CHAPTER 2

Configuring the Cisco TrustSec Solution

Revised: July 13, 2012, OL-22192-01

This chapter includes the following topics:

Configuration Overview

This guide documents elementary Cisco TrustSec configuration procedures for Cisco Catalyst switches and includes a TrustSec command reference.

For network-wide deployment configurations, see the section, "Cisco TrustSec Configuration How-to Documents."

A network-wide deployment includes the configuration, interoperability, and management of multiple devices, which may include the Cisco Identity Services Engine (Cisco ISE), The Cisco Secure Access Control System (Cisco ACS), Cisco IP Telephones, Cisco routers, Cisco network appliances, etc.

White papers and presentations explaining the Cisco TrustSec Solution are at the following URL: http://www.cisco.com/en/US/netsol/ns1051/index.html

Cisco TrustSec Configuration How-to Documents

A series of "How-to" configuration documents provides deployment guidelines and best practices for proven network architectures in complex scenarios. Find all Cisco TrustSec "How-To" documents at the following URL:

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

TrustSec 2.1 Configuration How-to Guide topics include the following:

- Introduction
- Planning and Pre-Deployment Checklist
- ISE Base Configuration: ISE Bootstrapping
- Adding ID Stores and Creating Authentication
- Global Switch Configuration

- Base configuration for the Wireless LAN Controller
- Phased Deployment Overview
- Monitor Mode
- Migrating from Monitor Mode
- Low Impact Mode
- Closed Mode
- ISE Profiling Services
- ISE Base Configurations: Promiscuous VMware
- Central Web Authentication
- User Authentication and Authorization to Multiple Active Directory Domains
- ISE Deployment Type and Guideline
- Using Certificates to Differentiate Access
- On-boarding and Provisioning
- Server to Server Segmentation using Security Group Access
- Deploying EAP Chaining with AnyConnect NAM and Cisco ISE
- Failed Authentications & Authorizations

Supported Hardware and Software

For a list of TrustSec supported hardware and software per TrustSec release, see, *Release Notes for Cisco TrustSec General Availability Releases* at the following URL: http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html

See also, the Release Notes, Configuration Guides, and Command References for your device.

Prerequisites for Cisco TrustSec

The following are the prerequisites for establishing a TrustSec network with Catalyst switches:

- TrustSec software on all network devices
- Connectivity between all network devices
- Network availability of the Cisco Secure ACS 5.1, or Cisco ISE operating with a TrustSec license
- Directory, DHCP, DNS, certificate authority, and NTP servers functioning in the network

Cisco TrustSec Guidelines and Limitations

Cisco TrustSec has the following guidelines and limitations for Catalyst switches:

- AAA for Cisco TrustSec uses RADIUS and is supported only by the Cisco Secure Access Control System (ACS), version 5.1 or later.
- You must enable the 802.1X feature globally for Cisco TrustSec to perform NDAC authentication. If you disable 802.1X globally, you will disable NDAC.
- Cisco TrustSec is supported only on physical interfaces, not on logical interfaces.
- Cisco TrustSec does not support IPv6 in the releases referenced in this guide.
- If the default password is configured on a switch, the connection on that switch should configure the password to use the default password. If the default password is not configured on a switch, the connection on that switch should also not configure a password. The configuration of the password option should be consistent across the deployment network.
- Configure the **retry open timer** command to a different value on different switches.

Default Settings

Table 2-1 lists the default settings for Cisco TrustSec parameters.

Table 2-1 Default Cisco TrustSec Parameters

Parameters	Default
Cisco TrustSec	Disabled.
SXP	Disabled.
SXP default password	None.
SXP reconciliation period	120 seconds (2 minutes).
SXP retry period	60 seconds (1 minute).
Cisco TrustSec Caching	Disabled.

Additional Documentation

Release-Specific Documents

Release-Specific Document Title	TrustSec Topics
Release Notes for Cisco TrustSec General Availability Releases	• Open and resolved caveats • Current hardware and software support

Platform-Specific Documents

Platform-Specific Document Title	TrustSec Topics
Catalyst 3000 Series Switches	
Release Notes for Catalyst 3560 and 3750 Switches	Open and resolved caveats; supported features
Catalyst 3560 Software Configuration Guides	802.1x configuration procedures
Catalyst 3750-E and 3560-E Switch Software Configuration Guide	
Cisco Catalyst 3560-X Series Switches Software Configuration Guides	
Catalyst 3750 Metro Series Switches Software Configuration Guides	
Cisco Catalyst 3750-X Series Switches Software Configuration Guides	
Catalyst 4500 Series Switches	
Cisco Catalyst 4500 Series Switches Release Notes	Open and resolved caveats, supported features
Catalyst 4500 Series Switches Software Configuration Guides	802.1x configuration procedures
Catalyst 6500 Series Switches	
Cisco Catalyst 6500 Series Switches Release Notes	Open and resolved caveats, supported features
Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide	802.1x configuration procedures
Catalyst 6500 Release 12.2SY Software Configuration Guide	
Catalyst 6500 Release 15.0SY Software Configuration Guide	
Nexus 7000 Series Switches	
Cisco Nexus 7000 Series Switches Release Notes	Open and resolved caveats
Cisco Nexus 7000 Series Switches Configuration Guides	• TrustSec feature configurations for Cisco Nexus 7000 series switches, Release 4.1 and later • 802.1X configuration procedures
Cisco Secure Access Control System and Cisco Identity Services Engine	
Cisco Secure Access Control System Release Notes	Open and resolved caveats

Platform-Specific Document Title	TrustSec Topics
Cisco Secure Access Control System End-User Guides	TrustSec configurations for Cisco ACS 5.1 and later
Cisco Identity Services Engine	TrustSec Configurations. TrustSec is referred to as SGA, or Security Group Access in ISE documentation.

Cisco IOS TrustSec Documentation Set

Cisco IOS Document Title
Cisco IOS Security Configuration Guide: Securing User Services, Release 12.2SX
Securing User Services Configuration Guide Library, Cisco IOS Release 15SY