



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 Routers* and *System 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](#)

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

<i>ownership-voucher-path</i>	Path to the .tar file containing the Ownership Vouchers (OV) and Authenticated Variable (AV) to securely transfer device ownership
location { <i>location</i> 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 <i>key</i>		Appends certificates or hashes to Extensible Firmware Interface (EFI) to one of the following keys: <ul style="list-style-type: none"> • KEKCustomer—Key Exchange Key Customer • PKCustomer—Platform Key Customer • dbCustomer—Signature and key database Customer • dbxCustomer—Forbidden signature and key database Customer
update <i>key</i>		Removes or replace certificates or hashes in EFI for one of the following keys: <ul style="list-style-type: none"> • KEKCustomer—Key Exchange Key Customer • PKCustomer—Platform Key Customer • dbCustomer—Signature and key database Customer • dbxCustomer—Forbidden signature and key database Customer
<i>authenticated-variable-file-path</i>		Path to the AV file
GUID <i>av-customer-guid</i>		Cisco-provided Global Unique Identification number (GUID)
location { <i>location</i> 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
```

show platform security boot mode

```
=====  
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	Parameter	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 <i>location-name</i>		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	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 variable customer