

# Cisco TrustSec How-To Guide: Universal Configuration for the Cisco Wireless LAN Controller

For Comments, please email: <u>howtoguides@external.cisco.com</u> Current Document Version: 3.0 August 27, 2012

# Table of Contents

Table of Contents1	
Introduction	
What Is the Cisco TrustSec System?	3
About the TrustSec How-To Guides	3
What does it mean to be 'TrustSec Certified'?	4
Universal Configuration for the Cisco Wireless LAN Controller	
Initial Configuration for the Cisco WLC	5
Adding 802.1X and Central Web Authentication SSIDs	14
Configuring Cisco ISE for Wireless Authentication	19
Appendix A: References	
Cisco TrustSec System:	21
Device Configuration Guides:	21

# What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture<sup>TM</sup>, is an intelligent access control solution. Cisco TrustSec mitigates security risks by providing comprehensive visibility into who and what is connecting across the entire network infrastructure, and exceptional control over what and where they can go.

TrustSec builds on your existing identity-aware access layer infrastructure (switches, wireless controllers, and so on). The solution and all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

In addition to combining standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, the Cisco TrustSec system it also includes advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.



# About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for Cisco TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the Cisco TrustSec system. You can use these documents to follow the prescribed path to deploy the entire system, or simply pick the single use-case that meets your specific need.

Each guide is this series comes with a subway-style "You Are Here" map to help you identify the stage the document addresses and pinpoint where you are in the Cisco TrustSec deployment process (Figure 2).



# What does it mean to be 'TrustSec Certified'?

Each TrustSec version number (for example, Cisco TrustSec Version 2.0, Version 2.1, and so on) is a certified design or architecture. All the technology making up the architecture has undergone thorough architectural design development and lab testing. For a How-To Guide to be marked "TrustSec certified," all the elements discussed in the document must meet the following criteria:

- Products incorporated in the design must be generally available.
- Deployment, operation, and management of components within the system must exhibit repeatable processes.
- All configurations and products used in the design must have been fully tested as an integrated solution.

Many features may exist that could benefit your deployment, but if they were not part of the tested solution, they will not be marked as "Cisco TrustSec "certified". The Cisco TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the Cisco TrustSec test plans, pilot deployments, and system revisions. (i.e., Cisco TrustSec 2.2 certification).

Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore are not included in these documents. As an example, certain IEEE 802.1X timers and local web authentication features are not included.

**Note:** Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for Cisco TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.

# Universal Configuration for the Cisco Wireless LAN Controller

The following section describes the "universal configuration" for Cisco® Wireless LAN Controllers (WLC). These recommended configurations are compiled as a best practice to be used for all deployments, and they remain consistent through the different stages of deployment, as well as the different deployment types chosen.

### Initial Configuration for the Cisco WLC

#### Procedure 1 Bootstrap the Wireless LAN Controller

The following steps will take you through the initial configurations for the Cisco Wireless LAN Controller.

Step 1 Connect to the console port of the WLC. Refer to the following settings to bootstrap the WLC.

```
(Cisco Controller)
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]:yes
AUTO-INSTALL: process terminated -- no configuration loaded
System Name [Cisco 91:e2:64] (31 characters max):
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): ********
Re-enter Administrative Password
                                                 : *******
Service Interface IP Address Configuration [static][DHCP]:dhcp
Enable Link Aggregation (LAG) [yes][NO]: no
Management Interface IP Address: 10.1.60.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.1.60.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 10.1.100.100
Virtual Gateway IP Address: 192.0.2.1
Mobility/RF Group Name: cts.local
Network Name (SSID): CTS-CORP
Configure DHCP Bridging Mode [yes] [NO]: no
Allow Static IP Addresses [YES] [no]: no
```

```
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code list (enter 'help' for a list of countries) [US]:us
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
Configure a NTP server now? [YES][no]: yes
Enter the NTP server's IP address: 10.1.100.100
Enter a polling interval between 3600 and 604800 secs: 3600
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

Best Practice: It is recommended that you set the Cisco WLC virtual gateway address to 192.0.2.1. This should be a non-routed IP with a fully qualified domain name (FQDN) mapped in the Domain Name System (DNS). This FQDN/ IP address should be added to certificates generated by your CA. This will stop users from seeing "untrusted certificate" errors when they are redirected to the WLC's virtual gateway.

Step 2 Configure the switchport for the port connected to the WLC.

```
interface GigabitEthernet2/46
description WLC-5500 connection
ip address 10.1.60.1 255.255.255.0
end
```

Procedure 2 Disable the DHCP Proxy on the Cisco WLC

The Cisco WLC is configured to proxy Dynamic Host Configuration Protocol (DHCP) requests by default. We recommend disabling this feature since Cisco ISE relies on DHCP traffic from the endpoint to profile it accurately. Leaving the DHCP Proxy option enabled causes the Cisco WLC to modify DHCP attributes. As a result, we lose valuable information that aids in accurately profiling an endpoint.

Step 1 Navigate to Controller  $\rightarrow$  Advanced  $\rightarrow$  DHCP.

Step 2 Uncheck the Enable DHCP Proxy option (Figure 3).

Figure 3 Disabling DHCP Proxy on the Cisco WLC

uluilu cisco	MONITOR	<u>W</u> LANs	CONTROLLER		<u>S</u> ECURITY	MANAGEMENT
Controller	DHCP Pa	rameters	S			
General Inventory Interfaces Interface Groups Multicast Internal DHCP Server Mobility Management Ports NTP CDP IPv6	Enable DI DHCP Op DHCP Tim	HCP Proxy tion 82 Rem neout (5 - 1	note Id field forma 20 seconds)	t AP-MJ 120	ac ÷)	
DHCP Master Controller Mode						

## Procedure 3 Configure SNMP on the WLC

Cisco ISE will use Simple Network Management Protocol (SNMP) to query the WLC for certain attributes to help identify the devices connected to the wireless network. We will configure SNMP communities for Cisco ISE to query.

Step 1 Navigate to Management  $\rightarrow$  SNMP  $\rightarrow$  General and ensure that SNMPv2 is enabled for profiling (Figure 4).

Figure 4 SNMP Settings for Cisco WLC

 cısco	<u>M</u> onitor <u>w</u> lan	s <u>C</u> ONTROLLER	WIRELESS	SECURIT	MANAGEMENT
Management	SNMP System	Summary			
Summary SNMP General SNMP V3 Users Communities Trap Receivers Trap Controls Trap Controls Trap Logs HTTP-HTTPS Telnet-SSH	Name Location Contact System Descriptic System Object ID SNMP Port Numbe	Cisco_9	1:e2:64 roller .9.1.1069		
Serial Port	Trap Port Number	162			
Users	SNMP V1 Mode	Disable			
User Sessions	SNMP V2C Mode	Enable			
🕨 Logs	SNIMP V3 Mode	Enable	•		
Mamt Via Wirolocc					

Step 2 Click Communities and create a new community using the values in Table 1. Click Apply when done.

Attribute	Value
Community Name	RO
IP Address	10.1.100.0
IP Mask	255.255.255.0
Access Mode	Read Only
Status	Enable

Procedure 4 Configure the WLC to Use Cisco ISE as a RADIUS Server

The Cisco WLC uses the Cisco ISE as a RADIUS server. The following steps will walk you through the process of configuring the Cisco WLC to use Cisco ISE as its RADIUS server.

Step 1 Access the WLC GUI and navigate to Security  $\rightarrow$  RADIUS  $\rightarrow$  Authentication.

Step 2 Set the Call Station ID type to System MAC address (Figure 5).

Figure 5 Configuring RADIUS Servers on the Cisco WLC

،، ،،، ،، cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY
Security	RADIUS Authentication Servers
AAA     General     AdDIUS     Authentication     Accounting     Fallback     TACACS+     LDAP     Local Net Users     MAC Filtering     Disabled Clients     User Login Policies     AP Policies	Call Station ID Type I System MAC Address  Use AES Key Wrap Coesigned for FIPS customers and requires a key wrap compliant RADIUS server) MAC Delimiter Hyphen Network User Management Server Index Server Address Port IPSec Admin Status I. Cell Station ID Type will be applicable only for non 802.1x authentication only.
▶ Local EAP	

Step 3 Click Apply.

Note: When we send the MAC address of the endpoint versus IP address, RADIUS packets sent to a Cisco ISE Policy Service node configured for Profiling Services will be able to discover this MAC address and collect attributes for classification purposes.

Step 4 Click New... on the top-right corner to add a new RADIUS authentication server (Figure 6).

RADIUS authentication server settings are listed in Table 2.

Attribute	Value
Server Index (Priority)	1
Server IP Address	10.1.100.3
Shared Secret Format	ASCII
Shared Secret	Cisco123
Key Wrap	(Not checked)
Port Number	1812
Server Status	Enabled (checked)
Support for RFC 3576	Enabled (checked)
Server Timeout	2 seconds
Network User	Enabled (checked)
Management	Enabled (checked)
IPsec	(Not checked)

Table 2RADIUS Authentication Server Settings

#### Figure 6 RADIUS Server Settings

MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK	
RADIUS Authentication Servers > New									
Server Ir	ndex (Priori	ty)	2 🗸						
Server IF	Address								
Shared S	ecret Form	at	ASCII 👻						
Shared S	ecret								
Confirm	Shared Sec	ret							
Key Wraj	0		] (Designed fo	r FIPS custome	ers and requires a	key wrap compli	iant RADI	US server)	
Port Num	ber		1812						
Server S	tatus		Enabled 👻						
Support f	or RFC 357	6	Enabled 👻						
Server T	meout		2 secon	ds					
Network	User		🗹 Enable						
Managem	nent		🗹 Enable						
IPSec			📃 Enable						

Step 5 Click Apply and Save Configuration.

Step 6 Click Accounting and New... to add RADIUS accounting servers, as shown in Figure 7.

RADIUS accounting server settings are listed in Table 3.

## Table 3 - RADIUS Accounting Server Settings

Attribute	Value
Server Index (Priority)	1
Server IP Address	10.1.100.3
Shared Secret Format	ASCII
Shared Secret	Cisco123
Port Number	1813
Server Status	Enabled (checked)
Server Timeout	30 seconds
Network User	Enabled (checked)
IPSec	(Not checked)

Figure 7 RADIUS Accounting Server Settings

MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
RADIUS	Authenti	cation Servers	s > Edit					
Server Ir	ndex		1					
Server A	ddress		10.1.100.3					
Shared S	ecret Form	at	ASCII 👻					
Shared S	ecret		•••					
Confirm	Shared Sec	ret	•••					
Key Wraj	Þ		Oesigned fo	r FIPS custome	ers and requires a	key wrap compli	ant RADI	US server)
Port Num	ber		1812					
Server S	tatus		Enabled 👻					
Support f	for RFC 357	76	Enabled 👻					
Server T	imeout		2 secon	ds				
Network	User		🔽 Enable					
Managen	nent		🔽 Enable					
IPSec			📃 Enable					

Step 7 Click Apply and Save Configuration.

Procedure 5 Configuring RADIUS fallback options

The primary RADIUS server (the server with the lowest server index) is assumed to be the most preferable server for the Cisco WLC. If the primary server becomes unresponsive, the controller switches to the next active backup server (the server with the next lowest server index). The controller continues to use this backup server, unless you configure the controller to fall back to the primary RADIUS server when it recovers and becomes responsive or to a more preferable server from the available backup servers.

Step 1 Navigate to Security  $\rightarrow$  AAA  $\rightarrow$  RADIUS  $\rightarrow$  Fallback

Step 2 Set the Fallback Mode to Active.

**Note:** Selecting Active causes the Cisco WLC to revert to a server with a lower priority from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The controller ignores all inactive servers for all active RADIUS requests. Selecting Passive causes the Cisco WLC to revert to a server with a lower priority from the available backup servers without using extraneous probe messages. The controller ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent.

Step 3 For the Username, enter the name to be sent in the inactive server probes.

Step 4 Enter a value for the Interval in Sec. field.

The interval serves as inactive time in passive mode and probe interval in active mode. The valid range is 180 to 3600 seconds, and the default value is 300 seconds.

#### Procedure 6 Create an Airespace ACL for Posture Assessment

When a user connects to a network, the user is initially put into a quarantine state. During this stage, we allow only DNS and traffic from the Cisco Network Access Control [NAC] Appliance Agent to go to Cisco ISE. When Cisco ISE determines the user to be using a posture-compliant device, RADIUS change of authorization (CoA) is used to re-authenticate the user and provide the user with access appropriate to the user's role. Because the WLCs only support named-ACLs today, we need to predefine ACLs on the WLC.

Although we are defining this ACL for posture redirection at this stage, it will not be utilized until we move in to the Enforcement mode with posture enabled.

Note: ACLs on the Wireless LAN Controller enforce policies at Layer 3 and Layer 4. Airespace ACLs support up to 64 rules and can be applied on a per-interface or per-user basis.

Step 1 From the WLC, navigate to Security  $\rightarrow$  Access Control Lists. Click New.

Step 2 Use ACL-AGENT-REDIRECT as the ACL name, as shown in Figure 8.

Figure 8 Adding New ACLs to Cisco WLC

uluilu cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY		C <u>O</u> MMANE
Security	Access 0	Control L	ists > New				
AAA     General     RADIUS	Access Co	ontrol Lis	t ACL-AG	ENT-REDIRECT	2	-	_
<ul> <li>RADIUS         <ul> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> </ul> </li> <li>TACACS+         <ul> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Password Policies</li> </ul> </li> <li>Local EAP</li> <li>Priority Order</li> <li>Certificate</li> <li>Access Control Lists         <ul> <li>Access Control Lists</li> <li>CPU Access Control Lists</li> </ul> </li> </ul>	ACL Type	2	€ IPv	4			

Note: The ACL to be applied to a user session has to be predefined on the WLC. The name used in the Cisco ISE authorization profile should exactly match the ACL name on the WLC.

Step 3 Click ACL-AGENT-REDIRECT ACL, as shown in Figure 9.

Figure 9 Adding Rules to ACLs on Cisco WLC

رابیاب cısco	<u>M</u> ONITOR <u>W</u> LANs	CONTROLLER	WIRELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE
Security	Access Control L	ists					
▼ AAA General ▼ RADIUS Authentication	Enable Counters			Тур	e		
Accounting Fallback TACACS+ LDAP	ACL-AGENT-REDIREC	I 🔶	-	IPv4			
Local Net Users							

Step 4 Click Add New Rule. Use the values shown in Figure 10.

Step 5 Click Apply after each set of values and select Add New Rule for the next rule.

Security	Access Cor	ntrol Lists > Edit								
AAA     General     DADUIS	General									
Authentication	Access List Nam	e ACL-AGEN	T-REDIRECT							
Accounting Fallback TACACS+	Deny Counters	0								
LDAP	Seq Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
MAC Filtering Disabled Clients	1 Permit	0.0.0.0 /	0.0.0.0 /	ICMP	Any	Any	Any	Any	0	
User Login Policies AP Policies Password Policies	2 Permit	0.0.0.0 /	0.0.0.0 /	UDP	DNS	Any	Any	Any	0	
Local EAP	<u>3</u> Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0	
Priority Order     Certificate	4 Permit	0.0.0.0 / 0.0.0.0	10.1.100.3 / 255.255.255.255	тср	Any	8443	Any	Inbound	0	
<ul> <li>Access Control Lists</li> </ul>	<u>5</u> Permit	10.1.100.3 / 255.255.255.255	0.0.0.0 /	ТСР	8443	Any	Any	Outbound	0	
Access Control Lists CPU Access Control Lists FlexConnect ACLs	<u>6</u> Permit	0.0.0.0 / 0.0.0.0	10.1.100.3 / 255.255.255.255	тср	Any	8905	Any	Inbound	0	
Wireless Protection	7 Permit	10.1.100.3 / 255.255.255.255	0.0.0.0 / 0.0.0.0	тср	8905	Any	Any	Outbound	0	
Web Auth	<u>8</u> Permit	0.0.0.0 / 0.0.0.0	10.1.100.3 / 255.255.255.255	UDP	Any	8905	Any	Inbound	0	
TrustSec SXP Advanced	9 Permit	10.1.100.3 / 255.255.255.255	0.0.0.0 /	UDP	8905	Any	Any	Outbound	0	
	<u>10</u> Permit	0.0.0.0 / 0.0.0.0	10.1.100.3 / 255.255.255.255	тср	Any	8909	Any	Inbound	0	
	11 Permit	10.1.100.3 / 255.255.255.255	0.0.0.0 /	тср	8909	Any	Any	Outbound	0	
	12 Permit	0.0.0.0 / 0.0.0.0	10.1.100.3 / 255.255.255.255	UDP	Any	8909	Any	Inbound	0	
	<u>13</u> Permit	10.1.100.3 / 255.255.255.255	0.0.0.0 / 0.0.0.0	UDP	8909	Any	Any	Outbound	0	

Step 6 Confirm that the ACL is configured correctly.

Note: When a client is in the preposture state (POSTURE\_REQ as defined in the WLC), the default behavior of the WLC is to block all traffic except DHCP/DNS. The PRE-POSTURE ACL (which is called in the url-redirect-acl AV Pair received for Cisco ISE) is applied to the client, and it can reach only resources specifically allowed in the ACL.

#### Procedure 7 Add an Airespace ACL to Permit All Traffic

We will also create another access list to permit all traffic.

Step 1 Follow the steps in the section "Create an Airespace ACL for Posture Assessment" to create an ACL:

Table 4 shows the ACL-ALLOW settings for the WLC.

Table 4 ACL-ALLOW Settings for Wireless LAN Controller

ACL-ALLOW				
Sequence	1			
Source	Any			
Destination	Any			
Protocol	Any			
DSCP	Any			
Direction	Any			
Action	Permit			

## Procedure 8 Create Dynamic Interfaces for the Employee and Guest VLANs

We will be creating two different Service Set IDs (SSIDs) for wireless networks. One will be used for employees and the other for guests. Each SSID can be mapped to an individual dynamic interface. The following steps will walk you through the process of creating dynamic interfaces on the Cisco WLC.

Step 1 From the WLC GUI, navigate to Controller  $\rightarrow$  Interfaces and click New (Figure 11).

Figure 11 Adding	Dynamic	Interfaces to	Cisco WIC
i iguit i i nuuliig	Dynamic	multiaces u	

ululu cisco	<u>M</u> ONITOR <u>W</u> LANs		<u>S</u> ECURITY	M <u>A</u> NAGEMENT C <u>O</u> M	MANDS HELP <u>F</u> EEDBACK
Controller	Interfaces				
General Inventory	Interface Name	VLAN Identifie	er IP Address	Interface Type	Dynamic AP Management
Interfaces	management	untagged	10.1.60.2	Static	Enabled
Interface Groups	service-port	N/A	0.0.0.0	Static	Not Supported
Multicast	<u>virtual</u>	N/A	1.1.1.1	Static	Not Supported
Network Routes					

#### Step 2 Use the values listed in Table 5 and click Apply.

Table 5 Create a Dynamic Interface for Employee

Attribute	Value
Interface Name	Employee
VLAN id	10

### Step 3 Enter the values listed Table 6 for the Employee Interface.

Table 6 Settings for the Employee Dynamic Interface

Attribute	Value
Port Number	1
VLAN Identifier	10
IP Address	10.1.10.2
Netmask	255.255.255.0
Gateway	10.1.10.1
DHCP	10.1.100.100

## Step 4 Repeat the steps to create a dynamic interface for guests (see Tables 7 and 8).

#### Table 7 -Create a Dynamic Interface for Guests

Attribute	Value
Interface Name	Guest
VLAN id	20

## Table 8 Settings for the Guest Dynamic Interface

Attribute	Value
Port Number	1
VLAN Identifier	20
IP Address	10.1.20.2
Netmask	255.255.255.0

Gateway	10.1.20.1
DHCP	10.1.100.100

## Step 5 Save the configuration (Figure 12).

Figure 12 Verify the Dynamic Interface Configuration

uluulu cisco	MONITOR WLANS	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	MANAGEMENT CC	MMANDS	HE <u>L</u> P <u>F</u> EEDBACI
Controller	Interfaces						
General Inventory	Interface Name	VLA	N Identifier	IP Address	Interface Typ	e Dynamic	AP Management
Interfaces	employee	10		10.1.10.2	Dynamic	Disabled	
Interface Group	guest	20		10.1.20.2	Dynamic	Disabled	
Multicast	management	unta	igged	10.1.60.2	Static	Enabled	
Network Routes	service-port	N/A		0.0.0.0	Static	Not Supp	orted
Internal DHCP Server	virtual	N/A		1.1.1.1	Static	Not Supp	orted

# Adding 802.1X and Central Web Authentication SSIDs

#### Procedure 1 Add an 802.1X WLAN for Employees

We will now configure the SSID with the appropriate security settings to enable 802.1X authentication with Cisco ISE defined as the RADIUS server.

Step 1 From the WLC, navigate to WLANs  $\rightarrow$  WLAN ID to modify the SSID defined at bootstrap. If you want to define a new SSID, click WLANs  $\rightarrow$  Create New  $\rightarrow$  Go (Figure 13).

## Figure 13 Adding an 802.1X WLAN

uluilu cisco	<u>m</u> onitor <u>w</u> lans	NUTROLLER WIRELESS	<u>S</u> ECURITY M <u>A</u> NAGEMENT	C <u>o</u> mmands he <u>l</u> p <u>e</u> e	Sa EEDBACK	v <u>e</u> Configuratio
WLANs	WLANs					
WLANS	Current Filter: None	[Change Filter] [Cle	ar Filter]	Create New	- Go 🔶	
Advanced	WLAN ID Type	Profile Name CTS-CORP	WLAN SSID CTS-CORP	Admin Status Enabled	Security Policies [WPA2][Auth(802.1X)]	

Step 2 Set the values for the General tab of the WLAN settings (Figure 14).

Figure 14 General Tab Settings for the 802.1X WLAN

WLANs > Edit 'CTS-C	ORP'
General <del>Sec</del> urity	QoS Advanced
Profile Name Type SSID	CTS-CORP WLAN CTS-CORP
Status	✓ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy Interface/Interface Group(G)	All Map the SSID to the Employee VLAN
Multicast Vlan Feature	Enabled
Broadcast SSID	🔽 Enabled

Step 3 Set the values listed for the Security  $\rightarrow$  Layer 2 tab (Figure 15).

WLANs > Edit 'CTS-CORP'				
General	Security	Q <b>4</b> 5 A	dvanced	
Layer 2	dayer 3	AAA Serv	ers	
Layer 2	Security 🧕 🗍	WPA+WPA2	<b>▼</b>	
WPA+WPA	12 Paramete	ers		
WPA Po WPA2 P	olicy			
WPA2 E	WPA2 Encryption		Пткір	
Auth Key Mgmt		802.1X	•	

Step 4 Set the values listed for the Security  $\rightarrow$  AAA servers tab (Figure 16).

Figure 16 Mapping RADIUS Servers for the 802.1X WLAN

/LANs > Edit 'CTS-COF	P'				
General Security	J <del>S A</del> dvanced				
Layer 2 Layer 3	Layer 2 Layer 3 AAA Servers				
	a guarrida usa of datault sorugrs on this WIAN				
Select AAA servers below	U OVERTIDE USE OF DETAULT SERVETS OF THIS WEAR				
Select AAA servers below Radius Servers					
Radius Servers Delow	nterface Enabled				
Radius Servers Delow Radius Servers Radius Server Overwrite	nterface Enabled				
Radius Servers Delow Radius Servers Radius Server Overwrite	nterface  Enabled Authentication Servers Accounting Servers Enabled Enabled Enabled				
Radius Servers Delow Radius Server Overwrite Server 1	Authentication Servers Accounting Servers ✓ Enabled IP:10.1.100.3, Port:1812 ✓ IP:10.1.100.3, Port:1813				
Select AAA servers below Radius Servers Radius Server Overwrite Server 1 Server 2	terface □Enabled Authentication Servers Accounting Servers ✓ Enabled ✓ Enabled IP:10.1.100.3, Port:1812 ✓ IP:10.1.100.3, Port:1813 None ✓ None				

Step 5 Set the values for the Advanced tab (Figure 17).

Figure 17 Advanced Settings for the 802.1X WLAN

LANs > Edit 'CTS-CC	DRP'	
General Security	QoS Advanced	
Allow AAA Override	S Enabled	DHCP
Coverage Hole Detection	✓ Enabled	DHCP Server Override
Enable Session Timeout	Session Timeout (secs)	DHCP Addr. Assignment 🛛 🗹 Required
Aironet IE	✓Enabled	Management Frame Protection (MFP)
Diagnostic Channel	Enabled	
Override Interface ACL	IPv4 None + IPv6 None +	MFP Client Protection 4 Optional +
P2P Blocking Action	Disabled +	DTIM Period (in beacon intervals)
Client Exclusion <sup>3</sup>	✓Enabled Timeout Value (secs)	802.11a/n (1 - 255) 1
Maximum Allowed Clients	0	802.11b/g/n (1 - 255) 1
<u>e</u> e: :: :::::::::::::::::::::::::::::::		NAC
Static IP Tunneling ==		NAC State Radius NAC 🗧
WI-FI Direct Clients Policy		Load Balancing and Band Select
Per AP Radio	200	Client Load Balancing
Off Channel Scanning Defe	r	Client Band Select Z
Scan Defer Priority	0 1 2 3 4 5 6 7	Passive Client
		Passive Client
Scan Defer Time(msecs)	100	Voice
lexConnect		Media Session Snooping   Enabl
FlexConnect Local		Re-anchor Roamed Voice Clients 📄 Enabl
Switching <sup>2</sup>		KTS based CAC Policy   Enabl
FlexConnect Local Auth 12	Enabled	Client Profiling
Learn Client IP Address 5	Senabled	DHCP Profiling

Note: The RADIUS NAC setting is required for CoA enforcement. Although we define it at this stage, it will not have any effect until Cisco ISE is configured to send the redirect Vendor Specific Attribute (VS) to the WLC to invoke the preposture assessment ACL.

Step 6 Click Apply to save the WLAN settings.

## Procedure 2 Add an Open SSID for Wireless Central Web Authentication

This procedure will walk you through the steps to configure a SSID for Central Web Authentication (CWA).

Note: Support for Wireless Central Web-Auth is available only in Cisco Wireless LAN Controller Software Version 7.2 and above. For configuring local Web Authentication, refer to the Cisco TrustSec 2.0 Design and Implementation Guide available at: http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec\_2.0/trustsec\_2.0\_dig.pdf

Step 1 From the WLC GUI, navigate to WLANs  $\rightarrow$  Create New  $\rightarrow$  Go.

Step 2 Enter the values in Table 9 and click Apply.

Table 9 SSID Settings for Central Web Authentication

Attribute	Value
Profile Name	CTS-GUEST-CWA
SSID	CTS-GUEST-CWA

#### Step 3 Set the values in the General tab of the WLAN settings (Figure 18).

Figure 18 General Tab Settin	igs for Open SSID
WLANs > Edit 'CTS-G	UEST-CWA'
General <del>Scority</del>	QoS Advanced
Profile Name Type SSID Status	CTS-GUEST-CWA WLAN CTS-GUEST-CWA Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	guest Map SSID to the
Multicast Vlan Feature	Enabled     Guest VLAN
Broadcast SSID	I Enabled

Step 4 Set the values in Layer 2 tab under Security (Figure 19).

Figure 19 Layer 2 Security settings for Open SSID Using CWA
WLANs > Edit 'CTS-GUEST-CWA'
General Security <del>QeS</del> Advanced
Layer 2 Asyor-3 AAA Servers
Layer 2 Security 💁 None 🗸 🗸
🔽 2MAC Filtering 🔫

Step 5 Set the values for the AAA Servers under the Security tab (Figure 20).

Figure 20 Mapping RADIUS Servers for the Open SSID Using CWA

WLANs > Edit 'CTS-GUEST-CW/	۹.			
General Security 405 A	dvanced			
Layer 2 Layer 3 AAA Serv	vers 🔶			
Select AAA servers below to overr	ide use of default servers	on this WLAN		
Radius Servers			LDAP Server	<b>'</b> 5
Radius Server Overwrite interface	Enabled		Server 1	None 👻
	Authentication Servers	Accounting Servers	Server 2	None 👻
	🗷 Enabled 🛛 🗲 💳	🗷 Enabled 🛛 🛨	Server 3	None 👻
Server 1	IP:10.1.100.3, Port:1812 👻	IP:10.1.100.3, Port:1813 👻		
Server 2	None 👻	None 👻		
Server 3	None -	None 🗸		

Step 6 Set the values for the Advanced tab (Figure 21).

Figure 21 Advanced Settings for the Open SSID Using CWA

WLANs > Edit 'CTS-GU	IEST'	
General Security	QoS Advanced	
Allow AAA Override	Senabled	DHCP
Coverage Hole Detection	C Enabled	DHCP Server Override
Enable Session Timeout	1800	
	Session Timeout (secs)	DHCP Addr. Assignment 🗌 Required
Aironet IE	✓Enabled	Management Frame Protection (MFP)
Diagnostic Channel	Enabled	
Override Interface ACL	IPv4 None + IPv6 None +	MFP Client Protection 4 Optional \$
P2P Blocking Action	Disabled +	DTIM Period (in beacon intervals)
Client Exclusion <sup>3</sup>	✓Enabled Timeout Value (secs)	802.11a/n (1 - 255) 1
Maximum Allowed Clients	0	802.11b/g/n (1 - 255) 1
8		NAC
Static IP Tunneling		NAC State Radius NAC 🗧 🕇 🗕
Wi-Fi Direct Clients Policy	Disabled 🗘	Load Balancing and Band Select
Maximum Allowed Clients Per AP Radio	200	Client Load Balancing
Off Channel Scanning Defe	r	Client Band Select Z
Scan Defer Priority	0 1 2 3 4 5 6 7	Passive Client
		Passive Client
Scan Defer Time(msecs)	100	Voice
FlexConnect		Media Session Snooping 📃 Enabled
FlexConnect Local		Re-anchor Roamed Voice Clients 🗌 Enabled
Switching <sup>2</sup>		KTS based CAC Policy   Enabled
FlexConnect Local Auth 12	Enabled	Client Profiling
Learn Client IP Address 5	Similar Enabled	DHCP Profiling 🛛 🚽 🗹 Enabled

Note: It is important to enable AAA Override to allow attributes from the AAA server to be applied.

Step 7 Save the WLC configuration.

# Configuring Cisco ISE for Wireless Authentication

Procedure 1 Configure Cisco ISE to accept Wireless authentication requests.

We are done with the basic Cisco WLC configuration. We will now configure Cisco ISE to process RADIUS requests from the Cisco WLC.

Step 1 Follow the *ISE Base Configurations: ISE Bootstrapping How-To Guide* to add the Cisco WLC as a network access device to Cisco ISE.

Step 2 From Cisco ISE, navigate to Policy  $\rightarrow$  Authentication.

Step 3 Expand the IF conditions for the MAB rule and select Add Condition from Library (Figure 22).

Figure 22 Adding Conditions to ISE Authentication Rules

Authentication Policy		
Define the Authentication Policy by selecting the protoc Policy Type O Simple   Rule-Based	ols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.	
MAB : If	Wired_MAB AN Oliver allow protocols Allowed Protocol : Default Netwo and	👾 Actions 🔻
Dot1X : If	Add All Conditions Below to Library	🙀 Actions 👻
Default Rule (If no match) : al	Condition Name Expression	🙀 Actions 👻
	Add A Add (	Attribute/Value Condition from Library 🚤
	Delet	e

## Step 4 From the Select Condition drop-down menu, select Compound Condition → Wireless\_MAB (Figure 23).

cisco Identity Services Engine		ise admin Logout Feedbilet
A Home Operations ▼ Policy ▼ Administration ▼		😶 Task Navigator 👻 😣
Authentication Authorization Profiling Operator	🕞 Client Provisioning 📄 Security Group Access 🥵 Policy Elements	
Authentication Policy		
Define the Authentication Policy by selecting the protocols that ISE should use to con Policy Type O Simple      Rule-Based	municate with the network devices, and the identity sources that it should use for authentication.	
MAB : If Wired_MAB OR	allow protocols Allowed Protocol : Default Networs and	🙀 Actions 💌
Dot1X : If Add All Conditions	Below to Library	🖗 Actions 💌
Default Rule (If no match) : all	C C C C C C C C C C C C C C C C C C C	🖗 Actions 🔻
Select Condition	OR OR	ŵ•
	Compound Condition	
	Wired_802.1X	
	Wireless_802.1X	
	Switch_Local_Web_Authentication	
	WLC_Web_Authentication	
	Wireless_MAB	

Figure 23 Adding the Wireless\_MAB Condition to the Authentication Rule

Step 5 Expand the IF conditions for the Dot1X rule and select Add Condition from Library.

Step 6 From the Select Condition drop-down menu, select Compound Condition  $\rightarrow$  Wireless\_802.1X (Figure 24).

Figure 24 Adding the Wireless\_802.1X Condition to the Authentication Rule

ali ali	Compound Condition	
CISCO Identity Services Engine	٩	ise-node1 admin Logout F
🛕 Home Operations 🔻 Policy 🔻 Administration 🔻	🕂 🔲 📜 🔛	😁 Task Navigator 👻
Authentication Authorization Confine Construct	Wired_MAB	
	Wired_802.1X	
Authentication Dolicy	Wireless_802.1X	<u> </u>
Perfers the Authentication Policy in relation the meteorie that 105 day id use to	Switch_Local_Web_Authentication	d dha bilandhu an mar dhab li aka did ya ƙwa a dhawilandan
Policy Type O Simple      Rule-Based	WLC_Web_Authentication	a the identity sources that it should use for authentication.
	Wired_802.1X_PEAP	
If Wired_MAB	Wired_802.1X_TEST	fault Netwoo and 🕨 🎬 Actions 👻
	Wired_802.1X_BUG	Charles and
	Aaron-Test	rault Netwood and
Default Rule (If no match) : all 💾 Add All Conditions B		🖗 Actions 🕶
Condition Name		AND -
Wired_802.1X		AND 🚔 🖌
# [Wireless_802.1X	A condition to match an 802.1X b	lased authentication req. ∰ ↓ ↓

Cisco ISE is now ready to accept RADIUS requests originating from wireless networks. When it receives a RADIUS request from a wireless source, it will check to see if the authentication protocol is permitted or not. Typically, the default networks options allow all authentication protocols supported by Cisco ISE. The next step for Cisco ISE is to query the specified identity store to validate the credentials received.

# Apple Captive Network Assistant (CNA)

Apple introduced an iOS feature to facilitate network access when captive portals are present. This feature attempts to detect the presence of captive portal by sending a web request upon connecting to a wireless network, and directs the request to <a href="http://www.apple.com/library/test/success.html">http://www.apple.com/library/test/success.html</a>.

If a response is received, then Internet access is assumed and no further interaction is required. If no response is received, Internet access is assumed to be blocked by captive portal and CNA auto-launches the pseudo browser to request portal login in a controlled window.

CNA may break when redirecting to an ISE captive portal. WLC version 7.2 added a CLI command that will prevent the pseudo browser from popping up.

# Configure WLC to bypass CNA:

Procedure 1 Enable the Captive Bypass CLI

Step 1 Login to the WLC Command Line Interface

- Step 2 Enable the Captive Bypass Command
  - > config network web-auth captive-bypass enable

Step 3 Save the configuration on the controller

> save config

Step 4 You must reboot the controller to apply this change

> reset system in 00:01:01

# Cisco TrustSec System:

- <u>http://www.cisco.com/go/trustsec</u>
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing\_DesignZone\_TrustSec.html

# Device Configuration Guides:

Cisco Identity Services Engine User Guides: http://www.cisco.com/en/US/products/ps11640/products\_user\_guide\_list.html

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches: http://www.cisco.com/en/US/products/ps6406/products\_installation\_and\_configuration\_guides\_list.html
- For Cisco Catalyst 3000 series switches: <u>http://www.cisco.com/en/US/products/ps7077/products installation and configuration guides list.html</u>
- For Cisco Catalyst 3000-X series switches: http://www.cisco.com/en/US/products/ps10745/products\_installation\_and\_configuration\_guides\_list.html
- For Cisco Catalyst 4500 series switches: <u>http://www.cisco.com/en/US/products/hw/switches/ps4324/products\_installation\_and\_configuration\_guides\_list.ht</u> <u>ml</u>
- For Cisco Catalyst 6500 series switches: http://www.cisco.com/en/US/products/hw/switches/ps708/products\_installation\_and\_configuration\_guides\_list.html
- For Cisco ASR 1000 series routers: <u>http://www.cisco.com/en/US/products/ps9343/products\_installation\_and\_configuration\_guides\_list.html</u>

For Cisco Wireless LAN Controllers: http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html