Overview of Release Notes for Cisco TrustSec General Deployability Releases

November 30, 2011

Information on the Cisco TrustSec Solution, including overviews, datasheets, and case studies, is available at the following URL:

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

Table 1 lists the TrustSec features to be eventually implemented on TrustSec 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 "Hardware Supported" sections for information on the TrustSec features that are implemented on which hardware platforms per release.

The *Cisco TrustSec Switch Configuration Guide* is located at the following URL:

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

Table 1 Cisco TrustSec Key Features

Cisco TrustSec Feature	Description
802.1AE Encryption (MACSec)	Protocol for IEEE 802.1AE-based wire-rate, hop-to-hop, Layer 2 encryption. 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. This feature is only available between 802.1AE-capable devices.
Endpoint Admission Control (EAC)	EAC is an authentication process for an endpoint user or a device connecting to the TrustSec domain. Usually EAC is configured 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).

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table 1 Cisco TrustSec Key Features

Cisco TrustSec Feature	Description
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 the 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 a NIST-allowed Cisco proprietary key exchange protocol. The protocol description is available under a Non-disclosure Agreement. To view protocol details, see the following URL: http://www.cisco.com/web/strategy/government/protocol_supporting_cisco_trusted_security.html
802.1X-REV	IEEE 802.1x-REV is an industry standard host authentication, and key negotiation protocol for host-to-switch 802.1AE encryption. Replaces SAP.
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.

Chronological List of Releases

This is a chronological list of the Cisco TrustSec General Availability releases starting with Release 1.6:

- 2010 Jun 09 —Release 1.0
- 2011 Sep 08 —Release 1.99
- 2011 Nov 30 —Release 2.0
- 2012 Jul 13 —Release 2.1
- 2013 Mar 01 —Release 3.0

Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://tools.cisco.com/RPF/register/register.do

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

This document is to be used in conjunction with the *Catalyst 6500 Series Cisco IOS Software Configuration Guide* and the *Catalyst 6500 Series Cisco IOS Command Reference* publications.