Configure TACACS+ for Device Administration of Cisco WLC

Contents

Introduction
<u>Prerequisites</u>
Requirements
Components Used
<u>Configuration</u>
Step 1. Check Device Administration License.
Step 2. Enable Device Administration on ISE PSN Nodes.
Step 3. Create a Network Device Group.
Step 4. Add WLC as a Network Device.
Step 5. Create a TACACS Profile for WLC.
Step 6. Create a Policy Set.
Step 7. Create Authentication and Authorization Policies.
Step 8. Configure WLC for Device Administration.
Verify
<u>Troubleshoot</u>

Introduction

This document describes how to configure TACACS+ for device administration of Cisco Wireless LAN Controller (WLC) with Identity Service Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Identity Service Engine (ISE)
- Basic knowledge of Cisco Wireless LAN Controller (WLC)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Service Engine 2.4
- Cisco Wireless LAN Controller 8.5.135

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

Configuration

Step 1. Check Device Administration License.

Navigate to **Administration > System > Licensing** tab and verify **Device Admin** license is installed, as shown in the image.

dentity S	ervices Engine Ho	me	▸ Operations	✓ Administration	Work Centers					
▼ System → Id	entity Management	etwork Resources	Portal Management pxGrid	Services						
Deployment Li	Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings									
Licensing Metr	00 ()									
Traditional	Licensing is currently in (use.								
Click below	Click below to switch to Cisco Smart Licensing ()									
Cisco Smar	Licensing									
License Usage Current Usage	How are licenses consume Usage Over Time	od?								
	Base									
	0			Lic	ensed :100 (Consumed :0)	0				
	Plus									
Advanced										
L	Apex									
	Updated : Aug 20,2019 09:3	30:00 UTC 👔 📃 Licensed	Consumed Exceeded							
Licenses (i) H	low do I register,modily or lookup	my licenses?								
Import License	Delete License									
	License File	Quantity	Terr	n	Exp	piration Date				
▼ □	POSITRONFEAT2019082	20025931403.lic								
	Base	100	Term	1	19-/	Aug-2020 (365 days remaining)				
▼ □	POSITRONFEAT2019082	20025911402.lic								
	Device Admin	50	Terr	1	19-/	Aug-2020 (365 days remaining)				

Note: Device admin license is required to use the TACACS+ feature on ISE.

Step 2. Enable Device Administration on ISE PSN Nodes.

Navigate to **Work Centers > Device Administration > Overview**, click **Deployment** tab, select the **Specific PSN Node** radio button. Enable Device Administration on the ISE node by selecting the **checkbox** and click **Save**, as shown in the image:

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Network Access Guest Access	TrustSec Device Administration PassiveID
✓ Overview → Identities User Iden	tity Groups Ext Id Sources + Network Resources + Policy Elements Device Admin Policy Sets Reports Settings
0	,
Introduction	Device Administration Deployment
TACACS Livelog	Activate ISE Nodes for Device Administration
Deployment	All Policy Service Nodes
	Specific Nodes
	ISE Nodes
	ISE-PSN.panlab.local
	Onto JOE Nodes with Deliver One day and displayed
	Univ ISE Nodes with Policy Service are displayed.
	TACACS Ports * 49
	Save Reset

Step 3. Create a Network Device Group.

In order to add WLC as a network device on the ISE, navigate to **Administration > Network Resources > Network Device Groups > All Device Types**, create a new group for WLC, as shown in the image:

dentity Services Er	ngine Home	▶ Context Visibility	 Operations 	▶ Policy ▼Adi	ministration V	ork Centers
 System Identity Mana 	igement - Network	k Resources > Device	Portal Management	pxGrid Services	▶ Feed Service	Threat Centric NAC
Network Devices Netwo	ork Device Groups	Network Device Profiles	External RADIUS	Servers RADIUS	Server Sequences	NAC Managers Ex
Network Device Group	S					
All Groups Choose	se group 🕶					
${\cal G}$ Refresh $+$ Add	Duplicate 🖸 Ed	dit <u> </u> Trash 💿 S	Show group members	s 🚊 Import	≛ Export 👻 🔳 F	lat Table 🦨 Expand
Name			De	scription		
 All Device Types 			All	Device Types		
All Locations			All I	Locations		
→ Is IPSEC Device			Is th	his a RADIUS over I	PSEC Device	

Add Group		~
Name *	WLC	
Description		
Parent Group *	All Device Types	x T
		Cancel Save

Step 4. Add WLC as a Network Device.

Navigate to Work Centers > Device Administration >Network Resources > Network Devices. Click Add, provide Name, IP Address and select the Device type as WLC, select TACACS+ Authentication Settings checkbox and provide the Shared Secret key, as shown in the image:

cisco	Identity Ser	vices Engine	Home	Context	Visibility	 Operations 	Policy	 Administration 	Work Centers
► Sys	stem Iden	tity Management	✓ Networ	rk Resources	Device	Portal Manageme	nt pxGrid S	Services	
▼ Net	twork Devices	Network Device	Groups	Network Device	ce Profiles	External RADIU	IS Servers	RADIUS Server Seque	ences
Networ Default Device	k Devices t Device Security Settir	ıgs	3 Netwo	ork Devices List	> New Netv es	Name Flo Description	orWLC		
				IP Address	· · ·	IP: 10.106.37	.180		/ 32
				* Network Dev Location [IPSEC [* D Softw rice Group <u>All Location:</u> Is IPSEC De	Nodel Name ware Version	Cisco 🔹 🕀		
			- I	Device Type	WLC	0	Set To Default	t	
				- DADUIG		0.4%			
				► RADIUS A	Authenticatio	on Settings			
			⊻	TACACS	Authenticatio	on Settings			
						S Enable Single C	hared Secret	Legacy Cisco Dev TACACS Draft Co	Show vice ompliance Single Connect Support
				► SNMP Set	ttings				

Step 5. Create a TACACS Profile for WLC.

Navigate to Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles. Click Add and provide a Name. In the Task attribute view tab, select WLC for Common Task Type. There are default profiles present from which select Monitor to allow limited access to users, as shown in the image.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Network Access Guest Access	TrustSec BYOD Profiler Posture Device Administration PassiveID
Overview Identities User Ident	ity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings
Overview Identities User Ident Overview Identities User Ident Overview Conditions Network Conditions Results Allowed Protocols TACACS Command Sets TACACS Profiles	ity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings TACACS Profiles > WLC MONITOR Name WLC MONITOR Description WLC MONITOR Task Attribute View Raw View Common Tasks Vert vert
	 All Monitor Lobby Selected WLAN Controller Wireless Security Management Commands The configured options give a mgmtRole Debug value of: 0x0 €

There is another default profile All which allows full access to the user as shown in the image.

Identity Services Engine	Home	ions ► Policy ► Administration
Network Access Guest Access	TrustSec BYOD Profiler Pos	ture
Overview Identities User Identi	ty Groups Ext Id Sources	ources Policy Elements Device Admin Policy Sets Reports Settings
Conditions	TACACS Profiles > WLC ALL	
Network Conditions	TACACS Profile	
▼ Results	Name	WLC ALL
Allowed Protocols	Description	WLC ALL
TACACS Command Sets		
TACACS Profiles	Task Attribute View Ra	w View
	Common Tasks	
	Common Task Type WLC	
	O All	
	Monitor	
	C Lobby	
	Selected	
	The configured options give	Introller Wireless Security Management Commands
	Custom Attributes	

Step 6. Create a Policy Set.

Navigate to **Work centers > Device administration > Device Admin Policy Sets.** Click (+) and give a name to the Policy Set. In the policy condition select **Device Type** as WLC, Allowed protocols can be **Default Device Admin**, as shown in the image.

cisco Identity Services Engine Home	Context Visibility Operations	Policy Administration Work Centers	License Warning 🔺 🔍 🎯 🗢 🌣
Network Access Guest Access TrustSec Overview Identities User Identity Groups	BYOD Profiler Posture Ext Id Sources Network Resource	Policy Elements Device Admin Policy Sets Reports Settings	Click here to do wireless setup Do not show this again. X
Policy Sets			Reset Save
+ Status Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Search			
⊘ wLC		DEVICE-Device Type EQUALS All Device Types#WLC	Default Device Admin × × + 0 ♦ >

Step 7. Create Authentication and Authorization Policies.

In this document, two sample groups **Admin-Read-Write** and **Admin-Read-Only** are configured on the Active directoryand one user inside each group **admin1**, **admin2** respectively. Active Directory is integrated with the ISE via a joinpoint named **AD-JointName**.

Create two authorization policies, as shown in the image:

/	0	Default			AD-JointName × v > Options	0	۰		
> Auth	orization F	Policy - Local Exceptions							
Authorization Policy - Global Exceptions									
♥ Auth	orization F	Policy (3)							
٠	Status	Rule Name	Conditions	Results Command Sets	Shell Profiles	Hits	Actions		
Search	h								
	Ø	WLCAdmin	AD-JointName-ExternalGroups EQUALS panlab.local/Users/Admin-Read- Write	+	WLC ALL × * +	0	٥		
	Ø	WLCMonitor	AD-JointName-ExternalGroups EQUALS panlab.local/Users/Admin-Read- Only	+	WLC MONITOR × * +	0	٥		
	Ø	Default		× DenyAllCommands +	Deny All Shell Profile x v +	0	٥		

Step 8. Configure WLC for Device Administration.

Navigate to **Security** > **AAA** > **TACACS**+ click **New** and add Authentication, Accounting server, as shown in the image.

cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	С <u>о</u> мм
Security	TACACS	• Auther	ntication Serv	ers > New			
 AAA General RADIUS Authentication Accounting Fallback DNS Downloaded AVP TACACS+ Authentication Accounting Authorization Fallback DNS 	Server Ind Server IP Shared Se Shared Se Confirm S Port Numl Server Sta Server Tir	dex (Priorit Address(Ip ecret Forma ecret chared Secr ber atus meout	y) ov4/Ipv6) at ret	1 0.106.37.18 ASCII 0 ••••• 49 Enabled 0 5 second	30 ds		

ıı ııı ı، cısco	<u>M</u> ONITOR <u>W</u> LANs <u>C</u> C	NTROLLER WIRE	LESS <u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS
Security	TACACS+ Accountin	g Servers > Nev	N		
 AAA General RADIUS Authentication Accounting Fallback DNS Downloaded AVP TACACS+ Authentication Accounting Authorization Fallback 	Server Index (Priority) Server IP Address(Ipv4/Ipv6) Shared Secret Format Shared Secret Confirm Shared Secret Port Number Server Status Server Timeout	1 0.106.37.13 ASCII 0 ••••• 49 Enabled 5 second	30 ds		

Change priority order and make TACACS+ on top and Local to bottom, as shown in the image:

CISCO	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C
Security	Priority C)rder > N	lanagement U	lser			
 AAA Local EAP Advanced EAP Priority Order Management User Certificate 	Authentic Not RAD	Used IUS	>	Order U	sed for Authe TACACS+ LOCAL	entication Up Do	wn
 Access Control Lists Wireless Protection Policies Web Auth 	If LOCAL is s LOCAL only i	elected as if first prior	second priority the ity is unreachable.	en user will be a	authenticated a	against	
Caution : Do not close	se the curren	t WLC G	UI session. Its r	ecommended	d to open WI	LC GUI in diffe	rent

web-browser and check whether login with TACACS+ credentials works or not. If not, verify the configuration and connectivity to the ISE node on TCP port 49.

Verify

Navigate to **Operations > TACACS > Live logs** and monitor the **Live Logs**. Open WLC GUI and log in with Active Directory user credentials, as shown in the image

ululu cisco	Identity Services Engine	Home 🔸	Context Visibility	✓ Operations	Policy → Adm	inistration	nters		
▶ R/	ADIUS Threat-Centric NAC Live L	.ogs TACAO	CS + Troubles	hoot + Adaptive	Network Control Rep	orts			
Live	Logs								
							Refresh Never	Show Latest 20 record	
c	Refresh 💆 Export To 🕶								
	Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Network Device	
×		2	•	Identity	•	Authentication Policy	Authorization Policy	Network Device Nam	
	Oct 03, 2019 03:15:55.969 PM	~	Q	admin2	Authorization		WLC >> WLCAdmin	FloorWLC	
	Oct 03, 2019 03:15:55.938 PM	Z	Q	admin2	Authentication	WLC >> Default		FloorWLC	
	Oct 03, 2019 03:15:39.298 PM	~	0	admin1	Authorization		WLC >> WLCMonitor	FloorWLC	
	Oct 03, 2019 03:15:39.268 PM		Q	admin1	Authentication	WLC >> Default		FloorWLC	
Last Updated: Thu Oct 03 2019 15:16:26 GMT+0530 (India Standard Time)									

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.