Configure a WLC and an ACS to Authenticate Management Users

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Background Information
<u>Configure</u>
Network Diagram
Configurations
WLC Configuration
Configure the WLC to Accept Management through the Cisco Secure ACS Server
Cisco Secure ACS Configuration
Add the WLC as an AAA Client to the RADIUS Server
Configure Users and Their Appropriate RADIUS IETF Attributes
Configure a User with Read-Write Access
Configure a User with Read-Only Access
Manage the WLC Locally as well as Through the RADIUS Server
<u>Verify</u>
Troubleshoot
Related Information

Introduction

This document describes how to configure a WLC and a Cisco Secure ACS so that the AAA server can authenticate management users on the controller.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to configure basic parameters on WLCs
- Knowledge of how to configure a RADIUS server like the Cisco Secure ACS

Components Used

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

- Cisco 4400 Wireless LAN Controller that runs version 7.0.216.0
- A Cisco Secure ACS that runs software version 4.1 and is used as a RADIUS server in this configuration.

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.

Conventions

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

Background Information

This document explains how to configure a Wireless LAN Controller (WLC) and an Access Control Server (Cisco Secure ACS) so that the Authentication, Authorization, and Accounting (AAA) server can authenticate management users on the controller. The document also explains how different management users can receive different privileges with Vendor-specific Attributes (VSAs) returned from the Cisco Secure ACS RADIUS server.

Configure

In this section, you are presented with the information on how to configure the WLC and the ACS for the purpose described in this document.

Network Diagram

This document uses this network setup:



Network Diagram

This configuration example uses these parameters:

- IP address of the Cisco Secure ACS —172.16.1.1/255.255.0.0
- Management interface IP address of the controller—172.16.1.30/255.255.0.0
- Shared secret key that is used on the access point (AP) and the RADIUS server—asdf1234
- These are the credentials of the two users that this example configures on the ACS:
 - 1. Username acsreadwrite

Password - acsreadwrite

2. Username - acsreadonly

Password - acsreadonly

You need to configure the WLC and Cisco Secure Cisco Secure ACS in order to:

• Any user who logs into the WLC with the username and password asacsreadwrite is given full

administrative access to the WLC.

• Any user who logs into the WLC with the username and password as acsreadonly is given read-only access to the WLC.

Configurations

This document uses these configurations:

- <u>WLC Configuration</u>
- <u>Cisco Secure ACS Configuration</u>

WLC Configuration

Configure the WLC to Accept Management through the Cisco Secure ACS Server

Complete these steps in order to configure the WLC so that it communicates with the RADIUS server:

 From the WLC GUI, click Security. From the menu on the left, click RADIUS > Authentication. The RADIUS Authentication serverspage appears. To add a new RADIUS Server, click New. In the RADIUS Authentication Servers > New page, enter the parameters specific to the RADIUS server. Here is an example.

cisco	NONETOR WLANS	gowneouse	wiseress	SECORDY	менноемент	COMMANDS	неце	FESORACE
Security	RADIUS Authentis	ation Server	s>New	· · ·				
 AAA FACOUS Authoritocation Accounting Fallback TacLACS+ EDAP Lace Met Users FAC Prinning Disabled Clients Harr Login Policies AF Policies 	Server Index Orient Server IP Address Shared Secret Formu Shared Secret Confirm Shared Sec Kty Wrss Port Namber Server Status	n) e na I	1 0 172:15.1.1 ASCT 0 received (Descipted f 1812 Tradied 10	tr FIPS outpr	ners and requires	a keey wrap, came	slast kåt	ituti nerver)

2. Check the **Management** radio button in order to allow the RADIUS Server to authenticate users who log in to the the WLC.



Note: Ensure that the shared secret configured on this page matches with the shared secret configured on the RADIUS server. Only then can the WLC communicate with the RADIUS server.

3. Verify whether the WLC is configured to be managed by Cisco Secure ACS. In order to do this, click **Security** from the WLC GUI. The resultant GUI window appears similar to this example.

cisco	MONITOR MUNIC	CONTROLLER	wjei.ess	SECURITY	MEMAGEMENT	COMMANDS	нецё	EROMO
Security	RADIUS Authentil	cation Server	8					
* AAA General	Call Station ID Type	A IP Address	¥					

You can see that the Management check box is enabled for RADIUS server 172.16.1.1. This illustrates that ACS is allowed to authenticate the management users on the WLC.

Cisco Secure ACS Configuration

Complete the steps in these sections in order to configure the ACS:

- 1. Add the WLC as an AAA Client to the RADIUS Server
- 2. Configure Users and Their Appropriate RADIUS IETF Attributes
- 3. Configure a User with Read-Write Access
- 4. Configure a User with Read-Only Access

Add the WLC as an AAA Client to the RADIUS Server

Complete these steps in order to add the WLC as an AAA client in the Cisco Secure ACS:

- 1. From the ACS GUI, click **Network Configuration**.
- 2. Under AAA Clients, click Add Entry.
- 3. In the Add AAA Client window, enter the WLC host name, the IP address of the WLC, and a shared secret key.

In this example, these are the settings:

- AAA Client Hostname is WLC-4400.
- 172.16.1.30/16 is the AAA Client IP Address, which, in this case is the WLC.
- The shared secret key is asdf1234.

Cinco Storens	Network Configuration
and the second	Add AAA Client
E Setus	AAA Client Hostname WLC- 4400
Barol Frofile	AAA Client IP Address
Configuration	shared Secret asdf1234
Configuration	RADIUS Key Wrap Key Encryption Key
Control	Key Input Format C ADCII @ Hesadecimal
Conferences	Authenticate Using RADIUS (Cisco Alrespace)
Portes	Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
C separate	C Log Update/Watchdog Packets from this AAA Client
E Boarrentation	Log RACOUS Turneling Packets from this AAA Client
	Replace RADIUS Port info with Osemana from this AAA Client
	Match Framed-DP-Address with user IP address for accounting packets from this AAA Client
	Submit Submit + Apply Cancel

Add AAA Client Window

This shared secret key must be the same as the shared secret key that you configure on the WLC.

- 4. From the Authenticate Using drop-down menu, choose RADIUS (Cisco Airespace).
- 5. Click **Submit + Restart** in order to save the configuration.

Configure Users and Their Appropriate RADIUS IETF Attributes

In order to authenticate a user via a RADIUS server, for controller log in and management, you must add the user to the RADIUS database with the IETF RADIUS attributeService-Typeset to the appropriate value based on the user privileges.

- In order to set read-write privileges for the user, set the Service-Type Attribute to Administrative.
- In order to set read-only privileges for the user, set theService-TypeAttribute to NAS-Prompt.

Configure a User with Read-Write Access

The first example shows the configuration of a user with full access to the WLC. When this user tries to log in to the controller, the RADIUS server authenticates and provides this user with full administrative access.

In this example, the username and password is **acsreadwrite**.

Complete these steps on the Cisco Secure ACS.

- 1. From the ACS GUI, click User Setup.
- 2. Type the username to be added to the ACS as this example window shows.

Cisco Systems	User Setup	
مظالتمطالتم	Select	
User Setup	· · · · · ·	
Graup Setap		User: acsreadwrite
Bhared Profile Components		Find Add/Edit
Network Configuration		List users beginning with letter/number:
Configuration		ABCREEGNIJELN NOF9BBISVNXYX 0123456789
Configuration		List all ricers
Administration Centrol		List di Osols
Databases		Remove Dynamic Users
Pesture Validation		
Network Access Profiles		Y Eack to Help
Reports and Activity		
Documentation		

User Setup Window

- 3. Click Add/Edit in order to go to the User Edit page.
- 4. In the User Edit page, provide the Real Name, Description and Password details of this user.
- 5. Scroll down to the IETF RADIUS Attributes setting and check Service-Type Attribute.
- 6. Since, in this example, user acsreadwrite needs to be given full access, choose **Administrative** for the Service-Type pull-down menu and click **Submit**.

This ensures that this particular user has read-write access to the WLC.



ETF RADIUS Attributes Settings

Sometimes, this Service-Type attribute is not visible under the user settings. In such cases, complete these steps in order to make it visible.

1. From the ACS GUI, navigate to **Interface Configuration > RADIUS (IETF)** in order to enable IETF attributes in the User Configuration window.

This takes you to the RADIUS (IETF) Settings page.

2. From the RADIUS (IETF) Settings page, you can enable the IETF attribute that needs to be visible under user or group settings. For this configuration, check **Service-Type** for the User column and click **Submit**. This window shows an example.



Interface Configuration

RADIUS (IETF)

User Setup		RADIUS (IETF)
Grosp Getup		
the ISharedirefie	User	Group
TSF Components	R	F [006] Service-Type
Configuration	Ē.	₽ [007] Framed-Protocol
The Supton		₽ [009] Framed-IP-Netmask
Configuration		₽ [010] Framed-Routing
Canfiguration		🖻 [011] Filter-Id
Acministration		€ [012] Framed-MTU
See Control		₱ [013] Framed-Compression
Del Databases		₽ [014] LogIn-IP-Host
Inner Posture		F [015] Login-Service
I di datest	<u> </u>	₽ [016] LogIn-TCP-Port
Profiles		F [018] Reply-Message
Co. Reports and		₽ [020] Callback-Id
- Castrony		[022] Framed-Route [022] []
E Courrentation		[023] Framed-IPX-Network
	1	₩ [024] State
		₽ [025] Class
		[027] Session-Timeout [027] Session-Timeout S
		₽ [028] Idle-Timeout

RADIUS (IETF) Settings Page



Note: This example specifies authentication on a per-user basis. You can also perform authentication based on the group to which a particular user belongs. In such cases, enable the Group check box so that this attribute is visible under Group settings. Also, if the authentication is on a group basis, you need to assign users to a particular group and configure the group setting IETF attributes to provide access privileges to users of that group. Refer to Group Management for detailed information on how to configure and manage groups.

Configure a User with Read-Only Access

This example shows the configuration of a user with read-only access to the WLC. When this user tries to logi n to the controller, the RADIUS server authenticates and provides this user with read-only access.

In this example, the username and password is acsreadonly.

Complete these steps on the Cisco Secure ACS:

- 1. From the ACS GUI, click User Setup.
- 2. Type the username you want to add to the ACS and click **Add/Edit** in order to go to the User Edit page.

Cisco Systems	User Setup	
	Select	
User Betup		
Group Setup		User: acsreadonly
Shared Profile Components		Find Add/Edit
Network Configuration Suptem Configuration Configuration Wherface Configuration Control Control		List users beginning with letter/number: ABCDEFGEIZEEB NOPORSTUYEX DI23456769 List all users Remove Dynamic Users
Reports and Activity		2 Back to Help

Add a Username

3. Provide the **Real Name**, **Description** and **Password** of this user. This window shows an example.

Cisco Systems	User Setup
	Edit
Setup	User: acsreadonly (New User)
Ga Shared Profile	Account Disabled
Network Configuration	Supplementary User Info
System Configuration	Real Name acsreadonly
Configuration	Description User with Read only
Administration Centrol	
Datatuses	User Setup
Pecture Velidation	Password Authentication: ACS Internal Database
Reportsand	Separate field is not checked.)
Dalia# Documentation	Confirm Password
	Separate (CHAP/MS-CHAP/ARAP)
	Password
	Confirm Password
	When a token server is used for authentication, supplying a Submit Cancel

Provide the Real Name, Description and Password of the Added User

- 4. Scroll down to the IETF RADIUS Attributes setting and check Service-Type Attribute.
- 5. Since, in this example, user acsreadonly needs to have read-only access, choose **NAS Prompt** from the Service-Type pull-down menu and click **Submit**.

This ensures that this particular user has read-only access to the WLC.

Account Disable User Strop Strop Composents Strong <	?
Never Startel Profile Startel Profile Startel Profile Startel Profile Startel Profile Date exceeds: Sep • 22 2011 Failed attempts exceed: Setting Interface Setting Seting Setting Setting Setting	
Stares Bridge Shares Bridge Composents Stares Bridge Composents Sep • 22 2011 Failed attempts exceed: S Failed attempts since last successful login: 0 Failed attempts since last successful login: 0 Reset current failed attempts count on submit	1
Starell Profile Bet vork Configuration Sep • 22 2011 Paled attempts exceed: Sep • 22 2011 Paled attempts exceed: S Faled attempts since last successful login: 0 Paled attempts count on submit	11
Network Configuration Sep Sep Sep Paled attempts exceed: S Faled attempts since last successful login: 0 Reset current failed attempts count on submit External User Failed attempts attempts count on submit External User Failed attempts Attributes	
Carrigeration System Configuration Interface Configuration	
System 5 Failed attempts since last successful login: 0 Configuration Administration Convirol External User Pailod Validation Interface	
Failed attempts since last successful login: 0 Failed attempts count on submit Reset current failed attempts count on submit Esternal User Pesture Validation IETE RADIUS Attributes	
Administration Control Detabases Police Validation	
Pesture Validation IETE RADIUS Attributes	
Pesture Validation IETF RADIUS Attributes	
IETF RADIUS Attributes	
Pierties	
Authenticate only	1
Authenticate only	
Documentation Participation	
Caliback NAS Prompt	
Administrative Caliback Administrative	
Callback login	
T Bads to Help Framed	

Check Service-Type Attribute

Manage the WLC Locally as well as Through the RADIUS Server

You can also configure the management users locally on the WLC. This can be done from the controller GUI, under **Management > Local Management Users**.

uluilu cisco	MONITOR MLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Management Summary > SNMP HTTP-HTTPS Telnet-SSH Serial Port Local Management Users User Sessions	Local Managemer User Name Password Confirm Password User Access Mode	nt Users > Nev User1 ••••• Read Read Lobby	V Dnly Vite Admin		

Configure the Management Users Locally on the WLC

Assume that the WLC is configured with management users both locally as well as in the RADIUS server with the **Management** check box enabled. In such a scenario, by default, when a user tries to log in to the WLC, the WLC behaves in this manner:

- 1. The WLC first looks at the local management users defined to validate the user. If the user exists in its local list, then it allows authentication for this user. If this user does not appear locally, then it looks to the RADIUS server.
- 2. If the same user exists both locally, as well as in the RADIUS server, but with different access privileges, then the WLC authenticates the user with the privileges specified locally. In other words, local configuration on the WLC always takes precedence when compared to the RADIUS server.

The order of authentication for management users can be changed on the WLC. In order to do this, from the **Security** page on the WLC, click **Priority Order > Management User**. From this page you can specify the order of authentication. Here is an example.

cisco		CONTROLLER	WIRELESS	SECURITY	MEMORHENT	COMMANDS	HELP
Security	Priority Order > M	lanagement U	ser				
AAA General # RADOUS Authentication Accounting Fallback TACACS+ LOAP Local Net Users	Authentication Not Used TACACS+	2	Order U	ed for Authe	ntication Dow	n	
Disabled Clients User Login Policies AP Policies Password Policies	If LOCAL is selected as LOCAL only if first prior	second priority th thy is unreachable	en user wil be	suthersticated	ogainet		
+ Local EAP							
* Priority Order							
Certificate Access Control Lists							

Priority Order > Management User Selection



Note: If LOCAL is selected as second priority, then the user is authenticated with this method only if the method defined as the first priority (RADIUS/ TACACS) is unreachable.

Verify

In order to verify whether your configuration works properly, access the WLC through the CLI or GUI (HTTP/HTTPS) mode. When the log in prompt appears, type the username and password as configured on the Cisco Secure ACS.

If you have the configurations correct, you are successfully authenticated into the WLC.

You can also ensure whether the authenticated user is provided with access restrictions as specified by the ACS. In order to do so, access the WLC GUI through HTTP/HTTPS (ensure that WLC is configured to allow HTTP/HTTPS).

A user with read-write access set in the ACS has several configurable privileges in the WLC. For example, a read-write user has the privilege to create a new WLAN under the WLANs page of the WLC. This window shows an example.



Configurable Privileges in the WLC

When a user with read only privileges tries to alter the configuration on the controller, the user sees this message.

cisco	MONITOR	VALARE	CONTROLLER	WIPELESS	SECURITY	малариент	COMMANDS	HELP	SEEDBACK
Security	Priority, D	edar≻M	anagement U	587					
 AAA General RADIUS Authentostian Accounting TREACS+ Looi Hill Users MAC Neering Disabled Chients User Logic Policies Artisette Orders Excal EAP Priority Onder Management User Contificate Access Control Lists Wineless Protection Policies Wineless Protection Policies Web Auth Advanced 	Authantic Not U TAGACS	et losi lacd 5+ selected sc 7 Drst prior	second proving the ty is anneoclaphie	Order U	LOCAL RADIUS Auto	nitication Dan Dan Italico Foloci. No ad	n. Ticlant prinkspis		

Cannot Alter the Controller with Read-only Access

These access restrictions can also be verified through the CLI of the WLC. This output shows an example.

```
<#root>
(Cisco Controller) >
?

debug Manages system debug options.
help Help
linktest Perform a link test to a specified MAC address.
logout Exit this session. Any unsaved changes are lost.
show Display switch options and settings.
(Cisco Controller) >config
Incorrect usage. Use the '?' or <TAB> key to list commands.
```

As this example output shows, a?at the controller CLI displays a list of commands available for the current user. Also notice that the **config** command is not available in this example output. This illustrates that a read-only user does not have the privilege to do any configurations on the WLC. Whereas, a read-write user does have the privileges to do configurations on the controller (both GUI and CLI mode).



Note: Even after you authenticate a WLC user through the RADIUS server, as you browse from page to page, the HTTP[S] server still fully authenticates the client each time. The only reason you are not prompted for authentication on each page is that your browser caches and replays your credentials.

Troubleshoot

There are certain circumstances when a controller authenticates management users via the ACS, the authentication finishes successfully (access-accept), and you do not see any authorization error on the controller.But, the user is prompted again for authentication.

In such cases, you cannot interpret what is wrong and why the user cannot log into the WLC with just

the debug aaa events enable command. Instead, the controller displays another prompt for authentication.

One possible reason for this is that the ACS is not configured to transmit the Service-Type attribute for that particular user or group even though the username and password are correctly configured on the ACS.

The output of the **debug aaa events enable** command does not indicate that a user does not have the required attributes (for this example, the Service-Type attribute) even though an **access-accept** is sent back from the AAA server. In this example, **debug aaa events enable** command output shows an example.

<#root>

(Cisco Controller) >

debug aaa events enable

Mon Aug 13 20:14:33 2011: AuthenticationRequest: 0xa449a8c Mon Aug 13 20:14:33 2011: Callback.....0x8250c40 Mon Aug 13 20:14:33 2011: protocolType.....0x00020001 Mon Aug 13 20:14:33 2011: proxyState.....1A:00:00:00:00:00:00-00:00 Mon Aug 13 20:14:33 2011: Packet contains 5 AVPs (not shown) Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Successful transmission of Authentication Packet (id 8) to 172.16.1.1:1812, proxy state 1a:00:00:00:00:00-00:00 Mon Aug 13 20:14:33 2011: ****Enter processIncomingMessages: response code=2 Mon Aug 13 20:14:33 2011: ****Enter processRadiusResponse: response code=2 Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Access-Accept received from RADIUS server 172.16.1.1 for mobile 1a:00:00:00:00:00 receiveId = 0 Mon Aug 13 20:14:33 2011: AuthorizationResponse: 0x9802520 Mon Aug 13 20:14:33 2011: resultCode.....0 Mon Aug 13 20:14:33 2011: protocolUsed.....0x00000001 Mon Aug 13 20:14:33 2011: proxyState.....1A:00:00:00:00:00:00-00:00 Mon Aug 13 20:14:33 2011: Packet contains 0 AVPs:

In this first example debug and events enable command output, you see that Access-Accept is successfully received from the RADIUS server but the Service-Type attribute is not passed onto the WLC. This is because the particular user is not configured with this attribute on the ACS.

Cisco Secure ACS needs to be configured to return the Service-Type attribute after user authentication. The

Service-Type attribute value must be set to either **Administrative** or **NAS-Prompt** based on the user privileges.

This second example shows the debug aaa events enable command output again. However, this time the Service-Type attribute is set to Administrative on the ACS.

<#root>

(Cisco Controller)> debug aaa events enable

Mon Aug 13 20:17:02 2011: AuthenticationRequest: 0xa449f1c Mon Aug 13 20:17:02 2011: Callback.....0x8250c40 Mon Aug 13 20:17:02 2011: protocolType.....0x00020001 Mon Aug 13 20:17:02 2011: proxyState.....1D:00:00:00:00:00:00-00:00 Mon Aug 13 20:17:02 2011: Packet contains 5 AVPs (not shown) Mon Aug 13 20:17:02 2011: 1d:00:00:00:00 Successful transmission of Authentication Packet (id 11) to 172.16.1.1:1812, proxy state 1d:00:00:00:00:00-00:00 Mon Aug 13 20:17:02 2011: ****Enter processIncomingMessages: response code=2 Mon Aug 13 20:17:02 2011: ****Enter processRadiusResponse: response code=2 Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Access-Accept received from RADIUS server 172.16.1.1 for mobile 1d:00:00:00:00:00 receiveId = 0 Mon Aug 13 20:17:02 2011: AuthorizationResponse: 0x9802520 Mon Aug 13 20:17:02 2011: structureSize.....100 Mon Aug 13 20:17:02 2011: resultCode.....0 Mon Aug 13 20:17:02 2011: protocolUsed.....0x00000001 Mon Aug 13 20:17:02 2011: proxyState.....1D:00:00:00:00:00:00-00:00 Mon Aug 13 20:17:02 2011: Packet contains 2 AVPs: Mon Aug 13 20:17:02 2011: AVP[01] Service-Type.....0x00000006 (6) (4 bytes) Mon Aug 13 20:17:02 2011: AVP[02] Class..... CISCOACS:000d1b9f/ac100128/acsserver (36 bytes)

You can see in this previous example output that the Service-Type attribute is passed onto the WLC.

Related Information

- <u>Configure Wireless LAN Controller Configuration Guide</u>
- <u>Configure VLANs on Wireless LAN Controllers</u>
- <u>Configure a RADIUS Server and WLC for Dynamic VLAN Assignment</u>
- <u>Configure Wireless LAN Controller and Lightweight Access Point Basic</u>
- <u>Configure the AP Group VLANs with Wireless LAN Controllers</u>
- <u>Cisco Technical Support & Downloads</u>