



Release Notes for Cisco TrustSec 1.0 General Deployability 2010 Release

Published: June 9, 2010

The most current version of this document is available on Cisco.com at the following URL:
www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html

Contents

This document contains the following sections:

- [Introduction, page 1](#)
- [Caveats, page 2](#)
- [Related Documentation, page 4](#)

Introduction

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>

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>

For an explanation of Cisco TrustSec features, see [Table 1](#) in the “[Overview of Release Notes for Cisco TrustSec General Deployability Releases](#)”



Americas Headquarters:

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

Supported Hardware and Software

For a complete table of features, platforms, IOS images, and servers supported for the TrustSec 1.0 release, please see the Platform Support Matrix in the *Cisco TrustSec 1.0 Product Bulletin* at the following URL:

http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns1051/product_bulletin_c25-616556.html

Caveats

Open Caveats - Trustsec 1.0 General Availability 2010 Release

Cisco Secure Access Control System (ACS)

- [CSCte75993](#)—ACS sends the same server list name and gen-ID when NAD switches ACS

Symptom: A Catalyst 6500 device will initially attempt to access a wrong ACS server, and later will continue to show that wrong server as its primary destination for TrustSec RADIUS services.

Conditions: If the server config is modified to point to a different ACS, the device is not able to recognize that a new server list has been updated from the new server:

- Device is configured with Server A
- Env-data download from Server A returns server list named "ACSServerList1" with Server A in it
- Device's private list now contains Server A
- Server A is brought down
- Device config changed - Server A is replaced with Server B
- Server A is marked DEAD on the device's private list
- Env-data download refresh sent to Server B (public list)
- Server B returns same server list named "ACSServerList1" with same gen-ID
- Since server list name is identical and gen-ID did not change, device sees no need to download the server info and never acquires info for Server B
- Device ends up with Server A in its private list

The Catalyst 6500 gives priority to private server list over the public list, so it will attempt to use it without knowing that it is the wrong one.

Workaround: The Catalyst 6500 does have server-keep-alive test where the device will eventually detect that the private server is DEAD, it will switch to the correct configured RADIUS server, but in the "show" command, the wrong private server will remain.

In order to work-around the wrong configuration in the private list, the user should remove the Private server list and invoke a new Environment Data request.

Cisco Nexus 7000 Series Switches

Identifier	Technology	Description
CSCso34820	CTS	CTS: "show cts interface" o/p shows interfaces when module is not Online
CSCsq41219	CTS	Match IOS priorities for IP-SGT maps learnt via various methods
CSCsu54644	CTS	Need to accept multiple RBACLs per SGT, DGT cell downloaded from ACS
CSCsv67814	CTS	CTS SGT : Inconsistent programming of IP-SGT map with SVIs
CSCsw30353	CTS	CTS : 'ERROR: CTS is not supported on this interface'
CSCtg07773	CTS	Client "\"sal\"": skipping delete rnh - not found observed when toggle sxp Requires Caveat in Release Note documents, unless there is a quick fix
CSCtg10086	CTS	cts timeout in respond to ethpm message

Resolved Caveats

Cisco Catalyst 6500 Series Switches

Identifier	Technology	Description
CSCsz23686	CTS	"cts dot1x" command configured incorrectly on the interfaces.
CSCsz93221	CTS	During link-flap error recovery, active Sup5 detected data structure err Symptom: A Cisco switch may report the following error message: %UTIL-3-TREE: Data structure error--attempt to remove an unthreaded node from a tree Conditions: This issue is seen when dot1x is configured on the device. Workaround: There is no known workaround.
CSCta49126	CTS	TB on W2.2 image with W2.clix(IPv6Learning Capable) having SXP conn. b/w
CSCtb40877	CTS	Auth-mgr does not remove the auth session on removing cts dot1x from int
CSCtc12860	CTS	config gets applied in interface range sub-mode '@syntax check mode'
CSCtg23769	CTS	PAC does not get provisioned if switch has a very old PAC

Related Documentation

Release-Specific Documents

Release-Specific Document Title	TrustSec Topics
Cisco TrustSec Switch Configuration Guide	<ul style="list-style-type: none"> TrustSec feature configurations for Cisco Catalyst series switches System error messages
Release Notes for Cisco TrustSec 1.0 General Availability 2010 Release	<ul style="list-style-type: none"> Open and resolved caveats Current hardware support status

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
Catalyst 3560 Software Configuration Guide, Release 12.2(52)SE	802.1x configuration procedures
Catalyst 3750 Switch Software Configuration Guide, 12.2(52)SE	
Catalyst 4500 Series Switches	
Release Note for the Catalyst 4500 Series Switch, Cisco IOS, 12.2EW and 12.2SG	Open and resolved caveats
Catalyst 4500 Series Switch Software Configuration Guide, 12.2(53)SG	802.1x configuration procedures
Catalyst 6500 Series Switches	
Catalyst 6500 Series Release Notes for Cisco IOS Release 12.2(33)SXH and Later Releases	Open and resolved caveats
Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide	802.1x configuration procedures
Nexus 7000 Series Switches	
Cisco Nexus 7000 Series Switches Release Notes	Open and resolved caveats
Cisco Nexus 7000 Series Switches Configuration Guides	<ul style="list-style-type: none"> TrustSec feature configurations for Cisco Nexus 7000 series switches, Release 4.1 and more recent 802.1X configuration procedures
Cisco Secure Access Control System	

Platform-specific Document Title	TrustSec Topics
Cisco Secure Access Control System Release Notes	Open and Resolved caveats
Cisco Secure Access Control System End-User Guides	TrustSec configurations for Cisco ACS 5.1 and more recent

Cisco IOS Software Documentation Set

Cisco IOS Document Title	TrustSec Topics
Cisco IOS Security Configuration Guide: Securing User Services	802.1x configuration procedures
Cisco IOS Security Command Reference	Syntax and usage guidelines for TrustSec-specific and related commands

