



无线局域网控制器的 ISE TACACS+ 配置 指南

安全访问操作指南用户系列

作者: Aruna Yerragudi(由 Hsing-Tsu Lai 编辑) 日期: 2015 年 12 月



目录

皆南简介	3
概述	. 3
使用本指南	. 3
使用的组件	. 3
设备管理的 ISE 配置	. 4
在 ISE 上许可设备管理	. 4
在 ISE 上启用设备管理	. 4
设备管理工作中心	. 5
配置网络设备和网络设备组	. 5
定义身份库	. 7
配置 TACACS 配置文件	. 8
设备管理策略集	. 9
ACACS+ 的 WLC 配置	12
添加 TACACS+ 身份验证服务器	12
添加 TACACS+ 授权服务器	13
添加 TACACS+ 记帐服务器	13
配置管理用户身份验证的优先级顺序	14
5续内容	15

指南简介

概述

增强型终端访问控制器访问控制系统 (TACACS+) 是为用户提供集中式安全控制来获取对路由器或任何网络访问设备的管理访问权限的客户端-服务器协议。TACACS+ 提供以下 AAA 服务:

- 身份验证 用户是谁
- 授权 允许用户执行什么操作
- 记帐-谁做过什么以及时间

本文档提供以思科身份服务引擎 (ISE) 作为 TACACS+ 服务器并以思科无线局域网控制器 (WLC) 作为 TACACS+ 客户端的 TACACS+ 配置示例。

使用本指南

本指南将活动划分为两个部分,以启用 ISE 来管理 WLC 的管理员访问权限。

- 第1部分-为设备管理配置 ISE
- 第2部分 为 TACACS+ 配置 WLC

使用的组件

本文档中的信息基于以下软件和硬件版本:

- ISE 版本 2.0
- 使用 AireOS 软件版本 7.6 和 8.0 的 WLC

本文档中的信息是从实验室环境中的设备所创建。所有设备最初都采用出厂(默认)配置。

设备管理的 ISE 配置

在 ISE 上许可设备管理

设备管理根据部署获得许可,但是需要现有且有效的 ISE 库或移动许可证。

在 ISE 上启用设备管理

在 ISE 节点中,默认情况下未启用设备管理服务 (TACACS+)。第一步是启用该服务。

- **第 1步:** 使用其中一个受支持的浏览器登录到 ISE 管理 Web 门户。
- **第 2 步:** 导航到**管理 (Administration) > 系统 (System) > 部署 (Deployment)**。选中 ISE 节点的对应复选框, 然后点击**编辑 (Edit)**。



图 1. ISE 部署页面

第 3 步: 在**常规设置** (General Settings)下,向下滚动并选中启用设备管理服务 (Enable Device Admin Service)的对应复选框。

cisco Identity Services Engine Home	Operations Policy Guest Access	Administration Work Centers	🕕 License Warning 🔺 🔍 🐵 🏦 🌣
System Identity Management Network F	Resources	Services Feed Service Identity Mapping	
System Identity Management Network F Deployment Leensing Certificates Log Deployment ·································	Resources	Bervice Isontty Mapping Enable SXP Service U Enable Device Admin Servi Enable Identity Mapping pxGrid i ace Oppositement 0 i <lii< li=""> <lii< li=""> i <lii< li=""></lii<></lii<></lii<>	Jse Interface GigabitEthernet 0 v (i) nice (i)
	L		

图 2. ISE 部署常规设置

第 4步: 保存 (Save) 配置。此时在 ISE 上已启用设备管理服务。

设备管理工作中心

ISE 2.0 引入了 TrutSec 和设备管理工作中心。工作中心包含特定功能的所有元素。

第1步: 转至工作中心 (Work Centers) > 设备管理 (Device Administration) > 概述 (Overview)





设备管理概述提供设备管理使用案例所需的高级步骤。

配置网络设备和网络设备组

现在,让我们来探索网络设备和网络设备分组。

ISE 以多个设备组层次结构的形式提供强大的设备分组。每个层次结构都表示一个不同且独立的网络设备分类。

第1步: 导航到工作中心 (Work Centers) > 设备管理 (Device Administration) > 网络设备组 (Network Device Groups)

dhaho Gisco	Identity Services Engine	Home	Operations F	Policy • Guest Acce	ss • Administration	▼Work Centers			
♦ Tru	stSec								
Overv	iew Identities User Identit	y Groups	Network Resources	Network Device Grou	ps • Policy Conditions	 Policy Results 	Device Admin Policy Sets	Reports	Settings
Ne	twork Device Groups	(م	Network Devi	ce Groups					
<	· E ·	÷	🥖 Edit 🛛 🕂 Add	Duplicate XDelete	🔂 Import 🔹 Export 👻			Show 🛛	All
•	Croups		Name	-	Туре	Descriptio	n		
	All Device Types		All Device Ty	/pes	Device Type	All Device	Types		
	All Locations		All Location	s	Location	All Locatio	ns		



"所有设备类型"(All Device Types)和"所有位置"(All Locations)是 ISE 提供的默认层次结构。 您可以添加自己的层次结构或定义各种组件来识别稍后将在策略条件中使用的网络设备。 第2步: 在定义各种层次结构后, "网络设备组"(Network Device Groups)将如下所示:



图 5. 网络设备组树状视图

我们在此处添加了各种设备类型以及位置。

第 3 步:现在,请添加 WLC 作为网络设备。转至工作中心 (Work Centers) > 设备管理 (Device Administration) > 网络资源 (Network Resources)。点击添加 (Add) 以添加新的网络设备 DMZ_BLDO_vWLC。

* Name DMZ BLDO VWLC	
* Name DMZ BLDO vWLC	
Description Virtual WLC	
Address: 10.1.100.170 / 32	
* Device Profile dit Cisco 💌 🕀	
Model Name 🛛 👻	
Software Version 🔹	
work Device Group cation San Jose 📀 Set. To Default	
e Type Wireless Devices 📀 Set To Default	
ADIUS Authentication Settings	
ACACS+ Authentication Settings	
Shared Secret Sho	w
Enable Single Connect Mode 🗌	
Legacy Cisco Device	Single Connect Supp

图 6. 添加网络设备

输入设备的 IP 地址并确保映射设备的位置和设备类型。最后, 启用 TACACS+ 身份验证设置 (TACACS+ Authentication Settings)并指定共享密钥。

定义身份库

本节旨在定义设备管理员的身份库。身份库可以是 ISE 内部用户和/或任何受支持的外部身份源。对于此配置, 我们将使用外部身份源 Active Directory (AD)。

第1步: 导航到管理 (Administration) > 身份管理 (Identity Management) > 外部身份库 (External Identity Stores) > Active Directory。点击添加 (Add) 以定义新的 Active Directory 加入点。指定加入点名称和 AD 域名,然后点击提交 (Submit)。

cisco Identit	y Services Engine	Home	• Operations	Policy	• Guest Access	 Administration 	Work Centers	
• System	r Identity Management	• Network R	esources 🔸 D	evice Portal M	lanagement pxGri	id Services 🔹 🕨 Feed S	Service 🔹 Identity Mappin	ig
 Identities 	Groups External Ide	ntity Sources	Identity Source	Sequences	 Settings 			
External Io	lentity Sources		Conne	ction				
 Certin Activ 	 icate Authentication Profile Directory 	ŵ₊	* Jo * Active Di	oin Point Nam rectory Domai	ne demoAD in securitydemo.ne	t		(i) (i)

图 3. 添加 AD 加入点

第 2步: 当提示"是否要将所有 ISE 节点都加入到此 Active Directory 域?" (Would you like to Join all ISE Nodes to this Active Directory Domain?) 时点击是 (Yes)

输入具有 AD 加入权限的凭证,然后将 ISE 加入到 AD。检查状态以验证其是否可操作。

Connection Authentication Do	mains Gro	oups Attributes	Advanced Settings	
* Join Point Name demoAD			Ð	
* Active Directory Domain securitydemo.r	et		0	
👷 Join 👷 Leave 🤦 Test User 💼 Diagnostic	Tool 🛞 Refresh Tab	ble		
ISE Node	ISE Node Role	Status	Domain Controller	Site
ise-1.securitydemo.net	STANDALONE	🖾 Operational	demoAD.securitydemo.net	Default-First-Site-Name

图 4. 将 ISE 加入到 AD

第3步: 转至组 (Groups) 选项卡,然后点击添加 (Add) 以获取需要的所有组,基于这些组可授权用户进行 设备访问。下面显示本指南的授权策略中使用的组

Connection A	Authentication Domains Groups
🖊 Edit 🕂 Add 👻 🗙 Delete	Group Update SID Values
Name	
securitydemo.net/Demo	Groups/Contractors
securitydemo.net/Demo	Groups/Doctors
securitydemo.net/Demo	Groups/East_Coast
securitydemo.net/Demo	Groups/Employees
securitydemo.net/Demo	Groups/HelpDesk
securitydemo.net/Demo	Groups/Network_Operators
securitydemo.net/Demo	Groups/Nurses
securitydemo.net/Demo	Groups/Physicians
securitydemo.net/Demo	Groups/Security_Operators
securitydemo.net/Demo	Groups/Staff
securitydemo.net/Demo	Groups/Students
securitydemo.net/Demo	Groups/West_Coast
securitydemo.net/Users/	Domain Admins
securitydemo.net/Users/	Domain Computers
securitydemo.net/Users/	Domain Users
securitydemo.net/Users/	Super Device Admin

图 5. AD 组

配置 TACACS 配置文件

我们将定义要在授权策略中使用的三个 TACACS 配置文件 -

- WLC_Monitor_Only: 具有"监控"(Monitor)选项卡访问权限的服务中心
- WLC_Security_Access: 具有"安全"(Security)和"命令"(Commands)选项卡访问权限的安全操作员
- WLC_Admin: 具有完全访问权限的管理员。

WLC 使用需要定义为 role1、role2 等的 TACACS+ 自定义属性。可用角色为 MONITOR、WLAN、 CONTROLLER、WIRELESS、SECURITY、MANAGEMENT、COMMAND、ALL 和 LOBBY。前七个角色对 应于 WLC 管理 Web UI 上的菜单选项。您可以输入一个或多个角色来允许对特定功能进行读写访问,并对其 余功能进行只读访问。

要向 WLAN、SECURITY 和 CONTROLLER 授予读写访问权限,请输入以下文本:

role1=WLAN role2=SECURITY role3=CONTROLLER

 第1步:在ISE GUI 上,转至工作中心 (Work Centers) > 设备管理 (Device Administration) > 策略结果 (Policy Results) > TACACS 配置文件 (TACACS Profiles)。添加新的 TACACS 配置文件(称为 WLC_Monitor_Only)。向下滚动到自定义属性 (Custom Attributes) 部分以仅定义对 MONITOR 的访问权限。

Custom Attributes					
+Add	G Edit		o-		
Г Туре	Name	Value			
MANDATORY	role1	MONITOR	0 B		

图 6. WLC_Monitor_Only 的 TACACS 配置文件

点击保存 (Save) 以保存配置文件。

第 2 步: 添加另一个配置文件(称为 WLC_Security_Access)以提供对 SECURITY 和 COMMANDS 的访问 权限。

Custom Attributes			
+Add	G , Eqit		٥-
Г Ъре	Name	Value	
MANDATORY	role1	SECURITY	G 🛙
MANDATORY	role2	COMMANDS	c ii

图 7. WLC_Security_Access 的 TACACS 配置文件

点击保存 (Save) 以保存配置文件。

第 3步: 添加第三个配置文件(称为 WLC_Admin),通过以 role1=ALL 为属性来提供对所有选项卡的访问 权限。

Cust	om Attributes			
+	Add ∎Trash ▼ @E	dit		0-
Г	Туре	Name	Value	
П	MANDATORY	role1	ALL	G 🖩

图 8. WLC_Admin 的 TACACS 配置文件

设备管理策略集

对于设备管理,默认情况下会启用策略集。策略集可以根据设备类型划分策略,从而轻松应用 TACACS 配置 文件。例如,Cisco IOS 设备使用权限级别和/或命令集,而 WLC 设备则使用自定义属性。

第 1 步: 导航到工作中心 (Work Centers) > 设备管理 (Device Administration) > 设备管理策略集 (Device Admin Policy Sets)。添加具有以下条件的新策略集(称为 WirelessLanControllers) DEVICE:Device Type EQUALS Device Type#All Device Types#Network Device#Wireless Devices

Status	Name	Description	Conditions
	WirelessLanControllers		DEVICE:Device Type EQUALS Device Type#All Device Types#Network Devices#Wireless Devices

图 9. 策略集条件

第2步: 创建身份验证策略。对于身份验证,我们将使用 Active Directory 作为 ID 库。



图 10. 身份验证策略

第 3步: 定义授权策略。此处我们将根据 Active Directory 中的用户组和设备的位置来定义授权策略。例如, Active Directory 组 West Coast 中的用户只能访问位于 West Coast 的设备,而 Active Directory 组 East Coast 中的用户只能访问位于 East Coast 的设备。

S	规则名称	条件	Shell 配置文件
\checkmark	WLC HelpDesk West	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/ <mark>HelpDesk</mark> AND	WLC_Monitor_Only
		securitydemo.net/DemoGroups/West_Coast	
		DEVICE:Location CONTAINS All Locations#West_Coast	
\checkmark	WLC HelpDesk East	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/ <mark>HelpDesk</mark> AND	WLC_Monitor_Only
		demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND	
		DEVICE:Location CONTAINS All Locations#East_Coast	
\checkmark	WLC Security West	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/ <mark>Security_Operators</mark> AND	WLC_Security_Access
		demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND	
		DEVICE:Location CONTAINS All Locations#West_Coast	
\checkmark	WLC Security East	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/ <mark>Security_Operators</mark> AND	WLC_Security_Access
		demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND	
		DEVICE:Location CONTAINS All Locations#East_Coast	
\checkmark	WLC Admin E and W	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators AND	WLC_Admin
		demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND	
		demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast	

S	规则名称	条件	Shell 配置文件
	WLC Admin West	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND DEVICE:Location CONTAINS All Locations#West_Coast	WLC_Admin
	WLC Admin East	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND DEVICE:Location CONTAINS All Locations#East_Coast	WLC_Admin
\checkmark	Default	DenyAllCommands	

图 11. 授权策略

我们现在已完成 WLC 设备的设备管理的 ISE 配置



TACACS+的WLC 配置

为在 WLC 控制器中配置 TACACS+, 您需要完成下列步骤:

- 1. 添加 TACACS+ 身份验证服务器
- 2. 添加 TACACS+ 授权服务器
- 3. 添加 TACACS+ 记帐服务器
- 4. 配置管理用户身份验证的优先级顺序

添加 TACACS+ 身份验证服务器

完成下列步骤,以便添加 TACACS+ 身份验证服务器。

第 1步:从WLC GUI 中,导航到安全 (Security) > AAA > TACACS+ > 身份验证 (Authentication),然后点 击新建 (New)...

CISCO MONITOR WL	ANS <u>C</u> ONTROLLER	WIRELESS	SECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK
Security	TACACS+ Auth	entication S	Servers				New
AAA General General RADIUS Authentication Accounting Fallback DNS Downloaded AVP TACACS+ Authentication Accounting Authorization DNS	Server Index	Server Ad	dress(Ipv4/I	pv6)	Port A	dmin Stat	us

图 12. TACACS+ 身份验证服务器

第2步: 输入作为 TACACS+ 服务器的 ISE 服务器的 IP 地址,并输入共享密钥。

CISCO	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P
Security	TACACS	⊦ Authen	tication Serve	ers > New				
 AAA General RADIUS Authentication Accounting Fallback DNS 	Server In Server IP Shared S Shared S	dex (Priori • Address(I ecret Form ecret	ty) pv4/Ipv6) at	1 • 10.1.100.22 ASCII •				
Downloaded AVP TACACS+ Authentication	Confirm S Port Numl	Shared Sec ber	ret	•••••				
Accounting Authorization DNS	Server St Server Ti	tatus meout		Enabled 💌 5 second	İs			

图 13. 添加 TACACS+ 身份验证服务器

第 3 步: 点击应用 (Apply)。

添加 TACACS+ 授权服务器

完成下列步骤,以便添加 TACACS+ 授权服务器。

- **第 1步:**从WLC GUI 中,导航到安全 (Security) > AAA > TACACS+ > 授权 (Authorization),然后点击新 建 (New)...
- 第2步: 添加 ISE 服务器的 IP 地址作为服务器 IP 地址,并输入共享密钥。

A	ACC+ Author				_
Security TAC	ACOT AULIIO	ization Server	s > New		
 AAA General RADIUS Authentication Accounting Fallback DNS Downloaded AVP Co TACACS+ Authentication Accounting Se Authorization Se 	ver Index (Prior ver IP Address() red Secret Form red Secret ifirm Shared Sec t Number ver Status	ity) pv4/Ipv6) aat cret	1 • 10.1.100.22 ASCII • •••••• 49 Enabled •	 	

- 图 14. 添加 TACACS+ 授权服务器
- 第3步: 点击应用 (Apply)

添加 TACACS+ 记帐服务器

完成下列步骤,以便添加 TACACS+ 记帐服务器。

- **第 1 步:**从 WLC GUI 中,导航到**安全 (Security) > AAA > TACACS+ > 记帐 (Accounting)**,然后点击**新建** (New)...
- 第2步: 输入 ISE 服务器的 IP 地址作为服务器 IP 地址,并输入共享密钥。

CISCO	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	
CISCO Security AAA General RADIUS Authentication Accounting Fallback DNS	Server In Server IP Address(1 Shared S Shared S	Accour Accour	ty) 1 at ASCI	ervers > New 1 • 10.1.100.22 ASCII •					
Downloaded AVP TACACS+ Authentication Accounting Authorization DNS	Confirm S Port Numi Server St Server Ti	Shared Sec ber tatus meout	ret ••••• 49 Enabl	ed 🔽 seconds]	

- 图 15. 添加 TACACS+ 记帐服务器
- **第 3 步:** 点击应用 (Apply)

配置管理用户身份验证的优先级顺序

此步骤说明如何配置管理用户身份验证的优先级顺序。默认控制器配置为*本地和 RADIUS (local and RADIUS)*。使用 TACACS+,身份验证的顺序可以为 TACACS+ 和本地 (TACACS+ and local) 或本地和 TACACS+ (local and TACACS+)。

第 1步: 从 GUI 中,转至**安全 (Security) > 优先级顺序 (Priority Order) > 管理用户 (Management User**)。使用向上和向下箭头按钮,选择"身份验证"(Authentication)并将其排序为 TACACS+ 后跟 LOCAL

CISCO MONITOR WLA	ANS <u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP
Security	Priority Order >	Manageme	nt User			
 AAA Local EAP 	Authentication					
Advanced EAP Priority Order Management User Certificate Access Control Lists Wireless Protection Policies	Not Used RADIUS	> <	Ore	der Used for Auth TACACS+ LOCAL	entication	Up own
Web Auth	If LOCAL is selected a LOCAL only if first price	s second priori ority is unreach	ty then user wi able.	ill be authenticated	against	

图 16. 配置身份验证顺序

第 2 步: 点击应用 (Apply)。

这将完成 TACACS+ 的 WLC 配置。

后续内容

此时,WLC的设备管理所需的所有配置都已完成。您将需要验证配置。

- 第1步: 以属于不同组并访问不同设备的各种用户身份登录到 WLC。
- 第2步: 当登录时,请验证用户是否有权访问适当的选项卡。
- **第3步:** 对于服务中心用户,请导航到不同的选项卡并尝试添加/修改/删除。例如,转至 WLAN 并尝试删除 其中一个 WLAN。由于此用户仅有 MONITOR 访问权限,因此会因以下错误而拒绝操作



图 17. WLC 上授权失败的错误消息

第 4步:从 ISE GUI 中,导航到操作 (Operations) > TACACS 实时日志 (TACACS Livelog)。在此处捕获所 有 TACACS 身份验证和授权请求,并且详细信息按钮将提供有关特定事务通过/失败的原因的详细 信息。

RADIUS Livelog TACACS	Livelog	Reports	Troublesho	ot Adaptive Net	work Control				
G Add or Remove Columns *	🚯 Refred					Refrech	Every 1 minute	• Show Latest 20 records • •	the Last 24 hours *
Logged Time	Status Al •	Details	Username (2)	Type Al *	Authentication Policy	Authorization Policy	ISE Node (7)	Network Device Name	Network Device 3P
2015-11-03 21:29:56.087		.0	inder	Authorization		WrelessLanControllers >> WLC_Security_West	ise-1	DM2_BLDO_VMLC	10.1.100.170
2015-11-03 21:29:56.066		.ò	inter	Authentication	WirelessLanControllers >> Default >> Def		ice-1	DM2_RLDO_WLC	10.1.100.170
2015-11-03 21:29:37.717		ė	lumith	Authorization		WirelessLanControllers >> WLC_Admin_West	ice-1	DM2_BLDO_VWLC	10.1.100.170
2015-11-03 21:29:37.691		.0	bmth	Authentication	WirelessLanControllers >> Default >> Def		08-1	DM2_BLDO_vWLC	10.1.100.170
2015-11-03 21:15:00.308		.0	ytak	Authorization		WrelessLanControllers >> WLC_HelpDeck_West	me-1	DM2_BLDO_WLC	10.1.100.170
2015-11-03 21:15:08:355		à	ptak	Authentication	WirelessanControllers >> Default >> Def		ise-1	DM2_BLDO_VWLC	10.1.100.170

图 18. TACACS 实时日志

第 5步: 对于历史报告,请在 ISE 上转至**工作中心 (Work Centers) > 设备管理 (Device Administration) > 报告 (Reports) > 设备管理 (Device Administration) 以获取身份验证、授权和记帐报告。**