# cisco.



### Wireless TrustSec Deployment Guide

Introduction 2Pre-requisite 2Requirements 2Components Used 2Conventions 2Feature Overview 2Implementation 3Workflow 4Wireless TrustSec Support on WLC 8.4 5Use case for Wireless TrustSec Deployment 5CLI Commands for Wireless TrustSec Configuration 24

Revised: October 3, 2024

# Introduction

This document introduces Wireless TrustSec feature and provides general guidelines for its deployment. The purpose of this document is to:

- Provide an overview of Wireless TrustSec feature
- Highlight supported Key Features
- · Provide details on deploying and managing Wireless TrustSec on WLC

The focus of this guide is only on Wireless TrustSec features.

For deep dive on wired TrustSec, please refer to the following:

http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html

http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/design-guide-listing.html

# **Pre-requisite**

Customers must have AireOS 8.0 or higher release on a Wireless LAN Controller in order to upgrade to the 8.4 code.

# **Requirements**

There is no specific requirement for this document.

# **Components Used**

The information in this documentwas created from devices in a specificlab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

# **Conventions**

Refer to Cisco Technical Tips Conventions for more information on document conventions.

# **Feature Overview**

The Cisco TrustSec (CTS) architecture provides an end-to-end secure network where each entity is authenticated and trusted by its neighbors and communication links secured that help ensure data confidentiality, authenticity and integrity protection. In addition, CTS facilitates to create a consistent and unified set of policies across network. The following sections describe specific aspects related to CTS infrastructure support on AireOS WLC platforms.

# Implementation

Figure 1: Wireless TrustSec Solution



Every end point that touches the TrustSec domain gets classified by ISE based on end user identity like role, device-type (other client attributes) and is associated with a unique tag called SGT(Security Group Tag) that is then shared with the device that requested the client authentication upon successful authentication. This allows grouping of clients based on client identity attributes thereby reducing the number of Access Control Entities (ACE) considerably. A major benefit to SGACL use is the consolidation of access ACEs and the operational savings involved with maintenance of those traditional access lists.

Trustsec solution is realized across the following three distinct phases within TrustSec domain:

- Client classification at ingress by a centralized policy database (ISE) and assigning unique SGT to client based on client identity attributes like role and so on.
- Propagation of IP to SGT binding to neighboring devices using SXPv4 and / or inline tagging methods.
- SGACL policy enforcement: AP will be enforcement point for central / local switching (central authentication).

### SXPv4 on AP

WLC still supports SXPv2 Speaker mode to propagate IP to SGT bindings to neighboring devices, we don't support SXPv4. AP will support SXPv4 listener and speaker mode.

### **CTS PAC Provisioning and Device Enrollment**

Any device that participates in the CTS network requires it to be authenticated and trusted. In order to facilitate the authentication process new devices connected to CTS network under goes an enrollment process where in the device obtains the credentials that is specifically needed for CTS device authentication and obtain general CTS environment information.

The WLC device enrollment is initiated by the WLC as part of PAC provisioning with ISE server. The WLC will initiate EAP-FAST and obtains a PAC. This is accomplished by using the infrastructure of LOCAL-EAP EAP-FAST PAC-provisioning. The PAC obtained uniquely maps to the Device ID. If the Device ID changes, PAC data associated with the previous Device ID is removed from the PAC store. PAC provisioning is triggered when a radius server instance is enabled to provision the PAC.

In case of High Availability (HA) setup, PACs will be synced to the standby box.

### **Environment Data**

CTS Environment data is a set of information or attributes that helps the device to perform CTS related functions.

The device (AirOS WLC) acquires the environment data from the authentication server when the device first joins a Cisco Trust Sec domain by sending a secure radius access-request. The authentication server returns RADIUS Access-Accept with attributes including

environment expiry timeout attributes. This is the time interval that controls how often the Cisco Trust Sec device must refresh its environment data.

### **Inline Tagging**

Inline tagging functionality is a transport mechanism by which a wireless controller or an access point understand the source SGT (S-SGT). It covers the following two types:

- **Central switching**: For centrally switched packets, WLC performs inline tagging for all packets sourced from wireless clients that reside on the WLC by tagging it with Cisco Meta Data (CMD) tag. For packets inbound from the DS, inline tagging also involves WLC will strip the packet of the header and send it to the AP over CAPWAP for the AP to learn the S-SGT tag. SGACL enforcement will happen at the AP.
- Local switching: For transmitting ,locally switched traffic AP performs inline tagging for packets sourced from clients that reside on the AP. When receiving traffic, AP will handle both locally switched and centrally switched packets and use S-SGT tag for packets and apply the SGACL policy.

With wireless TrustSec enabled on WLC the choice of also enabling and configuring SXP to exchange tags with the switches is optional and both modes i.e. SXP speaker mode and inline tagging are supported; however there is no use case to have both SXP and wireless TrustSec on AP to be enabled simultaneously

### Workflow

Before a WLC can start downloading SGACL policies from ISE, it must initiate PAC (Protected Access Credential) provisioning over an EAP-FAST TLS tunnel. This will be used to download SGACL as required, based on authenticated client SGT tag. Currently, ISE supports SGACL policy download for given destination SGT (D-SGT) from all known source SGT (S-SGT). When a wireless client is authenticated by ISE, WLC receives a SGT associated with the client. WLC will treat client SGT as D-SGT and initiate download of SGACL policy names for the destination from ISE. The policy names returned will be all possible / known S-SGTs paired with the specific client D-SGT. These policies associated with the D-SGT are cached on WLC and pushed to the AP associated with the client.

#### Figure 2: Simplified ACL management for Inter/Intra VLAN traffic



Client classification happens at ingress by centralized policy database (ISE) that assigns a unique S- SGT to client based on client identity as per policy rules. SGACL download and policy is enforced (associated with the D-SGT) on the egress side.

- SGACL enforcement for local and central switched traffic happens on AP and not on WLC.
- In a flex mode AP doing local authentication, enforcement point will be the AP.

#### Figure 3: Ingress Classification, Egress enforcement



### Wireless TrustSec Support on WLC 8.4

Feature	Platform
Inline SGT tagging and SG-ACL enforcement	17xx, 27xx, 37xx, 18xx, 28xx, 38xx, 5520 and 8540
SXPv2	5520, 8540, 8510, 7510, vWLC, 5508, WISM2, 2504
SXPv4	17xx, 27xx, 37xx, 18xx, 28xx and 38xx

### Use case for Wireless TrustSec Deployment

The configuration example below demonstrates a simple use case when clients with different roles (employee and contractor) connect to the same WLAN (single SSID) and obtain IP address from a same VLAN but inherit different SGT tags from ISE. Furthermore, we will create a policy on ISE which blocks communication between these two user groups (employee and contractor) over wireless. In this process, you will understand how to configure ISE and the WLC for Cisco Wireless TrustSec.

ISE is the central point for all TrustSec configurations that include the following:

- Defining NDAC (Network Device Admission Control) for trusted domain of network devices.
- Centrally defining SGT (Security Group Tag).
- SGACL / Name table: TrustSec policy matrix to be pushed down to the enforcers through secure channel.
- ISE authenticates Wired/Wireless/VPN clients and assigns SGTs.

Clients that are not authenticating through ISE (open/webauth/PSK) can be configured for a SGT tag on the WLCs as shown below by navigating through the WLAN > Advanced setting.

Advanced		
	Universal AP Admin	
	11v BSS Transition Support	
	BSS Transition	<b>v</b>
_	Optimized Roaming Disassociation Timer(0 to 40 TBTT)	40
	BSS Max Idle Service	
	Directed Multicast Service	
	Tunneling	
	Tunnel Profile	None 🔻
	mDNS	
	mDNS Snooping	Enabled
	TrustSec	
	Security Group Tag	40
	OpenDNS	
	OpenDNS Mode	Ignore 🔻
	OpenDNS Profile	None 🔻

### Wireless TrustSec Configuration Checklist (Reference)

- Basic Infrastructure setup: Certificates, Active Directory integration and so on.
- Create Security Group Tags to be used in the network.
- Setup Network Device Admission Control (NDAC).
- Define Authentication and Authorization policies for users and devices.
- Configure SGACL and Egress Policies.

### **Configuration Steps**

The following procedure shows ISE configuration for adding device:

1. Verify WLC is added to ISE for Radius and TrustSec. Go to Administration > Network Resources > Network Devices from ISE main menu.

cisco	Identity Serv	vices Engine	Home	Context Visibility	• Operations	Policy	Administration	• Work Centers		
Summary Endpoints G METRICS Total Endpoint CCC Hently Store Identity Group Network		Guests points	Vulnerability	Threat H	+ System Deploymen Licensing Certificates Logging Maintenane Upgrade Backup & F Admin Acc Settings Identity Mar Identity Sor External Idi Identity Sor Settings		ent Sources equences	Network Resources Network Device Group Network Device Profile External RADIUS Server Seque NAC Managers External MDM Location Services Device Portal Manager Blacklist BYOD Certificate Provisioning Cilent Provisioning Mobile Device Manager My Devices Settinos	rs sovers ences ment g ement	
silvalis cisco	Identity Se	rvices Engine	Hor Hor	ne  Context Vis vork Resources	sibility ► Opera Device Portal Mar	ations	Policy ←Admini	istration 💛 W	Kork Centers ▶ PassivelD   ▶ Thr	Teat Centric NAC
▼ Ne	twork Devices	Network De	evice Groups	s Network Device	Profiles Externa	I RADIUS S	ervers RADIUS S	erver Sequences	NAC Managers	External MDM   Locatio
Netwo	rk devices t Device		GN	letwork Devices						
				/ Edit 🕂 Add 🛛	Duplicate	mport 💽	Export 👻 🕑 Genera	ate PAC X Del	ete 💌	
				Name	IP/Mask	Profile Na	me	Location		Туре
				POD1-WLC	10.10.10.2/32	disce Cisco	0	All Locatio	ons	All Device Types
				WLC-5520-CTS	10.10.200.2/32	dela Cisco	Ð	All Locatio	ons	All Device Types

We have pre-configured the Network Device page with the following inputs:

- WLC Name
- IP Address of WLC
- Enabled Radius Authentication Settings by checking the box
- Shared secret
- Enabled Advance TrustSec Settings > Identification by checking the box for use Device ID
- Under Device Authentication Settings, configured password

cisco IUEII	tity Services Engli	ne Home	Context Visibility	Operations	▶ Policy	▼ Admin	nistration	► Work 0	Centers
System	Identity Manager	ment •Netwo	rk Resources Device	e Portal Managemen	t pxGrid	Services	Feed Ser	rvice 🕨 F	assiveID
▼Network I	Devices Network	Device Groups	Network Device Profiles	External RADIUS	Servers	RADIUS S	Server Seque	ences N	AC Managers
Network devi	ces ce	G Netw Netv	ork Devices List > POD2-1 work Devices * Name F Description * IP Address: 10.10.;	WLC POD2-WLC 20.2 /	32				
			RADIUS Authenticatio	on Settings Enable Authentication	n Settings Protocol	RADIUS			
				on Settings Enable Authentication * Shar	n Settings Protocol red Secret	RADIUS		Show	
				on Settings Enable Authentication * Shar Enable	n Settings Protocol red Secret KeyWrap	RADIUS	•	Show	]
			ADIÚS Authenticati     I	on Settings Enable Authentication * Shar Enable * Key Encry	n Settings Protocol red Secret KeyWrap yption Key	RADIUS	•	Show	
			RADIUS Authenticati	on Settings Enable Authentication * Shar Enable * Key Encry ssage Authenticator	n Settings Protocol red Secret KeyWrap yption Key Code Key	RADIUS	•	Show Show	
			◆ RADIUS Authenticati	on Settings Enable Authentication * Shar Enable * Key Encr ssage Authenticator Key Inpi	n Settings Protocol red Secret KeyWrap yption Key Code Key ut Format	RADIUS	• • • HEXADE(	Show Show	

Any device that participates in the CTS network requires it to be authenticated and trusted. In order to facilitate the authentication process new devices connected to CTS network under goes an enrollment process where in the device obtains the credentials that is specifically needed for CTS device authentication and obtain general CTS environment information

۹.

Identity Services Engine Home	Context Visibility     Operations     Policy     Administration     Work Centers	License Warning 🔺
System Identity Management     Vetwork	Resources   Device Portal Management pxGrid Services   Feed Service   PassiveID   Threat Centric NAC	
Network Devices Network Device Groups	Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services	
©	Advanced TrustSec Settings	
Network devices		
Default Device	Device Authentication Settings Use Device ID for TrustSec Identification     Device Id     WLC-5520-CTS     Password     Show	
	▼ TrustSec Notifications and Updates	
	* Download environment data every 1 Days *	
	* Download peer authorization policy every 1 Days *	
	* Reauthentication every 1 Days *	
	* Download SGACL lists every 1 Days *	
	Other TrustSec devices to trust this device 🛛 🗹 🦛	
	Send configuration changes to device Using CoA CLI (SSH) Ssh Key	
	Device Configuration Deployment	
	Include this device when deploying Security Group Tag Mapping Updates	
	Device Interface Credentials	

2. For ISE TrustSec Policy Configuration, go to Work Centers > TrustSec from ISE main menu.

letwork Access	TrustSec
Overview	Overview
Identities	Components
Id Groups	TrustSec Policy
Ext Id Sources	Authentication Policy
Network Resources	Authorization Policy
Device Groups	SXP
Policy Elements	Troubleshoot
Authentication Policy	Reports
Authorization Policy	Settings
Troubleshoot	RYOD
Reports	Overview
Settings	Identifies
Dictionaries	Identity Groups
Quest Access	Network devices
Overview	Ext Id Sources
Identities	Client Provisioning
Identity Groupe	Configure
Ext Id Sources	Policy Elements
Administration	Authentication Bolicy
Network Devices	Authorization Policy
Configure	Reports
Manage Accounts	Settings
Policy Elements	Octanga
Authentication Policy	
Authorization Policy	
Reports	
Settinge	

3. Under Work Centers>TrustSec> Components, Security Groups and the associated SGT are listed.

dentity Services Engine	Home → Operations → Policy → Guest Access → Administration ▼Work Centers
TrustSec	
Overview Authentication Policy	Authorization Policy Components > Policy > SXP Reports > Settings
0	
Security Groups	Security Groups
Security Group ACLs	
Network Devices	/ Edit 🕂 Add 🕼 Import 🕼 Export 👻 🗙 Delete 🔻 😮 Push
Trustsec AAA Servers	Icon Name SGT (Dec / Hex) Description
	Contractors 30/001E Contractors User Group
	Employee_BYOD 20/0014 Employees with Personal Assets
	L Employee_FullAccess 10/000A Employees with Corporate Assets
	Mail_Servers 120/0078 Email Servers
	PCI_Devices     100/0064     Point-of-Sales (POS) terminals and PCI Servers
	Image: Second state         Z/0002         Network Device SGT
	?         Unknown         0/0000         Unknown Security Group
	Unregist_Dev_SGT 255/00FF Unregistered BYOD Devices
	Ueb_Servers 110/006E Web Servers

4. To create a SGACL, go to **TrustSec > Components > Security Group ACLs.** Example on how to configure a SGACL is shown below:

dentity Services Engine	Home → Operations → Policy → Guest Access → Administration	
▼TrustSec		
Overview Authentication Policy	Authorization Policy Components Policy SXP Reports Settings	
Security Groups	Security Groups ACLs List > Permit_Email_Traffic Security Group ACLs	
Security Group ACLs	* Nome Dermit Empil Traffic	
Network Devices		
Trustsec AAA Servers	Description Access control policy to permit Email service	
	IP Version O IPv4 O IPv6   Agnostic	
	* Security Group ACL content permit tcp dst eq 110 permit tcp dst eq 143 permit tcp dst eq 25 permit tcp dst eq 465 permit tcp dst eq 585 permit tcp dst eq 993 permit tcp dst eq 995 deny all log	

5. Go to Work Centers>TrustSec>TrustSec Policy and view the created policies. We have configured a policy to deny employee and contractor from communicating with each other. Notice that the employee tag is 4 and contractor tag is 5. These tags will be inherited by clients once they associate to the WLAN.

dentity Services Engine Hol	ome   Context Visibility	Operations     Policy	Administration      Work Centers	2	License Warning 🔺 🔍 🔞
Network Access     → Guest Access     ▼T	TrustSec + BYOD + Pr	ofiler   Posture   Device A	dministration		
Overview      Components      TrustSec	Policy Authentication Pol	icy Authorization Policy + S	XP + Troubleshoot Reports + Se	ettings	
0	Production Matrix	Populated cells:	7		
✓ Egress Policy	/ Edit 👍 Add 🗙 Clear	* 📀 Deploy 💿 Monitor All -	- Off 👔 Import 👔 Export 📳 View	Show All     T	
Matrix			J.		S. S. S.
Source Tree	Destination •	s	ment	Servi Vers	on_Us
Destination Tree	uditors	0009 VOD Nirad	0005 evelop svelop	nploye uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests uests	Mint_of V/000A V/000B
Network Device Authorization	₹ Source +	6 6 H 0		1 7 0 0 X M X X	
(	D Auditors				
	9/0009				
(	BYOD				
	15/000F				
		🖾 der	nyicmp	DenyTraffic	
•	Contractors				
L					
	Development				
e	8/0008				
6	Development Ser				
	12/000C				
E CONTRACTOR OF CONTRACTOR OFO			e		Permit IP
	Employees	Deny	Traffic		
	4/0004				

Default Rule can be Permit or Deny

Following is the SGACL configuration to deny rule:

Security	Group ACLs	~	
Name P Version ACEs	DenyTraffic IP Agnostic icmp deny tcp deny udp deny		€ DenyTraffic

6. Also, under **Policy > Authorization** we have configured Authorization rules for employee and contractor to pass the tags once the clients get authenticated.

entication	Authorization	Profiling Post	ure Client Provisionir	ng			
e the Autho	rization Policy by co	onfiguring rules ba	sed on identity groups a	and/or other conditions. Drag and	drop rules to change	the order.	
olicy Expor	go to Administratio	on > System > Bac	ckup & Restore > Policy	Export Page	p to onlinge		
st Matched R	ule Applies	*					
	(0)						
Exception	S (U)						
Exception	s (U)						
Exception Standard	s (U)						
Exception Standard Status	Rule Name		Conditions	(identity groups and other conditi	ons)	F	Permissions
Exception Standard Status	Rule Name employee		Conditions if Employee	(identity groups and other conditi AND Wireless_802.1X	ons)	F	Permissions employee AND Employees

7. For integrating Wireless LAN Controller with ISE, go to **Security** >**RADIUS**>**Authentication** from WLC GUI main menu and verify that ISE server is added.

uluilu cisco	MONITOR	<u>W</u> LANs (	ONTROLLER	WIRELESS	SECURITY MANAGEME	NT C <u>O</u> MMANDS	HELP FEEDBA	ск	Sa	<u>v</u> e Confi
Security	RADIUS	Authentica	tion Serve	ers						
AAA     General     Authentication     Actounting     Fallback     DNS     Downloaded AVP	Auth Ca Use AES MAC De Framed	lled Station ID 5 Key Wrap limiter MTU	Type AP	MAC Address:SSI signed for FIPS of ohen	D 😧	vrap compliant RADI	US server)			
TACACS+     LDAP     Local Net Users	Network User	Managemen	Tunnel S t Proxy I	erver ndex Serv	er Address(Ipv4/Ipv6)		Port	IPSec	Admin Status	
MAC Filtering  Disabled Clients			0 1	* 10.1	0.105.18		1812	Disabled	Enabled	
AP Policies Password Policies										

8. Click on server index for ISE and verify that PAC Provisioning is 'Enabled' and the PAC parameters are downloaded from ISE.

Network User	Management	Tunnel Proxy	Server		Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status	
			1	*	10.10.105.18	1812	Disabled	Enabled	

### **RADIUS Authentication Servers > Edit**

Server Index	1
Server Address(Ipv4/Ipv6)	10.10.105.18
Shared Secret Format	ASCII ᅌ
Shared Secret	•••
Confirm Shared Secret	
Key Wrap	<ul> <li>(Designed for FIPS customers and requires a key wrap compliant RADIUS server)</li> </ul>
Port Number	1812
Server Status	Enabled
Support for CoA	Enabled
Server Timeout	2 seconds
Network User	🕑 Enable
Management	🕑 Enable
Management Retransmit Timeout	2 seconds
Tunnel Proxy	Enable
Realm List	
PAC Provisioning	Z Enable
PAC Params	
PAC A-ID Length	16
PAC A-ID	c70d6d339885b77d3db9ff8d8abdc4e1
PAC Lifetime	Mon Dec 12 13:10:39 2016
IPSec	Enable

- 9. Verify the following from Security > TrustSec > General:
  - CTS is Enabled
  - Configure Device ID
  - Password is configured the same as on ISE
  - Current Status shows Complete
  - Security Group Table should be populated

General		
CTS	Enable	
Device Id	WLC-5520-CTS	
Password		
Inline Taging		
nvironment l	Data	
Current Stat	e COMPLETE	
Last Status	START	
Local Device	SGT	0-00:Unknown
Environment	Data Lifetime (seconds)	86400
Last update	time (seconds)	Mon Oct 3 03:10:21 2016
Environment	Data expiry	0:23:59:37 (dd:hr:mm:sec)
Environment	Data refresh	0:23:59:37 (dd:hr:mm:sec)
Security Gro	up Name Table	
:Unknown :TrustSec_Do :Network_Sec :Employees :Contractor :Guests :Production :Developers :Auditors	vices rvices s Users	

10. Navigate to **SECURITY** > **TrustSec** > **Policy** and verify the SGT-TAG list to see that the policy is downloaded on the WLC.



**Note** In order for the SGT-TAG list to populate on the Wireless LAN Controller (WLC), a client must first connect with the targes SGT. Once the client is connected, the WLC will pull the SGT-TAG list and install it, similar to the process on the wired size Ensure that a client connection is established to trigger this synchronisation.

cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Security								Intries 1 -
* AAA	Total SGT Aut	horization	Policy count 4					
General RADIUS	D-SGT		Ger	neration Id	Policy Dov Status	vnload Nu SG	mber of clients F	with this
Authentication	Unknown-0		00		Success	1		
Accounting	4:Employees		01		Success	0		
DNS	5:Contractors		00		Success	2		
Downloaded AVP	Default-65535		01		Success	0		
LDAP								
Local Net Users								
<ul> <li>Disabled Clients</li> </ul>								
User Login Policies								
AP Policies Password Policies								
Local EAP								
Advanced EAP								
Priority Order								
Certificate								
Access Control Lists								
Wireless Protection Policies								
Web Auth								
TrustSec								
SXP Config Policy								
Local Policies								
OpenDNS								
Advanced								

Drill down the Policy and you can see the SGACL:

SGACL > Detail	
SGACL Name	DenyTraffic
Generation Id	02
SGACL Policy Capability	IPv4v6
Number of ACEs Associated	2
ACEs List Info	
ACEs List Info 1. deny icmp 2. permit any	
ACEs List Info 1. deny icmp 2. permit any	
ACEs List Info 1. deny icmp 2. permit any	
ACEs List Info 1. deny icmp 2. permit any	
ACEs List Info 1. deny icmp 2. permit any	

You can drill down further to see the ACEs per SGACL:

SGT Detail				
Policy Matrix	for SGT	4:Employ	ees	
Generation Io	i	03		
Entries 1 - 1 o	f 1			
No	SGACL Name		S-SGT	D-SGT
1	DenyTraffic		0005	0004

11. To configure WLANs on WLC, Select Create New from WLANs and click Go.

CISCO	MONITOR	<u>W</u> LANs		WIRELES	S <u>S</u> ECURITY	M <u>A</u> NAGEMENT	COMMANDS	HELP	FEEDBACK	🔒 <u>H</u> ome
WLANs		WI	ANs						Entries	1 - 1 of 1
WLANS	5	Cur	rent Filter:	None [	Change Filter] [Cl	ear Filter]	Create M	New	📀 🛛 Go 📌	

Set the profile name as POD1-CTS and click **Apply**.

WLANs > New		< Back	Apply
Туре	WLAN 🔻		
Profile Name	POD1-CTS		
SSID			
ID	1 •		

### From General Tab, **Enable** the WLAN.

LANs > E	dit 'POI	D1-CTS'			< Back	Apply
General	Security	QoS	Policy-Mapping	Advanced		
Profile Na	me	POD1-CTS				í
Туре		WLAN				
SSID		POD1-CTS				
Status	-	Enabled				
Security P	Policies (	[WPA2][Aut Modifications	th(802.1X)] done under security tal	o will appear after app	blying the changes.)	
Radio Poli	cy [	All	•			
Interface/ Group(G)	Interface	management	•			
Multicast Feature	Vlan (	Enabled				
	ana l					

**12.** From **Security** > **AAA Servers**, select the AAA server which is configured above and click**Apply**.

eneral	Security	QoS Poli	cy-Mapping	Advanced		/
layer 2	Layer 3	AAA Servers	•			
						_
alact AAA	comions holou	to ouomido u	o of dofault o	among on this W	I A BI	
elect AAA	servers below	to override us	se of default s	ervers on this W	LAN	
ADIUS Se	servers below	to override us	se of default s	ervers on this W	LAN	
ADIUS Se RADIUS	servers below ervers Server Overwrite	to override us	nabled	ervers on this W	'LAN	
RADIUS Se RADIUS Apply Ci	servers below ervers Server Overwrite sco ISE Default s	to override us interface Settings Z E	nabled	ervers on this W	'LAN	
RADIUS Se RADIUS Apply Ci	servers below ervers Server Overwrite sco ISE Default s Authenticatio	to override us interface Settings E on Servers	nabled nabled Accounting	ervers on this W	EAP F	Parameters

- 13. Once you enable ISE default settings, the WLC automatically configures the following settings on the WLAN advance tab:
  - Allow AAA override=Enabled

Allow AAA Override	Enabled	DHCP	
Coverage Hole Detection	C Enabled	DHCP Server	Override
Enable Session Timeout	1800 Session Timeout (secs)	DHCP Addr. Assignment	E Required
Aironet IE	CEnabled	OEAP	
Diagnostic Channel <u>18</u>	Enabled	Split Tunnel	Enabled
Override Interface ACL	IPv4 None ON None	ne 💿 Management Frame Prot	ection (MFP)
Layer2 Acl	None 📀	MFP Client Protection 4	Optional ᅌ
	None	DTIM Period (in beacon	intervals)
P2P Blocking Action	Disabled		
Client Exclusion <sup>2</sup>	Enabled 60	802.11a/n (1 - 255)	1
	Timeout Value (secs)	802.11b/g/n (1 - 255)	1
Maximum Allowed	0	NAC	
static in runneling	Enabled	INAC State ISE INAC	

- 14. To test with client traffic without enforcing SGACL on the AP, follow the below steps:
  - a. Using your client devices, log in as an employee from one client and as a contractor from a different client.

•••••• Ve	●●●○ Verizon 중 3:30 PM Enter the password for " Demo-TrustSec "							53% 🔳	•
Cano	cel	Enter t	he pas Enter	sword	for " De	mo-Trus	tSec "	Join	
User	name	Emplo	oyee						
Password Cisco 123									
a	we	-		τIA			ilo	ln	
9			4						
а	S	d	f	g	h	j	k	L	
�	z	x	С	V	b	n	m	×	)
123		₽		spa	ace		ret	urn	

•••• Verizon 🗢 3:30 PM							53% 🔳	•	
		Enter t	he pas	sword	for " De	mo-Trus	tSec "		
Cano	el		Enter	Pass	word			Join	
User	name	Contr	actor						
Pass	word	Cisco	123						
q	we	e r		t y	/ ι	J	i o	р	
-		A	f		h	Ĥ			
a	S	u		y		<u> </u>	ĸ		
$\Diamond$	z	x	с	v	b	n	m	$\propto$	)
123	•	Q		spa	ace		ret	turn	

**b.** From the WLC page, check client details under **Monitor** > **Clients** for both users and SGT security tag pushed on both.

lax Number of Records	10 Clear AVC Stats			
General AVC Stat	tistics			
<b>Client Properties</b>		Security Information		
MAC Address	18:65:90:b2:a8:11	Security Policy Completed	Yes	
IPv4 Address	10.10.40.228	Policy Type	RSN (WPA2)	
IPv6 Address	fe80::14e7:ca98:c9cc:c5d3,	Auth Key Mgmt	FT-802.1x	
		Encryption Cipher	CCMP (AES)	
		ЕАР Туре	PEAP	
		SNMP NAC State	Access	
		Radius NAC State	RUN	
		CTS Security Group Tag	4	
		AAA Override ACL Name	none	
		AAA Override ACL Applied	Unavailable	
Client Type	Regular Simple IP			
User Name	employee			
Port Number	1			
MONITOR WLANs lients > Detail	<u>C</u> ontroller W <u>i</u> reless <u>s</u> ea	CURITY MANAGEMENT		
MONITOR WLANS lients > Detail ax Number of Records General AVC Stat	CONTROLLER WIRELESS SE	CURITY MANAGEMENT		
MONITOR WLANS lients > Detail ax Number of Records General AVC Stat	CONTROLLER WIRELESS SE	CURITY MANAGEMENT	on	
MONITOR WLANS ients > Detail ax Number of Records General AVC Stat Client Properties	CONTROLLER WIRELESS SE	CURITY MANAGEMENT Security Informati Security Policy Comp	on Vieted Yes	
MONITOR WLANS lients > Detail ax Number of Records General AVC Stat Client Properties MAC Address	CONTROLLER WIRELESS SE	CURITY MANAGEMENT Security Informati Security Policy Comp Policy Type	bleted Yes RSN (WPA2)	
MONITOR WLANS lients > Detail ax Number of Records General AVC Stat Client Properties MAC Address IPv4 Address	CONTROLLER         WIRELESS         Set           10 +         Clear AVC Stats         istics           18:65:90:b2:a8:11         10.10.40.228         istics	CURITY MANAGEMENT Security Informati Security Policy Comp Policy Type Auth Key Mgmt	Yes           RSN (WPA2)           FT-802.1x	
MONITOR WLANS lients > Detail ax Number of Records General AVC Stat Client Properties MAC Address IPv4 Address IPv6 Address	CONTROLLER         WIRELESS         SE           10 :         Clear AVC Stats         istics           18:65:90:b2:a8:11         10.10.40.228         fe80::14e7:ca98:c9cc:c5d3,	CURITY MANAGEMENT Security Informati Security Policy Comp Policy Type Auth Key Mgmt Encryption Cipher	Neted Yes RSN (WPA2) FT-802.1x CCMP (AES)	
MONITOR WLANS lients > Detail ax Number of Records General AVC Stat Client Properties MAC Address IPv4 Address IPv6 Address	CONTROLLER         WIRELESS         Set           10 +         Clear AVC Stats         istics           18:65:90:b2:a8:11         10.10.40.228         fe80::14e7:ca98:c9cc:c5d3,	CURITY MANAGEMENT Security Informati Security Policy Comp Policy Type Auth Key Mgmt Encryption Cipher EAP Type	Neted Yes RSN (WPA2) FT-802.1x CCMP (AES) PEAP	
MONITOR WLANS lients > Detail ax Number of Records General AVC Stat Client Properties MAC Address IPv4 Address IPv6 Address	CONTROLLER         WIRELESS         Set           10 ÷         Clear AVC Stats         istics           istics         18:65:90:b2:a8:11         10.10.40.228           fe80::14e7:ca98:c9cc:c5d3,         10.10.40.228         10.10.40.228	CURITY MANAGEMENT Security Informati Security Policy Comp Policy Type Auth Key Mgmt Encryption Cipher EAP Type SNMP NAC State	Neted Yes RSN (WPA2) FT-802.1x CCMP (AES) PEAP Access	
MONITOR WLANS lients > Detail ax Number of Records General AVC Stat Client Properties MAC Address IPv4 Address IPv6 Address	CONTROLLER         WIRELESS         Set           10 ÷         Clear AVC Stats         istics           18:65:90:b2:a8:11         10.10.40.228         fe80::14e7:ca98:c9cc:c5d3,	CURITY MANAGEMENT Security Informati Security Policy Comp Policy Type Auth Key Mgmt Encryption Cipher EAP Type SNMP NAC State Padius NAC State	Neted Ves RSN (WPA2) FT-802.1x CCMP (AES) PEAP Access PLIN	
MONITOR WLANS lients > Detail ax Number of Records General AVC Stat Client Properties MAC Address IPv4 Address IPv6 Address	CONTROLLER         WIRELESS         Set           10 ÷         Clear AVC Stats         istics           istics         18:65:90:b2:a8:11         10.10.40.228           fe80::14e7:ca98:c9cc:c5d3,         14:67:ca98:c9cc:c5d3,	CURITY MANAGEMENT Security Informati Security Policy Comp Policy Type Auth Key Mgmt Encryption Cipher EAP Type SNMP NAC State Padius NAC State CTS Security Group	Yes           RSN (WPA2)           FT-802.1x           CCMP (AES)           PEAP           Access           PIN           Tag         5	
MONITOR WLANS lients > Detail ax Number of Records General AVC Stat Client Properties MAC Address IPv4 Address IPv6 Address	CONTROLLER         WIRELESS         Set           10 +         Clear AVC Stats         istics           istics         18:65:90:b2:a8:11         10.10.40.228           fe80::14e7:ca98:c9cc:c5d3,         fe80::14e7:ca98:c9cc:c5d3,	CURITY MANAGEMENT Security Informati Security Policy Comp Policy Type Auth Key Mgmt Encryption Cipher EAP Type SNMP NAC State Padius NAC State CTS Security Group AAA Override ACL Na	Yes       RSN (WPA2)       FT-802.1x       CCMP (AES)       PEAP       Access       PIN       Tag     5       ame     none	
MONITOR WLANS lients > Detail ax Number of Records General AVC Stat Client Properties MAC Address IPv6 Address IPv6 Address	CONTROLLER         WIRELESS         Set           10 ÷         Clear AVC Stats         istics           18:65:90:b2:a8:11         10.10.40.228         fe80::14e7:ca98:c9cc:c5d3,	CURITY MANAGEMENT Security Informati Security Policy Comp Policy Type Auth Key Mgmt Encryption Cipher EAP Type SNMP NAC State Padius NAC State CTS Security Group	Neted Yes RSN (WPA2) FT-802.1x CCMP (AES) PEAP Access PIN Tag 5 none	
MONITOR WLANS lients > Detail ax Number of Records General AVC Stat Client Properties MAC Address IPv4 Address IPv6 Address IPv6 Address	CONTROLLER         WIRELESS         Set           10 •         Clear AVC Stats         istics           10 •         Clear AVC Stats         istics           18:65:90:b2:a8:11         10.10.40.228         istics           fe80::14e7:ca98:c9cc:c5d3,         fe80::14e7:ca98:c9cc:c5d3,         istics           Regular         Istics         Istics         Istics         Istics	CURITY MANAGEMENT Security Informati Security Policy Comp Policy Type Auth Key Mgmt Encryption Cipher EAP Type SNMP NAC State Padius NAC State CTS Security Group AAA Override ACL Na	on Ves RSN (WPA2) FT-802.1x CCMP (AES) PEAP Access PLIN Tag 5 one none	
MONITOR WLANS lients > Detail ax Number of Records General AVC Stat Client Properties MAC Address IPv4 Address IPv6 Address IPv6 Address Client Type Client Type	CONTROLLER         WIRELESS         Set           10 +         Clear AVC Stats         istics           istics         10.10.40.228         680::14e7:ca98:c9cc:c5d3,           fe80::14e7:ca98:c9cc:c5d3,         Regular         simple IP	CURITY MANAGEMENT Security Informati Security Policy Comp Policy Type Auth Key Mgmt Encryption Cipher EAP Type SNMP NAC State CTS Security Group AAA Override ACL Na	on Ves RSN (WPA2) FT-802.1x CCMP (AES) PEAP Access PLIN Tag 5 ane none	
MONITOR WLANS lients > Detail ax Number of Records General AVC Stat Client Properties MAC Address IPv4 Address IPv6 Address IPv6 Address Client Type Client Type Client Type User Name	CONTROLLER WIRELESS SEE	CURITY MANAGEMENT Security Informati Security Policy Comp Policy Type Auth Key Mgmt Encryption Cipher EAP Type SNMP NAC State Padius NAC State CTS Security Group	on Ves RSN (WPA2) FT-802.1x CCMP (AES) PEAP Access DIN Tag 5 ame none	

**c.** To test applications per SGACL, use one device to connect as an employee and other device as a contractor, and make sure that both clients can ping each other. Below is an example of ICMP communication from Contractor device to an employee device (IP: 10.10.40.200).

10.10	.40.200		Stop		
	64 bytes TTL=64				
#4	<b>10.10.40.200</b> 64 bytes TTL=64		190.111 ms		
#5	<b>10.10.40.200</b> 64 bytes TTL=64		8.150 ms		
#6	10.10.40.200 64 bytes TTL=64		174.768 ms		
#7	10.10.40.200 64 bytes TTL=64		113.948 ms		
#8	10.10.40.200 64 bytes TTL=64		56.193 ms		
#9	10.10.40.200 64 bytes TTL=64		186.947 ms		
#10	10.10.40.200 64 bytes TTL=64		140.000 ms		
#11	10.10.40.200 64 bytes TTL=64		7.543 ms		
#12	10.10.40.200 64 bytes TTL=64		8.816 ms		
#13	10.10.40.200 64 bytes TTL=64		23.080 ms		
#14	10.10.40.200		10.933 ms		
Ser 15 Mir 7.54	Received           5         15           n         Avg           43         72.789	Lost 0 Max 190.111	Loss 0.00% Stddev 68.895		
ſ <sup>↑</sup> ]	ш	<u>ين</u>	()		

**15. a.** To enable TrustSec enforcement on a local mode AP, navigate to **Wireless tab** > **Select an Access point** > **Advanced** tab and enforce SGACL as shown below.

II APs > Details for AP5	8ac.78de.8ae8						< Back	Apply
General Credentials	Interfaces High Av	vailability Inventory Adv	anced					
Regulatory Domains		802 11bc-0 802 11b-R	Bauwan Owan Ethan	nat Cattings =				
Country Code		US (Iloited States)	Power over Ether	net settings				
Cisco Discovery Protocol			Pre-standard 80	2.3af switches	0			
AP Group Name		default-group +	Power Injector	state	U			
Statistics Timer		30	AP Core Dump					
Data Encryption		0	AP Core Dump	_	0	Enabled		
Rogue Detection			AP Retransmit Co	ntig Parameters				
2 Teinet		Global Config +	AP Retransmit (	Count	5			
▲ SSH		Global Config ≑ 🗌	AP Retransmit I	nterval	3			
TCP Adjust MSS (IPv4: 536 -	- 1363, IPv6: 1220 - 1331)	0	VLAN Tagging					
LED State		Enable +	VLAN Tagging			Enabled		
LED Flash State		0 (1-3600)seconds	mDNS Configurat	ion				
		OIndefinite	mDNS Snooping	1	$\Box$	Enabled		
		Olisable	VLAN List					
Hyperlocation Configuration			AP Virtual IP con	figuration				
Enable Hyperlocation		Global Config 🗧	Override Global	configured Virtual IP		Enabled		
ink Latency			Trusted Security	-				
Enable Link Latency		0	TrustSec Config					
AP Image Download			Trustate coning					
Pre-download on this AP Download Primary Perform an interchange of both the images on this AP	Pre-download on this AP Download Backup Perform an abort of predownload on this AP							
uluilu cisco	MONITOR <u>W</u> LANS	<u>Controller</u> Wireless	SECURITY MANAGEI	MENT C <u>O</u> MMAN	DS	HELP	FEEDBACK	
Vireless	All APs > AP58ac	.78de.8ae8 > Trusted Secu	urity					
Access Points								
All APs	AP Name A	AP58ac.78de.8ae8						
<ul> <li>Radios</li> <li>802.11a/n/ac</li> </ul>	Base Radio MAC	c:16:7e:30:47:d0						
802.11b/g/n Dual-Band Radios	Trusted Security							
Global Configuration	Sgacl Enforcement	☑ ←						
Advanced		-						
Mesh	1.Inline tagging is support	orted in only Flex mode AP (Applica	ble to 11ac					
ATF	2.SXPv4(Listener/Speak	er/Both) is supported in Flex,Flex+	bridge AP					
RF Profiles	(Applicable to 11ac AP)							
FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates								
OFAD ACLA								

b. To add SXP or inline config on a Flexconnect AP, go to Wireless > AP > Advanced > Trusted Security > TrustSec Config.

### All APs > POD1-3800 > Trusted Security

AP Name	POD1-3800				
Base Radio MAC	cc:16:7e:ac:8c:f0				
Trusted Securit	y				
Sgacl Enforceme	ent				
Inline Taging					
Total AP SXP Cor	nnections		0		
AP SXP State		Disabled ▼			
Default Password	•••••				
SXP Listener Mir	Hold Time (second	ls)	90		
SXP Listener Ma	x Hold Time (secon	ds)	180		
SXP Speaker Hol	d Time (seconds)		120		
Reconciliation Ti	me Period (seconds	;)	120		
Retry Period (se	conds)		120		
Peer IP config					
Peer IP Address					
Password		Defa	ult 🔻		
Mode		Spea	ker 🔻		
		AD	D		

16. After enforcing "TrustSec" on AP, you should not be able to ping between the two clients (employee and contractor) as shown below.

10.10.40.2	200		Ping
#61 Rec	quest time-out		
<b>#</b> 62 <b>Rec</b>	quest time-out		
<b>#</b> 63 <b>Rec</b>	quest time-out		
<b>#</b> 64 <b>Rec</b>	quest time-out		
#65 Rec	quest time-out		
#66 Rec	quest time-out		
<b>#</b> 67 <b>Rec</b>	quest time-out		
<b>#</b> 68 <b>Rec</b>	quest time-out		
<b>#</b> 69 <b>Rec</b>	quest time-out		
#70 Red	quest time-out		
<b>#</b> 71 Red	quest time-out		
Sent 77 Min	Received O Avg	Lost 72 Max	Loss 100.00% Stddev
Ê		<b>1</b>	i

# **CLI Commands for Wireless TrustSec Configuration**

### 1. PAC download on WLC

# config radius auth pac <server-index> enable
# config radius acct pac <server-index> enable

#### It enables the CTS PAC download on the server.

# config cts device-id <device-id> password <pwd>

Configures the CTS device ID and Password to be used during initial PAC download.

# show cts pacs

To check PAC download status on WLC.

# clear cts pac <A-ID>

To clear the PAC.

### 2. Inline tagging

### CLI commands on WLC:

# config cts inline tagging {enable | disable}
# show cts summary

#### CLI command on AP:

#config cts inline-tag (enable|disable)
# show cts ap summary
# show ap config general
#config cts ap inline-tagging {enable | disable} <apname/all>

#### 3. SXPv4

```
# config cts sxpv ap {ap name} enable/disable
# show cts ap summary
# show ap config general
#config sxp ap enable/disable <ap_name/all>
#config cts sxp ap connection default password <passwd> <ap/all>
#config cts sxp ap connection peer <ipaddr> password [default | none] mode [speaker | listener | both]
<ap/all>
#config cts sxp ap listener holdtime <min> <max> <ap-name/all>
#config cts sxp ap speaker holdtime <secs> <ap-name/all>
#config cts sxp ap reconciliation period <secs> <ap-name/all>
#config cts sxp ap retry period <val> <ap_name/all>
```

### 4. Debug

Available debug options:

```
#debug cts ?
               Configure the CTS AAA debug options.
aaa
authz
               Configures the CTS SXP debug options.
               Debugs for CTS policy download over capwap messages
capwap
env-data
               Configure the CTS environment data debugs.
               Configure the CTS HA debug options.
ha
key-store
               Configure the CTS Key-store debug options.
               Configure the CTS PAC Provisioning debug options.
provisioning
               Configures the CTS SXP debug options.
sxp
```

#### 5. Show commands on AP



Note There are difference in commands for different AP platforms.

```
11AC wave1 and earlier APs (17xx, 27xx, 37xx):
```

### SXPv4:

#sh ct sxp connections brief

#### to check connections

# sh ct sxp sgt-map brief

#### to check SXP bindings

# sh ct role-based sgt-map all

#### to check IP-SGT binding for local switching ONLY.

```
# sh controllers dot11Radio 1 | beg SG
```

to check SGT for central switching clients

### Check SGALC:

```
#sh ct role permissions ?
    default Default Permission list
    from Source Group
    ipv4 Protocol Version - IPv4
    ipv6 Protocol Version - IPv6
    to Destination Group
    | Output modifiers
    <cr>
    sh access-lists <name>
```

#### Debug:

```
#debug rbm dp packets.
#sh cts role-based counters ?
default Default policy counters
from Source Group
ipv4 Protocol Version - IPv4
ipv6 Protocol Version - IPv6
to Destination Group
| Output modifiers
<cr>
```

### Wave2 APs (18xx, 28xx, 38xx):

### <u>SXP:</u>

#sh ct sxp connections

to check connections

#sh ct sxp sgt-map

to check SXP bindings

# sh ct role-based sgt-map all

to check IP-SGT binding (for both central and local switching only)

### Check SGALCs:

#sh cts role-based permissions
#sh cts access-lists <name>

### Debug:

#debug ct enforcement
#sh cts role-based counters

# cisco.

Americas Headquarters Cisco Systems, Inc. San Jose, CA 95134-1706 USA Asia Pacific Headquarters CiscoSystems(USA)Pte.Ltd. Singapore Europe Headquarters CiscoSystemsInternationalBV Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.