Management Access for AireOS WLC through Microsoft NPS

Contents

Introduction Prerequisites Requirements Components Used Background Information Configurations WLC Configuration Microsoft NPS Configuration Verify Troubleshoot

Introduction

This document describes how to configure management access for AireOS WLC GUI and CLI through the Microsoft Network Policy Server (NPS).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Wireless Security Solutions
- AAA and RADIUS concepts
- Basic knowledge of Microsoft Server 2012
- Installation of Microsoft NPS and Active Directory (AD)

Components Used

The information provided in this document is based on the following software and hardware components.

- AireOS controller (5520) on 8.8.120.0
- Microsoft Server 2012

Note: This document is intended to give the readers an example of the configuration required on a Microsoft server for WLC management access. The Microsoft Windows server configuration presented in this document has been tested in the lab and found to work as expected. If you have trouble with the configuration, contact Microsoft for help. The Cisco Technical Assistance Center (TAC) does not support the Microsoft Windows server

configuration. Microsoft Windows 2012 installation and configuration guides can be found on Microsoft Tech Net.

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.

Background Information

When WLC CLI/GUI is accessed, the user is prompted to enter the credentials to successfully log in. The credentials can be verified against either a local database or an external AAA server. In this document, Microsoft NPS is being used as the external authentication server.

Configurations

In this example, two users are configured on the AAA (NPS) viz. **loginuser** and **adminuser**. **loginuser** has just the read-only access while **adminuser** is granted full access.

WLC Configuration

Step 1. Add the RADIUS server on the controller. Navigate to **Security > RADIUS > Authentication**. Click **New** to add the server. Ensure **management** option is enabled so that this server can be used for management access, as shown in this image.

cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Se
Security	RADIUS	Authenti	ication Server	rs > Edit					
 AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella 	Server In Server Ad Shared Si Shared Si Confirm S Key Wrap Apply Cis Apply Cis Port Num Server St Support fi Server Til Network I Managem Tunnel Pri Realm Lis PAC Provi IPSec Cisco ACA	dex ddress(Ipv4 ecret Formi ecret Shared Secr o co ISE Defa co ACA Def ber tatus for CoA meout User tent tent Retrans oxy t isioning	/Ipv6) at ret sult settings ault settings smit Timeout	2 10.106.33.39 ASCII © (Designed fo 0 1812 Enabled © 5 secon ✓ Enable 5 second Enable Enable Enable	er FIPS custom ds	ers and requires a k	œy wrap complia	nt RADIU	S server;
Advanced									

Step 2. Navigate to **Security > Priority Order > Management User**. Ensure that the RADIUS is selected as one of the authentication types.

MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Priority O	rder > N	lanagement l	Jser		
Authentic	ation				
Not U	lsed		Order U	sed for Authe	ntication
TACACS	+	>		RADIUS	Up
		<			Down

Note: If RADIUS is selected as the first priority in the authentication order, local credentials will be used for authentication only if the RADIUS server is unreachable. If RADIUS is selected as a second priority, the RADIUS credentials will be first verified against the local database and then, checked against the configured RADIUS servers.

Microsoft NPS Configuration

Step 1. Open the Microsoft NPS server. Right-click on **Radius Clients**. Click **New** to add the WLC as the RADIUS client.

Enter the required details. Please ensure that the shared secret is the same as the one configured on the controller while the RADIUS server is added.

Step 2. Navigate to **Policies > Connection Request Policies**. Right-click to add a new policy, as shown in the image.

•	Cisco WLC Properties	-
File Action View Help File Action View Help NPS (Local) RADIUS Clients and Servers RADIUS Clients Remote RADIUS Server Policies Connection Request Po Network Policies Health Policies Network Access Protection System Health Validato Remediation Server Gro	Cisco WLC Properties Overview Conditions Settings Policy name: Elsco WLC Policy State # # enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy. Policy enabled Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but nether is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server:	
Metwork Access Protection	select Unspecified	
	OK Cancel Apr	sły

Step 3. Under the **Conditions** tab, select **NAS Identifier** as the new condition. When prompted, enter the hostname of the controller as the value, as shown in the image.

	Cisco WLC Properties	x
Overview Conditions Settin	ngs	
Configure the conditions for the conditions match the connection request, NPS skip	his network policy. ection request, NPS uses this policy to authorize the connection request. If conditions do not match the ps this policy and evaluates other policies, if additional policies are configured.	
Condition	Value	
NAS Identifier	Cisco-WLC	
Condition description: The NAS Identifier condition syntax to specify NAS names	specifies a character string that is the name of the network access server (NAS). You can use pattern matching a	
	Add Edit Remove	
	OK Cancel Ap	ply

Step 4. Navigate to **Policies > Network Policies**. Right-click to add a new policy. In this example, the policy is named **Cisco WLC RW** which implies that the policy is used to provide full (read-write) access. Ensure that the policy is configured as shown here.

0	Cisco WLC RW Properties	x
File Action View Help	Overview Conditions Constraints Settings Policy name: Disco WLC RW Policy State If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. If Policy enabled	
Connection Request Po Network Policies Health Policies Network Access Protection Accounting Templates Management	Access Permission If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. <u>What is access permission?</u>	
	authorization with network policy only; do not evaluate the dial-in properties of user accounts . Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Image: Type of network access server: Unspecified Vendor specific: 10	
< III >	OK Cancel Apply	

Step 5. Under the **Conditions** tab, click **Add**. Select the **User groups** and click **Add**, as shown in the image.

If condition connection	is match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the request, NPS skips this policy and evaluates other policies, if additional policies are configured.	×
	Select condition	
Select a	condition, and then click Add.	^
	 Windows Groups The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups. Machine Groups The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups. User Groups The User Groups condition specifies that the connecting user must belong to one of the selected groups. 	
	Location Groups The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.	-

Step 6. Click on **Add Groups** on the dialog box that appears. On the **Select Group** window that appears, select the desired **object type** and **location** and enter the required object name, as shown in the image.

		Cisco WLC RW P	roperties	s	
Ov	User Group	s	x		
C Specify the g	roup membership required to mate	ch this policy.		on reques	t. If conditions do not match the
Groups				are conf	igured.
					A
				iter must	■ belong to one of the selected
	Add Groups	Remove		: belong to	o one of the selected groups.
	Select G	ОК Са	ncel	o one of t	the selected groups.
Select this obje	ect type:	ioup			pcol (HCAP) location groups
Group			Object Ty	pes	NPS and some third party
From this locati wlanlsc.com	on:		Locatio	ns	Add Cancel
Enter the object	t name to select (<u>examples</u>):				
Domain Admin	<u>s</u>		Check N	ames	. Edit Remove
Advanced.		ОК	Car	ncel	

The condition, if added correctly, should look as shown here.

			Cisco WLC RW Properties	2
verview	Conditions	Constraints	Settings	
Configure If condition	the condition ons match the on request, N	ns for this network of the second sec	work policy. request, NPS uses this policy to authorize the connection request. If conditions do not match the policy and evaluates other policies, if additional policies are configured.	
Cor	ndition	V	/alue	
🚜 Use	er Groups	W	VLANLSC\Domain Admins	
Condition The User	description: Groups cond	lition specifies	s that the connecting user must belong to one of the selected groups.	
			Add Edit Remo	ve

Note: To find out the location and object name details, open the active directory and look for the desired username. In this example, **Domain Admins** consists of users who are given full access. **adminuser** is part of this object name.

	Ac	tive Directory Use	rs and Con	nputers			-	x
File Action View Help Active Directory Users and Com Active Directory Users and Com Saved Queries Wanlsc.com Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accour Users	Admi Name Admi Admi Admi Admi Allow Anan AP US Ar US Ar US AC ert P AC Contr C	Remote control Member Of General Address Admin Use First name: Last name: Display name: Description: Office:	rs and Con Admin Us Remote D Dial-in Account er User Admin User	er Prope Desktop Sen Envir Profile	erties vices Profile onment Telephones	COM+ Sessions Organization		×
< III >	St Doma Doma Doma Emple Enter; Coup Login RAS a Read-	Office: Telephone number: E-mail: Web page:	K C	ancel	Apply	Other Other		

	Active Directory Users and Compute	ers	
File Action View Help	Admin User Properties	? X	
Active Directory Users and Active Directory Users and Saved Queries Managed Service A Users	Remote control Remote Desktop Services Profile General Address Account Profile Telephones Member Of Dial-in Environment Member of: Name Active Directory Domain Services Folder Domain Admins wlanisc.com/Users	COM+ Organization Sessions	rou rou rou rou rou rou rou rou rou rou
	Primary group: Domain Admins Set Primary Group There is no need to change Primary you have Macintosh clients or POSI2 applications. OK Cancel Apply	group unless X-compliant	istra rou rou ir gi rou ip c rou

Step 7. Under the **Constraints** tab, navigate to **Authentication Methods** and ensure only **unencrypted authentication** is checked.

Overview Constraints Settings Configure the constraints for this network policy. F all constraints Y all constraints Constraints Constraints Authentication Methods Authentication Methods EAP types are negotiated between NPS and the client in the order in which they are listed. EAP types are negotiated between NPS and the client in the order in which they are listed. EAP types are negotiated between NPS and the client in the order in which they are listed. EAP types are negotiated between NPS and the client in the order in which they are listed. EAP types are negotiated between NPS and the client in the order in which they are listed. EAP types are negotiated between NPS and the client in the order in which they are listed. EAP types are negotiated between NPS and the client in the order in which they are listed. EAP types are negotiated between NPS and the client in the order in which they are listed. EAP types are negotiated between NPS and the client in the order in which they are listed. EAP types are negotiated between NPS and the client in the order in which they are listed. EAP types Constraints More Down More Down Add Edt Remove Less secure authentication methods: Ouer can change password after thas expired <t< th=""><th></th><th>Cisco WLC RW Properties</th></t<>		Cisco WLC RW Properties
Add Edt Remove Less secure authentication methods: Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired Encrypted authentication (MS-CHAP) User can change password after it has expired Encrypted authentication (CHAP) Vuencrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method Perform machine health check only	Overview Conditions Constraints Settings Configure the constraints for this network poli If all constraints are not matched by the constraints: Constraints: Constraints Constraints: Constraints Muthentication Methods Idle Timeout Session Timeout Session Timeout Called Station ID Day and time restrictions NAS Port Type	Cisco WLC RW Properties Cisco WLC RW Properties Cy. ection request, network access is denied. Allow access only to those clients that authenticate with the specified methods. EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types: Move Up Move Down
	NAS Port Type	Add Edt Remove Less secure authentication methods:

Step 8. Under the **Settings** tab, navigate to **RADIUS Attributes > Standard**. Click **Add** to add a new attribute, **Service-Type**. From the drop-down menu, select **Administrative** to provide full access to the users mapped to this policy. Click on Apply to save the changes, as shown in the image.

ADILIS Attributes	Attailude Information X	
Charderd	Attribute information	andard attribute, and
Standard	Attribute name:	ADIOS CIEILS, See
Vendor Specific	Service-Type	
Network Access Protecti	Attribute number:	
NAP Enforcement	6	
Extended State	Attribute format: Enumerator	
Routing and Remote Acc		
Multilink and Bandwid Allocation Protocol (B	Attribute Value: Commonly used for Dial-Up or VPN	
IP Filters	<pre></pre>	
Encryption	O Commonly used for 802.1x	
No IP Settings	<none></none>	
	Others	
	Administrative	
	OK Crock	
	UK Calicei	

Note: If you want to give read-only access to specific users, select NAS-Prompt from the drop-down. In this example, another policy named **Cisco WLC RO** is created to provide read-only access to users under **Domain Users** object name.

	Cisco WLC RO Properties
Overview Conditions Constr	aints Settings
Configure the conditions for thi If conditions match the connec connection request, NPS skips	s network policy. tion request, NPS uses this policy to authorize the connection request. If conditions do not match the this policy and evaluates other policies, if additional policies are configured.
Condition	Value
all User Groups	WLANLSC\Domain Users
Condition description: The User Groups condition spe	ecifies that the connecting user must belong to one of the selected groups.
	OK Cancel Apply

	Cisco WLC RO Properties	×			
Overview Conditions Constr Configure the settings for this r If conditions and constraints m	aints Settings etwork policy. atch the connection request and the policy grants access, settings are applied.				
Settings: RADIUS Attributes	Attribute Information X	_			
Standard Vendor Specific	Attribute name: Service-Type				
Network Access Protection	Attribute number: 6				
Routing and Remote Acc Build Remote Acc Build Remote Acc	Attribute Value:				
Allocation Protocol (B P IP Filters	Commonly used for Dial-Up or VPN				
Encryption	Commonly used for 802.1x Image: A state of the state of th				
	NAS Prompt V OK Cancel				
	OK Cancel &	sply			

Verify

1. When **loginuser** credentials are used, the user is not allowed to configure any changes on the controller.



General	Security	QoS	Policy-Mapping	Advanced		
Profile Na	ame	tes	tr			
Туре		WL	AN			
SSID		tes	t2			
Status			Enabled			
Security	Policies					
						inges.)
		Autho	rization Failed. No su	fficient privileges		
Radio Pol	icy					
Interface	/Interface Gro					
Multicast	Vlan Feature				Close	
Broadcas	t SSID	0	Lilavieu			
NAS-ID		nor	ne			
Multicast Broadcas NAS-ID	t SSID	nor	ne		Close	

From **debug aaa all enable**, you can see that the service-type attribute's value in authorization response is 7 which corresponds to NAS-prompt.

```
*aaaQueueReader: Dec 07 22:20:14.664: 30:01:00:00:00:00 Successful transmission of
Authentication Packet (pktId 14) to 10.106.33.39:1812 from server queue 0, proxy state
30:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:20:14.664: 00000000: 01 0e 00 48 47 f8 f3 5c 58 46 98 ff 8e f8 20 7a
\dots HG. \backslash XF. . . . z
*aaaQueueReader: Dec 07 22:20:14.664: 00000010: f6 a1 f1 d1 01 0b 6c 6f 67 69 6e 75 73 65 72 02
.....loginuser.
*aaaQueueReader: Dec 07 22:20:14.664: 00000020: 12 c2 34 69 d8 72 fd 0c 85 aa af 5c bd 76 96 eb
...4i.r....\.v..
*aaaQueueReader: Dec 07 22:20:14.664: 00000030: 60 06 06 00 00 07 04 06 0a 6a 24 31 20 0b 43
....j$1..C
*aaaQueueReader: Dec 07 22:20:14.664: 00000040: 69 73 63 6f 2d 57 4c 43 isco-WLC
:
:
*radiusTransportThread: Dec 07 22:20:14.668: 30:01:00:00:00:00 Access-Accept received from
RADIUS server 10.106.33.39 (gid:0) with port:1812, pktId:14
*radiusTransportThread: Dec 07 22:20:14.668: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:20:14.668: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Dec 07 22:20:14.668:
protocolUsed.....0x0000001
*radiusTransportThread: Dec 07 22:20:14.668:
*radiusTransportThread: Dec 07 22:20:14.668: Packet contains 2 AVPs:
*radiusTransportThread: Dec 07 22:20:14.668: AVP[01] Service-
*radiusTransportThread: Dec 07 22:20:14.668: AVP[02]
Class.....DATA (44 bytes)
```

2. When **adminuser** credentials are used, the user should have full access with **service-type** value 6, which corresponds to **administrative**.



```
*aaaQueueReader: Dec 07 22:14:27.439: AuthenticationRequest: 0x7fba240c2f00
*aaaQueueReader: Dec 07 22:14:27.439:
proxyState.....2E:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:14:27.439: Packet contains 5 AVPs:
*aaaQueueReader: Dec 07 22:14:27.439: AVP[01] User-Name......adminuser
(9 bytes)
*aaaQueueReader: Dec 07 22:14:27.439: AVP[04] Nas-Ip-
*aaaQueueReader: Dec 07 22:14:27.439: AVP[05] NAS-Identifier.....Cisco-WLC
(9 bytes)
:
:
*radiusTransportThread: Dec 07 22:14:27.442: 2e:01:00:00:00 Access-Accept received from
RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:13
*radiusTransportThread: Dec 07 22:14:27.442: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:14:27.442:
protocolUsed.....0x00000001
*radiusTransportThread: Dec 07 22:14:27.442:
proxyState.....2E:01:00:00:00:00-00:00
*radiusTransportThread: Dec 07 22:14:27.442: AVP[01] Service-
Type.....0x00000006 (6) (4 bytes)
*radiusTransportThread: Dec 07 22:14:27.442: AVP[02]
Class.....DATA (44 bytes)
```

Troubleshoot

In order to troubleshoot management access to WLC through NPS, run **debug aaa all enable** command.

1. The logs when incorrect credentials are used is shown here.

```
*aaaQueueReader: Dec 07 22:36:39.753: 32:01:00:00:00:00 Successful transmission of
Authentication Packet (pktId 15) to 10.106.33.39:1812 from server queue 0, proxy state
32:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:36:39.753: 00000000: 01 0f 00 48 b7 e4 16 4d cc 78 05 32 26 4c ec 8d
....H....M.x.2&L...
*aaaQueueReader: Dec 07 22:36:39.753: 00000010: c7 a0 5b 72 01 0b 6c 6f 67 69 6e 75 73 65 72 02
..[r..loginuser.
*aaaQueueReader: Dec 07 22:36:39.753: 00000020: 12 03 a7 37 d4 c0 16 13 fc 73 70 df 1f de e3 e4
....7.....sp.....
*aaaQueueReader: Dec 07 22:36:39.753: 00000030: 32 06 06 00 00 07 04 06 0a 6a 24 31 20 0b 43
2....j$1..C
*aaaQueueReader: Dec 07 22:36:39.753: 00000040: 69 73 63 6f 2d 57 4c 43 isco-WLC
*aaaQueueReader: Dec 07 22:36:39.753: 32:01:00:00:00:00 User entry not found in the Local FileDB
for the client.
*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Counted 0 AVPs (processed 20
bytes, left 0)
*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Access-Reject received from
```

RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:15

*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00 Did not find the macaddress to be deleted in the RADIUS cache database

*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Returning AAA Error

'Authentication Failed' (-4) for mobile 32:01:00:00:00:00 serverIdx 1

*radiusTransportThread: Dec 07 22:36:39.763: AuthorizationResponse: 0x7fbaebebf860

*radiusTransportThread: Dec 07 22:36:39.763: structureSize......136

*radiusTransportThread: Dec 07 22:36:39.763: resultCode.....-4

*radiusTransportThread: Dec 07 22:36:39.763:

protocolUsed.....0xfffffff

*radiusTransportThread: Dec 07 22:36:39.763: Packet contains 0 AVPs:

*emWeb: Dec 07 22:36:39.763: Authentication failed for loginuser

2. The logs when service-type is used with a value other than **Administrative (value=6)** or **NAS**-**prompt (value=7)** is shown as follows. In such a case, login fails even if authentication succeeds.

```
*aaaQueueReader: Dec 07 22:46:31.849: AuthenticationRequest: 0x7fba240c56a8
*aaaQueueReader: Dec 07 22:46:31.849: Callback.....0xa3c13ccb70
*aaaQueueReader: Dec 07 22:46:31.849:
*aaaQueueReader: Dec 07 22:46:31.849: Packet contains 5 AVPs:
*aaaQueueReader: Dec 07 22:46:31.849: AVP[01] User-Name......adminuser
(9 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[03] Service-
Type.....0x00000007 (7) (4 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[04] Nas-Ip-
*aaaQueueReader: Dec 07 22:46:31.849: AVP[05] NAS-Identifier.....Cisco-WLC
(9 bytes)
:
*radiusTransportThread: Dec 07 22:46:31.853: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:46:31.853: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Dec 07 22:46:31.853: resultCode.....0
*radiusTransportThread: Dec 07 22:46:31.853:
protocolUsed.....0x0000001
*radiusTransportThread: Dec 07 22:46:31.853: Packet contains 2 AVPs:
*radiusTransportThread: Dec 07 22:46:31.853: AVP[01] Service-
Type.....0x00000001 (1) (4 bytes)
*radiusTransportThread: Dec 07 22:46:31.853: AVP[02]
Class.....DATA (44 bytes)
*emWeb: Dec 07 22:46:31.853: Authentication succeeded for adminuser
```