Cisco Unified Wireless Network TACACS+ Configuration

Document ID: 91631

Contents

Introduction **Prerequisites** Requirements Components Used Conventions TACACS+ Implementation in the Controller Authentication Authorization Accounting TACACS+ Configuration in the WLC Add a TACACS+ Authentication Server Add a TACACS+ Authorization Server Add a TACACS+ Accounting Server Configure the Order of Authentication Verify Configuration **Configure Cisco Secure ACS Server** Network Configuration Interface Configuration User/Group Setup Accounting Records in Cisco Secure ACS TACACS+ Configuration in the WCS WCS using Virtual Domains **Configure Cisco Secure ACS to Use WCS** Network Configuration Interface Configuration User/Group Setup Debugs Debugs from WLC for role1=ALL Debugs from WLC for Multiple Roles Debugs from a WLC for Authorization Failure **Related Information** Introduction

This document provides a configuration example of Terminal Access Controller Access Control System Plus (TACACS+) in a Cisco Wireless LAN Controller (WLC) and a Cisco Wireless Control System (WCS) for a Cisco unified wireless network. This document also provides some basic troubleshooting tips.

TACACS+ is a client/server protocol that provides centralized security for users that attempt to gain management access to a router or network access server. TACACS+ provides these AAA services:

- Authentication of users attempting to log in to the network equipment
- Authorization to determine what level of access users should have
- Accounting to keep track of all changes the user makes

Refer to Configuring TACACS+ for more information on AAA services and TACACS+ functionality.

Refer to TACACS+ and RADIUS Comparison for a comparison of TACACS+ and RADIUS.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of how to configure WLCs and lightweight access points (LAPs) for basic operation
- Knowledge of Lightweight Access Point Protocol (LWAPP) and wireless security methods
- Basic knowledge RADIUS and TACACS+
- Basic knowledge of Cisco ACS configuration

Components Used

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

- Cisco Secure ACS for Windows version 4.0
- Cisco Wireless LAN Controller that runs version 4.1.171.0. TACACS+ functionality on WLCs is supported on software version 4.1.171.0 or later.
- Cisco Wireless Control System that runs version 4.1.83.0. TACACS+ functionality on WCS is supported on software version 4.1.83.0 or later.

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, make sure that you understand the potential impact of any command.

Conventions

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

TACACS+ Implementation in the Controller

Authentication

Authentication can be performed using a local database, RADIUS, or TACACS+ server that uses a username and a password. The implementation is not fully modular. Authentication and Authorization services are tied to each other. For example, if authentication is performed using RADIUS/local database, then authorization is not performed with TACACS+. It would use the permissions associated for the user in the local or RADIUS database, such as read–only or read–write, whereas when authentication is performed with TACACS+, authorization is tied to TACACS+.

In cases where multiple databases are configured, a CLI is provided to dictate the sequence in which the backend database should be referred.

Authorization

Authorization is task based rather than an actual per–command based authorization. The tasks are mapped to various tabs that correspond to the seven menu bar items that are currently on the web GUI. These are the menu bar items:

- MONITOR
- WLANS
- CONTROLLER
- WIRELESS
- SECURITY
- MANAGEMENT
- COMMAND

The reason for this mapping is based on the fact that most customers use web interface to configure the controller instead of CLI.

An additional role for lobby admin management (LOBBY) is available for users that need to have lobby admin privileges only.

The task that a user is entitled is configured in the TACACS+ (ACS) server using the custom Attribute–Value (AV) pairs. The user can be authorized for one or multiple tasks. The minimum authorization is MONITOR only and the maximum is ALL (authorized to perform all seven tabs). If a user is not entitled for a particular task, the user is still allowed to access that task in read–only mode. If authentication is enabled and the authentication server becomes unreachable or unable to authorize, the user cannot log in to the controller.

Note: In order for basic management authentication via TACACS+ to succeed, you must configure authentication and authorization servers on the WLC. Accounting configuration is optional.

Accounting

Accounting occurs whenever a particular user–initiated action is performed successfully. The attributes changed are logged in the TACACS+ accounting server along with these:

- The user id of the individual who made the change
- The remote host from where the user is logged in
- The date and time when the command was performed
- Authorization level of the user
- A string that provides information as to what action was performed and the values provided

If the accounting server becomes unreachable, the user can still continue the session.

Note: Accounting records are not generated from WCS in software release 4.1 or ealier.

TACACS+ Configuration in the WLC

WLC Software release 4.1.171.0 and later introduces new CLIs and web GUI changes in order to enable the TACACS+ functionality on the WLC. The CLIs introduced are listed in this section for reference. The corresponding changes for web GUI are added under the Security tab.

This document assumes that the basic configuration of the WLC is already completed.

In order to configure TACACS+ in the WLC controller, you need to complete these steps:

- 1. Add a TACACS+ Authentication Server
- 2. Add a TACACS+ Authorization Server
- 3. Add a TACACS+ Accounting Server
- 4. Configure the Order of Authentication

Add a TACACS+ Authentication Server

Complete these steps in order to add a TACACS+ Authentication Server:

1. Use the GUI, and go to **Security > TACACS+ > Authentication**.

uluulu cisco	MONITOR MLANS	CONTROLLER WIPELESS	SECURITY	M&NAGEMENT	COMMANDS	ΗED	1	age Configuration	i Bing i Logout Befreih
Security	TACACS+ Authen	tication Servers							New
AAA General RADIUS Authentication Accounting TACACS+ Authentication Accounting Authentication Accounting Authentication	Server Index	Server Address	Pert	Admin Sta	lus				

2. Add the IP address of the TACACS+ server and enter the shared secret key. If required, change the default port of TCP/49.

cisco	MONITOR MUANS CONTRO	XLER WIRELESS	SECURITY	MUNAGEMENT	сомилоз	HEID	Sage Configuration (Bing) Logout (Befresh
Security	TACACS+ Authentication	Servers > New					< Back Apply
▼ AAA General	Server Index (Priority)	1 🛩					
KADOJS Authentication Accounting	Server IPAddress	10.3.1.12					
TACACS+ Aythentication	Shared Secret Format	ASCII 👻					
Accounting Authorization	Shared Secret]	
Local Net Users MAC Filtering	Confirm Shared Secret]	
User Login Policies AP Policies	Port Number	49					
+ Local EAP	Server Status	Enabled 💌					
Priority Order Access Control Lists	Retransmit Timoout	2 seconds					

3. Click Apply.

You can accomplish this from CLI using the **config tacacs auth add** *<Server Index> <IP addr> <port> [ascii/hex]* **<secret>** command:

(Cisco Controller) >config tacacs auth add 1 10.1.1.12 49 ascii ciscol23

Add a TACACS+ Authorization Server

Complete these steps in order to add a TACACS+ Authorization Server:

- 1. From the GUI, go to **Security > TACACS+ > Authorization**.
- 2. Add the IP address of the TACACS+ server and enter the shared secret key. If required, change the default port of TCP/49.

uluulu cisco	MONITOR MEANS CONTRO	uler wyeless g	ECURITY MANAGEMENT	COMMANDS	HELP	Sage Configuration Eng Logout Befreid
Security	TACACS+ Authorization S	Servers > New				< Back Apply
* AAA General	Server Index (Priority)	1 -				
RADIUS Authentication	Server IPAddress	10.1.1.12				
Accounting • TACACS+ Authentication	Shared Secret Format	ASCII 💌				
Accounting Authorization	Shared Secret	*****)	
LDAP Local Net Users MAC Filtering	Confirm Shared Secret	*****]	
Disabled Clients User Login Policies AP Policies	Port Number	49				
+ Local EAP	Server Status	Enabled 💌				
Priority Order						
Access Control Lists	Retransmit fimeout	seconds				

3. Click Apply.

You can accomplish this from CLI using the **config tacacs athr add** *<Server Index> <IP addr> <port> [ascii/hex] <secret>* command:

(Cisco Controller) >config tacacs athr add 1 10.1.1.12 49 ascii cisco123

Add a TACACS+ Accounting Server

Complete these steps in order to add a TACACS+ Accounting Server:

- 1. Use the GUI, and go to **Security > TACACS+ > Accounting**.
- 2. Add the IP address of the server and enter the shared secret key. If required, change the default port of TCP/49.

uludu cisco	HONILLON MITWAR	ONTROLLER WIREL	ISS SECURITY	MUNICEMENT	COMMINDS	Reb	Sege Configuration (Eing Logisut Befreih
Security	TACACS+ Accountin	ng Servers > New					< Back Apply
• ALA General • RADOUS	Server Index (Priority)	1 ¥					
Authentication Accounting	Server IPAddress	10.1.1.12					
TACACS+ Authentication	Shared Secret Forma	ASCII 🗸					
Authorization LDAP	Shared Secret						
Local Net Users MAC Filtering Disabled Clearts	Confirm Shared Secret	****					
User Login Policies AP Policies	Port Number	49					
+ Local EAP	Server Status	Enabled 💌					
Priority Order Access Control Lists	Retransmit Timeout	E seconds					

3. Click Apply.

You can accomplish this from CLI using the **config tacacs acct add** *<Server Index> <IP addr> <port> [ascii/hex]* **<secret>** command:

Configure the Order of Authentication

This step explains how to configure the AAA order of authentication when there are multiple databases configured. The order of authentication can be **local and RADIUS**, or **local and TACACS**. The default controller configuration for order of authentication is *local and RADIUS*.

Complete these steps in order to configure the order of authentication:

- 1. From the GUI, go to Security > Priority Order > Management User.
- 2. Select the Authentication Priority.

In this example, TACACS+ has been selected.

3. Click **Apply** in order for the selection to take place.



You can accomplish this from CLI using the **config aaa auth mgmt** *<server1> <server2>* command:

(Cisco Controller) >config aaa auth mgmt tacacs local

Verify Configuration

This section describes the commands used to verify TACACS+ configuration on the WLC. These are some useful **show** commands that help to determine if the configuration is correct:

• show aaa auth Provides information on the order of the authentication.

(Cisco Controller) >show aaa auth Management authentication server order: 1.....local 2..... Tacacs • show tacacs summary Displays a summary of TACACS+ services and statistics. (Cisco Controller) >show tacacs summary Authentication Servers Idx Server Address Port State Tout ----- -----___ 49 Enabled 1 10.1.1.12 2 Authorization Servers Idx Server Address Port State Tout

	1	10.1.1.12	49	Enabled	2
	Acco	unting Servers			
	Idx	Server Address	Port	State	Tout
	1	10.1.1.12	49	Enabled	2
• show ta	acacs	auth stats Displays T.	ACACS+	authenticati	on server statistics.

(Cisco Controller) >show tacacs auth statistics Authentication Servers: Server Index..... 1 Server Address..... 10.1.1.12 Msg Round Trip Time..... 0 (1/100 second) First Requests..... 7 Retry Requests..... 3 Accept Responses..... 3 Reject Responses..... 0 Error Responses..... 0 Restart Responses..... 0 Follow Responses..... 0 GetData Responses..... 0 Encrypt no secret Responses..... 0 Challenge Responses..... 0 Malformed Msgs..... 0 Bad Authenticator Msgs..... 0 Timeout Requests..... 12 Unknowntype Msgs..... 0 Other Drops..... 0

• show tacacs athr stats Displays TACACS+ authorization server statistics.

(Cisco Controller) >**show tacacs athr statistics** Authorization Servers:

Server Index	1
Server Address	10.1.1.12
Msg Round Trip Time	0 (1/100 second)
First Requests	3
Retry Requests	3
Received Responses	3
Authorization Success	3
Authorization Failure	0
Challenge Responses	0
Malformed Msgs	0
Bad Athrenticator Msgs	0
Timeout Requests	0
Unknowntype Msgs	0
Other Drops	0

• show tacacs acct stats Displays TACACS+ accounting server statistics.

(Cisco Controller) >**show tacacs acct statistics** Accounting Servers:

Server Index	1
Server Address	10.1.1.12
Msg Round Trip Time	0 (1/100 second)
First Requests	133
Retry Requests	0
Accounting Response	0
Accounting Request Success	0
Accounting Request Failure	0
Malformed Msgs	0
Bad Authenticator Msgs	0

Timeout Requests	399
Unknowntype Msgs	0
Other Drops	0

Configure Cisco Secure ACS Server

This section provides the steps involved in the TACACS+ ACS Server to create services and custom attributes, and assign the roles to the users or groups.

The creation of users and group is not explained in this section. It is assumed that the users and groups are created as needed. Refer to User Guide for Cisco Secure ACS for Windows Server 4.0 for information on how to create users and user groups.

Network Configuration

Complete this step:

Add the Controller management IP address as AAA client with Authentication mechanism as TACACS+ (Cisco IOS).



Interface Configuration

Complete these steps:

- 1. In the Interface Configuration menu, select the TACACS+ (Cisco IOS) link.
- 2. Enable the **New Services**.
- 3. Check both the User and Group check boxes.
- 4. Enter **ciscowlc** for Service and **common** for Protocol.
- 5. Enable the Advanced TACACS+ Features.

dress 🙋 http://127.0.0.1:1767/					💌 🔁 Go	Links
CISCO SYSTEMS Interfa	ace Conf	iguration				[
adili ilinaadili ilina -		TACACS+ S	ervices		?	-
User User User	Group					
Group	V	PPP IP				
🔮 Setup		PPP IPX				
Shared Profile Components		PPP Multilink				
Network		PPP Apple Talk				
nfiguration		PPP VPDN				
em iguration		PPP LCP				
		ARAP				
figuration	V	Shell (exec)				
ation		PIX Shell (pixshell)				
User		SLIP				
New S	ervices					
e tion		Service	F	Protocol		
Access	V	ciscowlc	[common		
			[
and			ſ			
ation						
		Advanced Configu	ration Opt	ions	?	
🔽 Ad	vanced TAC	ACS+ Features				
🗖 Dis	play a Time	of-Day access grid for	every TAC	ACS+ service when	e you can	-
		Submit	Cancel			

6. Click **Submit** in order to apply the changes.

User/Group Setup

Complete these steps:

- 1. Select a previously created User/Group.
- 2. Go to **TACACS+ Settings**.
- 3. Check the check box that corresponds to the *ciscowlc* service that was created in the Interface Configuration section.
- 4. Check the **Custom attributes** check box.

Cisco Systems	Group Setup
.allbs	Jump To Access Restrictions
User Satur	Shell Command Authorization Set
EA Group	@ None
Setup	Assign a Shell Command Authorization Set for any network device
Shared Profile Components	C Per Group Command Authorization
Network Configuration	Unmatched Cisco IOS commands
Wind Sustem	C Permit
Configuration	@ Deny
Configuration	Command:
Administration	
HA External User	Arguments:
90 Databases	
voices Validation	2
Network Access Profiles	Unlisted arguments
Reports and	C Permit
Activity	C Deny
Documentation	
	Custom attributes
	role1=ALL
	v 1
	_
	Wireless-WCS HTTP
	Custom attributes
	<u></u>
	2
	IETF RADIUS Attributes
	C [006] Service-Type
	Caliback NAS Drownt V
	adding adding the start adding

 In the text box below Custom attributes, enter this text if the user created needs access only to WLAN, SECURITY and CONTROLLER: role1=WLAN role2=SECURITY role3=CONTROLLER.

If the user needs access only to the SECURITY tab, enter this text: role1=SECURITY.

The role corresponds to the seven menu bar items in the controller web GUI. The menu bar items are MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT and COMMAND.

6. Enter the role that a user needs for role1, role2 and so on. If a user needs all the roles, then the keyword **ALL** should be used. For the lobby admin role, the keyword **LOBBY** should be used.

Accounting Records in Cisco Secure ACS

TACACS+ accounting records from the WLC are available in Cisco Secure ACS in the TACACS+ Administration of Reports and Activity:

Decelecter ACS - N	kroudt Internet Explorer										_1#1X
File Edit View Fare	orites Tools map										
4-54 + 17 - Q	3 3 Bierth Brunten Griede 3	0.0									
Address (a) http://127.6	.h.1:+087/									-	2 60 Links *
Google C+	💌 Ga - 📂 🙇 - 🤷 Backmarks -	🖗 I bloded 🛛 🚏 Oeck = 🔥 Auto	an = "color: 🕒 sector 🦉 👘								- Settings=
Care System	Reports and Activity										×
A A.	- opene and roomly										
	Select	Select									
1 Info		Tececs+ Administration a	ective.csv 🖸 Befrash 🕞 Que	micad							
and Dress	Reports	Regular Expression	Start Date	6 Time	End Date & Time	_	Pows per	Page			
PO 1414		L	[mm/dd/)00	y minimum as	[mm/dd/yyyy, Mr.mm.)	15	50	-			
6 Company	E TACACE+ Accounting	Apply Filter Clear F	üter .								
The Brings	C TACACE+ Administration	Filtering is not applied.									
Configration	Photo accounting	Date 🕈 Time Use	r-Name Group-Name		cmd	prix-b	d service	NAS-Portname	tash. Id	NAS-IP-Addre	ss reason
Configuration	Passed Authentications	02/22/2007 36:26:52 140	Tacacs Group for WLC	wian enable 1		249	shell		224	10.10.80.3	
and the state	B Lated Attempts	02/22/2007 16:26:52 tac	Tacacs Group for WLC	wian idap delete 3	position 2	249	shell		223	10.10.00.3	
Configeration	Logged-in Users	02/22/2007 16:26:52 tac	Tacacs Group for WLC	wian Idap delete 1	position 1	249	shell		222	10.10.80.3	
A DECEMBER OF STREET	Desibled accounts	02/22/2007 16:26:52 tac	Tacacs Group for WLC	wian Idap delete 1	position 0	249	shell		221	10.10.80.3	
Tested	ET ACS Beckup and Restore	92/22/2007 36 26 52 54	Tacacs Group for WLC	wan timeout 1.0		249	shell	a	220	10.10.80.3	
Briternal Uper	PD Induktory Institution	02/22/2007 16:26:52 140	Tacacs Group for WLC	wian mac-filtering	disable 1	249	shell		279	10.10.80.3	
T 2 I I R R R R	No	02/22/2007 36:26:52 tac	Tacace Group for WLC	wan security is M	one for wan-id 1	549	1740		331	10.10.80.3	
Tableton Tableton	He Administration, Audit	02/22/2007 16:26:52 140	Tacace Group for WLC	wan security with	(WPA/RIN) disable 1	249	phen.		217 - I	10.10.80.9	
Concentration of the local division of	User Rassword Changes	02/22/2007 15:26:52 fac	Tacacs Group for WLC	wian assroverride	disable 1	249	shell		216	10.10.00.3	
C Puller	ACS Service Monitoring	02/22/2007 16 26 52 Vac	Tacacs Group for WLC	wan gos 1 platinu	~	249	shell		235	10.10.80.9	
C. Busetrast		02/22/2007 16:26:52 140	Tacacs proup for WUC	wian radio 1 at	10000	549	sries		224	10.10.80.3	
- Artives		02/22/2007 36:26:52 540	Tacads luroup for WLC	wan drop_server	10.0.0.0 required	249	and a		938	10.10.00.3	
B Selar		02/22/2007 16:26:52 146	Tacact uroup for WUC	wan proadcast-st	tio enable 1	249	proper la		311	10.10.00.3	
	P Ball to Web	an and many interesting the	Tacact group for well	wan exclusioner	1.0	2.40	about the		110	10.10.00.0	
		22/22/20/7 16:20:52 140	Tacace Group for Web	wan exclusioner	1.02404		shell		100	10.10.80.7	
		00/00/00/114/06/00 har	Tacace Group for WLC	wise interface 1.1	00	240	'shell		104	10.10.00.0	
		02/22/2007 16 26 52 fac	Tacaca Group for WLC	wian disable 1		249	shall		207	10.10.00.2	
€) 100-eel 110-as 5	Condense Alton	Otto heread	elluded 🗍 🏟 Mudee by Ph.	ave Countrie	ta levetue	Mercuid	1 meret	Windowski (1974) Inco - Marcard	the Kat	vi de animi

TACACS+ Configuration in the WCS

Complete these steps:

- 1. From the GUI, log in to the WCS with the root account.
- 2. Add the TACACS+ server. Go to Administration > AAA > TACACS+ > Add TACACS+ Server.

ababa	Wireless Control System	Username: root Logout Refresh P	vint View 🖄
cisco	Bonitor = Beports = Certifiqure = Location = Administration = Belg =		
AAA	TACACS+	Select a command	- 60
Change Password	No TACACS+ Servers found in the system		
AAA Node			
Users			
Groups			
Active Sessions			
TACACS+			
RADIUS			

3. Add the TACACS+ server details, such as IP address, port number (49 is default), and shared secret key.

alada	Wireless Control S	ystem				Username: root	Logout	Refresh	Print View
cisco	Monitor - Reports - Co	nfigure = Location = A	dministration •	Belp •					
	TACACS+								
	Server Address	10.1.1.12							
AAA Node	Port	49							
	Shared Secret Format	ASCII 🛩							
Users	Shared Secret								
	Confirm Shared Secret	•••••							
	Retransmit Timeout	5 seconds							
TACACS+	Retries	1							
	Authentication Type	PAP 👻							
RADIUS	Submit Cancel								

4. Enable TACACS+ authentication for administration in the WCS. Go to Administration > AAA > AAA Mode > Select TACACS+.

ababa	Wireless Control System
cisco	Bonitor + Beports + Configure + Location + Administration + Bello +
AAA	AAA Mode Settings
Change Password	AAA Mode O Local O RADIUS @TACACS+
AAA Node	Palback on Local 🕑
Users	00
Groeps	Distant since bugier user is going to be an exprised autoencounted locally interpretive of the Aut Mode Settiongs.
Active Sessions	
TACACS+	
RADIUS	

WCS using Virtual Domains

Virtual Domain is a new feature introduced with WCS version 5.1. A WCS virtual domain consists of a set of devices and maps and restricts a user's view to information relevant to these devices and maps. Through a virtual domain, an administrator can ensure that users can only view the devices and maps for which they are responsible. In addition, because of the virtual domain's filters, users can configure, view alarms, and generate reports for only their assigned part of the network. The administrator specifies a set of allowed virtual domains for each user. Only one of these can be active for that user at login. The user can change the current virtual domain by selecting a different allowed virtual domain from the Virtual Domain drop–down menu at the top of the screen. All reports, alarms, and other functionality are now filtered by that virtual domain.

If there is only one virtual domain defined (root) in the system and the user does not have any virtual domains in the custom attributes fields in the TACACS+/RADIUS server, the user is assigned the root virtual domain by default.

If there is more than one virtual domain, and the user does not have any specified attributes, then the user is blocked from logging in. In order to allow the user to log in, the Virtual Domain custom attributes must be exported to the Radius/TACACS+ server.

The Virtual Domain Custom Attributes window allows you to indicate the appropriate protocol–specific data for each virtual domain. The Export button on the Virtual Domain Hierarchy sidebar pre–formats the virtual domain's RADIUS and TACACS+ attributes. You can copy and paste these attributes into the ACS server. This allows you to copy only the applicable virtual domains to the ACS server screen and ensures that the users only have access to these virtual domains.

In order to apply the pre–formatted RADIUS and TACACS+ attributes to the ACS server, complete the steps explained in the Virtual Domain RADIUS and TACACS+ Attributes section.

Configure Cisco Secure ACS to Use WCS

The section provides the steps involved in the TACACS+ ACS Server to create services and custom attributes, and assign the roles to the users or groups.

The creation of users and group is not explained in this section. It is assumed that the users and groups are created as needed.

Network Configuration

Complete this step:

Add the WCS IP address as AAA client with Authentication mechanism as TACACS+ (Cisco IOS).

CISCO SYSTEMS	Network Configuration
millitumilitum	Edit
User Setup	
Group Setup	AAA Client Setup For
Shared Profile Components	WCS
Network Configuration	192.168.60.5
System Configuration	AAA Client IP Address
Configuration	Key cisco
Administration Control	Authenticate Using TACACS+ (Cisco IOS)
External User Databases	Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
Posture Validation	Log Update/Watchdog Packets from this AAA Client
Network Access Profiles	Log RADIUS Tunneling Packets from this AAA Client
Reports and Activity	Replace RADIUS Port info with Username from this AAA Client
Online Documentation	Submit = Apply Delete Delete + Apply Cancel
	Pack to Help

Interface Configuration

Complete these steps:

- 1. In the Interface Configuration menu, select the TACACS+ (Cisco IOS) link.
- 2. Enable the **New Services**.
- 3. Check both the **User** and **Group** check boxes.
- 4. Enter **Wireless–WCS** for Service and **HTTP** for Protocol.

Note: HTTP must be in CAPS.

5. Enable the Advanced TACACS+ Features.

CISCO SYSTEMS	Inte	rface	Configuration	
		•	PPP IP	
User			PPP IPX	
Lig Setup			PPP Multilink	
Group Setup			PPP Apple Talk	
685. Shared Profile			PPP VPDN	
ීහි Components			PPP LCP	
Network Configuration			ARAP	
Sustem		✓	Shell (exec)	
₹ ³ Configuration			PIX Shell (pixshell)	
Interface Configuration			SLIP	
Administration	New	Servia	ces	
- L External liser			Service	Protocol
JO Databases		\checkmark	ciscowlc	common
Posture Validation		◄	Wireless-WCS	НТТР
Network Access Profiles				
C L Reports and				
Activity		A	dvanced Configurati	on Options 🛛 🤶
Online Documentation	Advanced TACACS+ Features			

6. Click **Submit** in order to apply the changes.

User/Group Setup

Complete these steps:

1. In the WCS GUI, navigate to Administration > AAA > Groups to select any of the pre–configured user groups, such as SuperUsers in the WCS.

alada	Wireless Control System			Uservarie: root Legout Refresh Prot Vare
CISCO	Bontor + Beports + Configure + Location + Administration + Help +			
AAA	All Groups			
Change Password	Group Name	Nembers	Audit Trad	Expert
Local Password Policy	Admin		20	Task List
AAA Node	Conflationecers	-	20	Tauk List
Users	Southern Manifaction		2	Task sist
Groups	Long, Assistant		20	Task List
Active Sessions	Lobbs Ambassador	hibha	20	Tank List
	Manifest Life		2	Task List
TALACEP	North Bound API	-	20	Task List
RADOUS	SuperStatus		28 C	Task List
	test	5365	2	Task List
	Uver.Defined.1		20 C	Tank Lint
	User.Defined.2		20 C	Task List
	User.Defined.3		2	Task List
	User Defined 4		20	Tank List

2. Select the Task List for the pre-configured user groups and copy paste to the ACS.

ababa	Wireless Control System	Username: root Logout	Refresh	Print View			
CISCO	Santar + Separta + Carligare + Lacator + Administrator + Belg +						
AAA	Export Task List						
Change Password	Please cut and paste the appropriate protocol data below into the outcom/vendor-specific attribute field in your AAA server.						
Local Password Policy	TACACS+ Custom Attributes RADIUS Custom Attributes						
AAA Node	vold-shart varies with involution varies with involution varies with involutions varies with involutions with involutions varies with involutions with involutions varies with involutions varies with involutions varies with involutions varies						
Groups	hask bellADD(1)5 Servers hask-fulgping Aust-S-Linkingung Aust-S-Linkingung Aust-S-Linkingung Aust-S-Linkingung						
Active Sessions	Tassid=StateStateStateStateStateStateStateStat						
TACACS+	haish-Daguarte Information Wirelesse wCS task-D-Daguarte Information Raislatives Alexa of Santha Wirelesse wCS task-D-Daguarte Information Raislatives Alexa of Santha						
RADIUS	Testill avies Autor and Execting Workson WCS stall aview Autor and Execting Workson WCS stall aview Autor and Execting Workson WCS stall aview Autor and Execting Workson WCS stall aview Autor and Execting Workson WCS stall aview Autor and Execting Workson WCS stall aview Autor and Execting Workson WCS stall aview Autor and Execting Workson WCS stall aview Autor and Execting Workson WCS stall aview Autor and Execting Workson WCS stall aview Autor and Execting Workson WCS stall aview Autor and Execting Workson WCS stall aview Autor and Execting Workson WCS stall aview Autor and Execting Workson WCS stall aview Autor and Execting Workson WCS stall aview						

- 3. Select a previously created User/Group and go to TACACS+ Settings.
- 4. In ACS GUI, select the check box that corresponds to Wireless-WCS service that was created earlier.
- 5. In ACS GUI, check the **Custom attributes** box.
- 6. In the text box below Custom attributes, enter this role and task information copied from the WCS. For example, enter the list of tasks permitted by the SuperUsers.

CISCO SYSTEMS	Group Setup
	Jump To TACACS+
User Setup	L Custom attributes
Group Setup	
Components	
System Configuration	Wireless-WCS HTTP Custom attributes
Configuration	roleO=SuperUsers
Administration Control	task2=TACACS+ Servers task3=RADIUS Servers
Databases	
Validation	
Profiles	Cisco IOS/PIX 6.x RADIUS Attributes
Reports and Activity Online Documentation	[009\001] cisco-av-pair

7. Then, log in to the WCS with the newly created username/password in the ACS.

Debugs

Debugs from WLC for role1=ALL

```
(Cisco Controller) >debug aaa tacacs enable
(Cisco Controller) >Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=2 session_id=5eaa857e
length=16 encrypted=0
Wed Feb 28 17:36:37 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:36:37 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:36:37 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=4 session_id=5eaa857e
length=6 encrypted=0
Wed Feb 28 17:36:37 2007: tplus_make_author_request() from tplus_authen_passed returns rc=
Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: author response body: status=1 arg_cnt=1 msg_len=0 data_len=0
```

Wed Feb 28 17:36:37 2007: arg[0] = [9][role1=ALL]
Wed Feb 28 17:36:37 2007: User has the following mgmtRole fffffff8

Debugs from WLC for Multiple Roles

```
(Cisco Controller) >debug aaa tacacs enable
Wed Feb 28 17:59:33 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=2
session_id=b561ad88 length=16 encrypted=0
Wed Feb 28 17:59:34 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:59:34 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:59:34 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=4 session_id=b561ad88
length=6 encrypted=0
Wed Feb 28 17:59:34 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:59:34 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: author response body: status=1 arg_cnt=4 msg_len=0 data_len=0
Wed Feb 28 17:59:34 2007: arg[0] = [11][role1=WLAN]
Wed Feb 28 17:59:34 2007: arg[1] = [16][role2=CONTROLLER]
Wed Feb 28 17:59:34 2007: arg[2] = [14][role3=SECURITY]
Wed Feb 28 17:59:34 2007: arg[3] = [14][role4=COMMANDS]
Wed Feb 28 17:59:34 2007: User has the following mgmtRole 150
```

Debugs from a WLC for Authorization Failure

(Cisco Controller) >debug aaa tacacs enable

```
Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=2 session_id=89c553a1
length=16 encrypted=0
Wed Feb 28 17:53:04 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:53:04 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:53:04 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=4 session_id=89c553a1
length=6 encrypted=0
Wed Feb 28 17:53:04 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: author response body: status=16 arg_cnt=0 msg_len=0 data_len=0
Wed Feb 28 17:53:04 2007: Tplus authorization for tac failed status=16
```

Related Information

- Cisco Wireless LAN Controller (WLC) and Cisco ACS 5.x (TACACS+) Configuration Example for Web Authentication
- Configuring TACACS+
- How to Configure TACACS Authentication and Authorization for Admin and non-Admin users in ACS 5.1
- TACACS+ and RADIUS Comparison
- Technical Support & Documentation Cisco Systems

Contacts & Feedback | Help | Site Map

^{© 2014 – 2015} Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.