



Cisco TrustSec Commands

This module describes the commands used to configure Cisco TrustSec (CTS).

For detailed information about CTS concepts, configuration tasks, and examples, see the *Cisco TrustSec L2 and L3 Security Group Tag Propagation* chapter in *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

- [hw-module cts-enable all, on page 2](#)
- [show controllers NP configSram, on page 3](#)

hw-module cts-enable all

To enable the Cisco TrustSec (CTS) for all ASR 9000 Enhanced Ethernet Line Cards use the **hw-module cts-enable all** command in Global Configuration mode.

hw-module cts-enable all

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Global Configuration mode

Command History	Release	Modification
	Release 5.2.0	This command was introduced.

Usage Guidelines The CTS solution allows you to intelligently control access to corporate data, allowing access control policies to be applied uniformly anywhere in the network. Use the **hw-module cts-enable all** command to manually enable an interface on the device for CTS, so that the device can propagate the CTS packet throughout the network.

Task ID	Task	Operation ID
	root-lr	read, write

Example

The following example shows how to enable CTS.

```
RP/0/0RP0RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:IMC0(config)#hw-module cts-enable all
```

Related Commands	Command	Description
	show controllers NP configSram, on page 3	Indicates if CTS is enabled for a device.

show controllers NP configSram

To command to check if CTS tag is enabled for a given port or not use the **show controllers NP configSram** command in EXEC mode.

```
show controllers NP configSram portnum {all | {np0 | np1}} location node-id}
```

Syntax Description	
<i>portnum</i>	Represents the port number and the value ranges from 0 to 4294967295.
{all {np0 np1}}	Indicates if results for all nodes or only the designated node must be included in the output.
location <i>node id</i>	Clears detailed adjacency statistics for the designated node. The node-id argument is entered in the rack/slot/module notation.

Command Default No default behavior or values

Command Modes EXEC mode

Command History	Release	Modification
	Release 5.2.0	This command was introduced.

Usage Guidelines Use the command to check if CTS tag is enabled for a given port or not.

Task ID	Task ID	Operation
	sonet-sdh, dwdm, interface, drivers	read

Example

This example shows the configuration with CTS-enabled for the specified port.

```
RP/0/RSP0/CPU0:IMC0#show controllers NP configSram 16 np1 location
0/0/CPU0
Step 4
Node: 0/0/CPU0:
-----
NP1 Port=16 Port Config SRAM
-----
0xce400000 00000000 00201005 9c66eb5f
-----
Field Name #Bits Value
-----
ELMI Enable 0x0
CFM Enable 0x0
EFM Enable 0x0
EFM Block 0x0
EFM Loopback 0x0
LLDP Enable 0x0
Sat Port Uses MACinMAC Encaps 0x0
Ingress MAC Accounting 0x0
UDLD Enable 0x0
```

```

MPLS Racetrack Enable 0x1
L2 Racetrack Enable 0x1
Ipv4 Racetrack Enable 0x1
IPV6 Racetrack Enable 0x1Satellite NP Port 0x4c45
Bundle NP Port of Sat 0x494d
Port Sampled Span 0x0
Port Sampled Span Rate 0x0
Satellite Mode Hub & Spoke 0x0
satellite ingress unicast state 0x0
Member of ICL Bundle 0x0
Port CTS Enable 0x1
Router ID 0x9c66eb5f
MPLS Propagate TTL 0x1
Global Bundle L2 LB 0x0
Egr QoS ACL Bypass 0x1
Global Hash Rotate Value 0x0
MT Enable 0x0
Qos before PBR 0x0
MPLS Global LSR, FRR match 0x1
MPLS LSR 0x1
MPLS Global FRR 0x0
My MAC 0x0

```

Related Commands

Command	Description
hw-module cts-enable all, on page 2	Enables Cisco TrustSec (CTS).