



Cisco TrustSec (CTS)

Cisco TrustSec is an umbrella term for security improvements to Cisco network devices based on the capability to strongly identify users, hosts and network devices within a network. TrustSec provides topology independent and scalable access controls by uniquely classifying data traffic for a particular role. TrustSec ensures data confidentiality and integrity by establishing trust among authenticated peers and encrypting links with those peers.

The key component of Cisco TrustSec is the [Cisco Identity Services Engine](#). It is typical for the Cisco ISE to provision switches with TrustSec Identities and Security Group ACLs (SGACLs), though these may be configured manually.

To configure Cisco Trustsec on the switch, see the publication, “*Cisco TrustSec Switch Configuration Guide*” at the following URL:

<http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html>

Release Notes for Cisco TrustSec General Availability releases are at the following URL:

http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html

Additional information on the Cisco TrustSec Solution, including overviews, datasheets, and case studies, is available at:

<http://www.cisco.com/en/US/netsol/ns1051/index.html>

[Table 1](#) lists the TrustSec features to be eventually implemented on TrustSec-enabled Cisco switches. Successive general availability releases of TrustSec will expand the number of switches supported and the number of TrustSec features supported per switch.

See the section, “[Hardware Supported](#)” for information on TrustSec features supported on switching modules.

Table 1 Cisco TrustSec Key Features—TrustSec 1.0 General Availability 2010 Release

Cisco TrustSec Feature	Description
802.1AE Tagging (MACSec)	<p>Protocol for IEEE 802.1AE-based wire-rate hop-to-hop layer 2 encryption.</p> <p>Between MACSec-capable devices, packets are encrypted on egress from the transmitting device, decrypted on ingress to the receiving device, and in the clear within the devices.</p> <p>This feature is only available between TrustSec hardware-capable devices.</p>
Endpoint Admission Control (EAC)	EAC is an authentication process for an endpoint user or a device connecting to the TrustSec domain. Usually EAC takes place at the access level switch. Successful authentication and authorization in the EAC process results in Security Group Tag assignment for the user or device. Currently EAC can be 802.1X, MAC Authentication Bypass (MAB), and Web Authentication Proxy (WebAuth).
Network Device Admission Control (NDAC)	NDAC is an authentication process where each network device in the TrustSec domain can verify the credentials and trustworthiness of its peer device. NDAC utilizes an authentication framework based on IEEE 802.1X port-based authentication and uses EAP-FAST as its EAP method. Successful authentication and authorization in NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption.
Security Group Access Control List (SGACL)	A Security Group Access Control List (SGACL) associates a Security Group Tag with a policy. The policy is enforced upon SGT-tagged traffic egressing the TrustSec domain.
Security Association Protocol (SAP)	After NDAC authentication, the Security Association Protocol (SAP) automatically negotiates keys and the cipher suite for subsequent MACSec link encryption between TrustSec peers. SAP is defined in IEEE 802.11i.
Security Group Tag (SGT)	An SGT is a 16-bit single label indicating the security classification of a source in the TrustSec domain. It is appended to an Ethernet frame or an IP packet.
SGT Exchange Protocol (SXP)	Security Group Tag Exchange Protocol (SXP). Devices that are not TrustSec-hardware capable can, with SXP, receive from the Cisco ACS, SGT attributes for authenticated users or devices then forward the sourceIP-to-SGT binding to a TrustSec-hardware capable device for tagging and SGACL enforcement.

Flexible MACsec Replay Protection

Flexible MACsec replay protection feature provides flexible and configurable out-of-order mode replay protection window on CTS links. You can configure MACsec window size, as defined by the number of out-of-order frames that are accepted. This value is used while installing the security associations in the MACsec. A value of 0 means that frames are accepted only in the correct order.

**Note**

The MACsec replay protection window configuration change will come into affect during a shut/no-shut or link flap.

The *macsec replay-protection window-size* command would be visible on all CTS supported ports, however value range option would be restricted to <0-0> for non-supported cases.

To configure MACsec replay protection window size, perform this task:

<i>switch1(config-if)# macsec replay-protection window-size value</i>	Enables replay protection, and configure the window size in number of frames. The range is from 0 to 4294967295. The default window size is 0.
---	--

This example shows how to verify whether MACsec replay protection is supported on your switch:

```
switch1(config-if)# macsec replay-protection window-size ?
<\<0-4294967295> window is the number of frames (packets)
```

This example shows how to fis the MACsec replay protection window size:


```
switch1(config-if)# macsec replay-protection window-size 2000
Term1#sh running-config interface t4/1
Building configuration...
!
interface TenGigabitEthernet4/1
 ip address 4.1.1.1 255.255.255.0
 macsec replay-protection window-size 2000
 cts dot1x
end
```

Hardware Supported

Table 72-2 lists the level of Cisco TrustSec supported switching modules. The table is derived from the white paper, “Cisco Catalyst 6500 Series with Supervisor Engine 2T: Enabling Cisco TrustSec with Investment Protection,” located at the following URL:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-658388.html

Table 72-2 Switching Module Support Levels for Cisco TrustSec

Cisco TrustSec Support Level	Description	Line Card
 Note Only the Security Association Protocol (SAP) for key negotiation in the CTS manual mode is supported on Cisco TrustSec Capable.	Supports full Cisco TrustSec capabilities with hardware acceleration for Security Group Tag imposition and IEEE 802.1AE MACsec	Supervisor Engine 2T, and all 6900 Series line cards
Cisco TrustSec Aware	Does not support Security Group Tag imposition or IEEE 802.1AE MACsec. These line cards are capable of understanding forwarding decisions, which include the Security Group Tag information. This allows them to forward traffic to a Cisco TrustSec capable line card for egress.	<ul style="list-style-type: none"> WS-X6816-10T-2T, WS-X6716-10T WS-X6816-10G-2T, WS-X6716-10GE
Not Capable of Using Cisco TrustSec	Do not support Security Group Tag imposition or IEEE 802.1AE MACsec, nor can they interpret forwarding decisions with Security Group Tag information.	<ul style="list-style-type: none"> WS-X6824-SFP-2T WS-X6724-SFP WS-X6848-SFP-2T WS-X6748-SFP WS-X6848-TX-2T WS-X6748-GE-TX WS-X6704-10G WS-X6148 series (all)

For all Cisco TrustSec hardware platform and feature support information, please see TrustSec Product Bulletins at the following URL:

<http://www.cisco.com/en/US/netsol/ns1051/index.html>