



## Configuring Cisco TrustSec

---

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 peer and encrypting links with those peers.

To configure Cisco Trustsec on the Cisco Catalyst 6500 Series switches, 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 1.0 General Availability 2010 Release are at the following URL:

[http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/cts1\\_0.html](http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/cts1_0.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 network devices. Successive general availability releases of TrustSec will expand the number of network devices supported and the number of TrustSec features supported per device. See the section, “**Hardware Supported**” for information on which TrustSec features are implemented.

**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)	<p>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).</p>
Network Device Admission Control (NDAC)	<p>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.</p>
Security Group Access Control List (SGACL)	<p>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.</p>
Security Association Protocol (SAP)	<p>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.</p>
Security Group Tag (SGT)	<p>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.</p>
SGT Exchange Protocol (SXP)	<p>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.</p>

## Hardware Supported

Table 2 lists the TrustSec features supported by platform on the release date of Cisco IOS 12.2(33) SXI4.

**Table 2** Feature and Platform support—TrustSec 1.0 General Availability 2010 Release

Hardware	Software Release	TrustSec Feature Introduced
Catalyst 3560 Series	Cisco IOS 12.2 (53) SE	EAC; SXP
Catalyst 3750 Series	Cisco IOS 12.2 (53) SE	EAC; SXP
Catalyst 4500 Series	Cisco IOS 12.2 (50) SG5	EAC; SXP
Catalyst 6500 Series	Cisco IOS 12.2(33) SXI3 <sup>1</sup>	EAC; SXP; NDAC (no SAP)
Nexus 7000 Series	Cisco NX-OS 4.2.1	EAC; SXP; NDAC; SGACL; MACSec

1. Cisco TrustSec was implemented on the Catalyst 6500 Series in SXI3, but announced as generally available in SXI4.

