *0|1* { **location all** | | **trustpoint ciscoaik nonce** *nonce value* } | **certificate** { **ciscoaik** | | **ciscosudi** } }

Syntax Description

attest	The attest keyword is used with either pcr or certificate keywords.
pcr	The pcr keyword takes the index number 0 or 1 as an argument. PCRs return the pcr-index and pcr-value of the specified node.
certificate	The certificate keyword takes ciscoaik or ciscosudi as an argument.
ciscoaik	The ciscoaik keyword returns the Cisco AIK Root, Cisco AIK CA, and Cisco AIK certificates. The AIK is a Certificate Enrollment Specification used to certify the trustworthiness of a router.
ciscosudi	The ciscosudi keyword returns the Cisco SUDI Root, Cisco SUDI CA, and Cisco SUDI certificates. The Secure Unique Device Identifier (SUDI) is a secure device identity in an X.509v3 certificate that maintains the product identifier and serial number.
trustpoint	Cisco AIK certificate to be used for the PCR quote.
Optional keywords for **ciscoaik and ciscosudi**	• **json** • **location all** • **nonce** *nonce value*

Command Default

None

Command Modes

XR EXEC

Command History

Release	**Modification**
Release 7.4.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	**Operations**
system	read, write

Examples

This example shows the truncated output of the certificates used to attest the trustworthiness of a router:

```
RP/0/RP0/CPU0:NCS-540-C-LNT#show platform security attest certificate ciscoaik
Thu Apr 11 06:09:57.026 UTC

+--------------------------------------+
   Node location: node0_RP0_CPU0
+--------------------------------------+
Certificate name: Cisco AIK Root
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
-----END CERTIFICATE-----

Certificate name: Cisco AIK CA
-----BEGIN CERTIFICATE-----
MIIEXzCCA0egAwIBAgIJCsCKA1bCuHJDMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV

-----END CERTIFICATE-----

Certificate name: Cisco AIK
-----BEGIN CERTIFICATE-----
MIIEFjCCAv6gAwIBAgIDGGJ9MA0GCSqGSIb3DQEBCwUAMCkxFzAVBgNVBAMTDkF0

-----END CERTIFICATE-----
```

This example shows the pcr-quote, pcr-quote-signature, pcr-index, and pcr-value of the specified nonce.

```
RP/0/RP0/CPU0:NCS-540-C-LNT#show platform security attest PCR 0 trustpoint ciscoaik nonce
4678
Thu Apr 11 12:58:41.963 UTC
Nonce: 4678

+--------------------------------------+
   Node location: node0_RP0_CPU0
+--------------------------------------+
Uptime: 1224771
pcr-quote: /1RDR4AYACCkyXSBYFKZw5Nurif7DYQRMrBTg6q91heoKFZW0kp0FQACRngAAAAABX7FPQAAA97/
////AQAAACQAAAALAAAAAQALAwEAAAAgrE798LlOkKp1kryIv50kG0/V461IQutuSVgCUwjG8q4=
pcr-quote-signature:
X3xo0M5DLWeJI3WGOM1XRLkE5sKyp9oEo0+EX8x5s13qdhdIe---<truncated>--KhmwAV8ETdxfgbccPYS6A==
pcr-index       pcr-value
  0            sL3H+Em2xzxXrNUoDF+kC47IXxN4V/d/7hYUXApXNoY=
```