

Aruba Airwave Authentication TACACS+ via ClearPass

Airwave - Create two new Roles

AMP Setup > Roles

- Create a administrator role amp-admin
- Create a read-only role amp-readonly

This roles will be used in the ClearPass TACACS+ service to enforce the right role.

Aruba AirWave AMP Setup Roles page. The page displays a table of roles with the following columns: NAME, ENABLED, TYPE, ACCESS LEVEL, TOP FOLDER, VISIBLE GROUPS, ALLOW AUTHORIZATION OF DEVICES, RAPIDS, VISUALRF, ARUBA CONTROLLER SINGLE SIGN-ON ROLE, and DISPLAY C. Two roles, 'amp-admin' and 'amp-readonly', are highlighted with a red box. The 'amp-admin' role is an AMP Administrator with an Access Level of '-' and is enabled. The 'amp-readonly' role is a Device Manager with an Access Level of 'Audit (Read Only)' and is enabled. Other roles include 'Admin', 'Read-Only Monitoring & Auditing', and 'Switches_admin'.

NAME	ENABLED	TYPE	ACCESS LEVEL	TOP FOLDER	VISIBLE GROUPS	ALLOW AUTHORIZATION OF DEVICES	RAPIDS	VISUALRF	ARUBA CONTROLLER SINGLE SIGN-ON ROLE	DISPLAY C
Admin	Yes	AMP Administrator	-	Top	All	Yes	Administrator	Read/Write	Disabled	No
amp-admin	Yes	AMP Administrator	-	Top	All	Yes	Administrator	Read/Write	Disabled	No
amp-readonly	Yes	Device Manager	Audit (Read Only)	Top	All	Yes	None	Read Only	Disabled	No
Read-Only Monitoring & Auditing	Yes	Device Manager	Audit (Read Only)	Top	All	Yes	None	Read Only	Disabled	No
Switches_admin	No	Device Manager	Manage (Read/Write)	Top > Switches	Switches	Yes	Read Only	Read/Write	Disabled	No

Aruba Airwave Authentication TACACS+ via ClearPass

Airwave - Role amp-admin

The screenshot shows the Aruba AirWave web interface. The top navigation bar includes the Aruba logo, 'AirWave' text, and status indicators for NEW DEVICES (0), UP (6), DOWN (1), ROGUE (27), CLIENTS (2), and ALERTS (0). A 'Log out marcelkoedijk' link is on the right. The left sidebar contains a menu with 'Home', 'Groups', 'Devices', 'Clients', 'Reports', 'System', 'Device Setup', 'AMP Setup', 'Roles', 'Authentication', and 'MDM Server'. The 'Roles' section is highlighted. The main content area is titled 'Security Verification' and shows the configuration for the 'amp-admin' role. The 'Name' field is 'amp-admin', the 'Type' is 'AMP Administrator', and the 'Aruba Controller Single Sign-on Role' is 'Disabled'. The 'Allow user to disable timeout' is set to 'No'. The 'Guest User Preferences' section has a 'Custom Message' field. 'Save' and 'Cancel' buttons are at the bottom.

aruba | AirWave

NEW DEVICES 0 UP 6 DOWN 1 ROGUE 27 CLIENTS 2 ALERTS 0

Log out marcelkoedijk

Home Groups Devices Clients Reports System Device Setup AMP Setup Roles Authentication MDM Server

Security Verification

Current password for 'marcelkoedijk':

Role

Name: amp-admin

Type: AMP Administrator

Aruba Controller Single Sign-on Role: Disabled

Allow user to disable timeout: Yes No

Guest User Preferences

Custom Message: Enter a Value

Save Cancel

Airwave - Role amp-readonly

The screenshot shows the Aruba AirWave web interface. The top navigation bar includes the Aruba logo, 'AirWave' text, and status indicators for NEW DEVICES (0), UP (6), DOWN (1), ROGUE (27), CLIENTS (2), and ALERTS (0). A 'Log out marcelkoedijk' link is on the right. The left sidebar contains a menu with 'Home', 'Groups', 'Devices', 'Clients', 'Reports', 'System', 'Device Setup', 'AMP Setup', 'Roles', 'Authentication', and 'MDM Server'. The 'Roles' section is highlighted. The main content area is titled 'Security Verification' and shows the configuration for the 'amp-readonly' role. The 'Name' field is 'amp-readonly', the 'Enabled' checkbox is checked, the 'Type' is 'Device Manager', and the 'Aruba Controller Single Sign-on Role' is 'Disabled'. The 'Allow user to disable timeout' is set to 'No'. The 'Guest User Preferences' section has a 'Custom Message' field. 'Save' and 'Cancel' buttons are at the bottom.

aruba | AirWave

NEW DEVICES 0 UP 6 DOWN 1 ROGUE 27 CLIENTS 2 ALERTS 0

Log out marcelkoedijk

Home Groups Devices Clients Reports System Device Setup AMP Setup Roles Authentication MDM Server

Security Verification

Current password for 'marcelkoedijk':

Role

Name: amp-readonly

Enabled: Yes No

Type: Device Manager

Aruba Controller Single Sign-on Role: Disabled

Allow user to disable timeout: Yes No

Guest User Preferences

Custom Message: Enter a Value

Save Cancel

Aruba Airwave Authentication TACACS+ via ClearPass

Airwave - TACACS+ Configuration

AMP Setup > Authentication

- Enter the ClearPass hostname or IP address and Pre-Shared Key in the TACACS+ Configuration area.

The screenshot shows the Aruba AirWave web interface for configuring authentication. The left sidebar lists various configuration areas: Authentication (selected), MDM Server, Device Type Setup, WLSE, ACS, NMS, RADIUS Accounting, PCI Compliance, External Server, RAPIDS, and VisualIRF. The main content area displays the 'Authentication' configuration page. At the top, there are status indicators for NEW DEVICES (0), UP (6), DOWN (1), ROGUE (27), CLIENTS (2), and ALERTS (0). The configuration options include:

- Enable AMP Whitelist:** Radio buttons for Yes and No.
- Certificate Authentication:**
 - Enable Certificate Authentication:** Radio buttons for Yes and No.
 - Single Sign-on:**
 - Enable Single Sign-on:** Radio buttons for Yes and No. A note states: "Single Sign-On only works with AOS 6.3.0.0 or later".
 - Authentication Priority:** Radio buttons for Local and Remote.
- RADIUS Configuration:**
 - Enable RADIUS Authentication and Authorization:** Radio buttons for Yes and No.
 - TACACS+ Configuration (highlighted with a red box):**
 - Enable TACACS+ Authentication and Authorization:** Radio buttons for Yes and No.
 - Primary Server Hostname/IP Address:** Text input field with value 172.16.200.2.
 - Primary Server Port (1-65535):** Text input field with value 49.
 - Primary Server Secret:** Password input field.
 - Confirm Primary Server Secret:** Password input field.
 - Secondary Server Hostname/IP Address:** Text input field with placeholder "Enter a Value".
 - Secondary Server Port (1-65535):** Text input field with value 49.
 - Secondary Server Secret:** Password input field.
 - Confirm Secondary Server Secret:** Password input field.
- LDAP Configuration:**
 - Enable LDAP Authentication and Authorization:** Radio buttons for Yes and No.

At the bottom right, there are **Save** and **Revert** buttons.

Aruba Airwave Authentication TACACS+ via ClearPass

ClearPass - Service Summary

The screenshot displays the Aruba ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with categories: Dashboard, Monitoring, Configuration, and Administration. The 'Configuration' section is expanded, showing sub-items like Service Templates & Wizards, Services, Authentication, Identity, Posture, Enforcement, Policies, Profiles, Network, Devices, Device Groups, Proxy Targets, Event Sources, Network Scan, and Policy Simulation. The main content area is titled 'ClearPass Policy Manager' and shows the configuration for 'Services - HomeLAB - Airwave Login Service'. The 'Summary' tab is selected, displaying the following details:

- Service:**
 - Name: HomeLAB - Airwave Login Service
 - Description:
 - Type: TACACS+ Enforcement
 - Status: Enabled
 - Monitor Mode: Disabled
 - More Options: -
- Service Rule:**
 - Match ANY of the following conditions:
 - | Type | Name | Operator | Value |
|---------------|----------------|------------------|------------------------|
| 1. Connection | NAD-IP-Address | BELONGS_TO_GROUP | HomeLAB - _AMP_SERVERS |
- Authentication:**
 - Authentication Sources: DC01.MARCLKOEDIJK.NL [Active Directory]
 - Strip Username Rules: -
- Roles:**
 - Role Mapping Policy: HomeLAB - Airwave Role Mapping
- Enforcement:**
 - Use Cached Results: Disabled
 - Enforcement Policy: HomeLAB - HomeLAB - Airwave Login Policy

At the bottom of the configuration area, there are buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'. The footer of the interface shows the copyright information: '© Copyright 2020 Hewlett Packard Enterprise Development LP', the date and time: 'Jul 04, 2020 19:08:44 CEST', and the version: 'ClearPass Policy Manager 6.9.0.130064 on CLABV (Trial Version) platform'.

Aruba Airwave Authentication TACACS+ via ClearPass

ClearPass - Service Rule

Configuration » Services » Edit - HomeLAB - Airwave Login Service

Services - HomeLAB - Airwave Login Service

Summary **Service** Authentication Roles Enforcement

Name: HomeLAB - Airwave Login Service

Description:

Type: TACACS+ Enforcement



Status: Enabled

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization

Service Rule

Matches ☒ ANY or ☐ ALL of the following conditions:

Type	Name	Operator	Value	
1. Connection	NAD-IP-Address	BELONGS_TO_GROUP	HomeLAB -_AMP_SERVERS	 
2. Click to add...				






ClearPass - Service Authentication

Configuration » Services » Edit - HomeLAB - Airwave Login Service

Services - HomeLAB - Airwave Login Service

Summary Service **Authentication** Roles Enforcement

Authentication Sources: DC01.MARCKOEDIJK.NL (Active Directory) [Add New Authentication Source](#)

--Select to Add--

Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Aruba Airwave Authentication TACACS+ via ClearPass

ClearPass - Service Roles

Configuration » Services » Edit - HomeLAB - Airwave Login Service

Services - HomeLAB - Airwave Login Service

Summary Service Authentication **Roles** Enforcement

Role Mapping Policy: HomeLAB - Airwave Role Mapping Modify Add New Role Mapping Policy

Role Mapping Policy Details

Description:

Default Role: [Other]

Rules Evaluation Algorithm: first-applicable

Conditions	Role
1. (Authorization:DC01.MARCLKOEDIJK.NL:UserDN <i>CONTAINS</i> CN=Users,DC=marcelkoedijk,DC=nl)	HomeLAB - _AMP_ADMIN_ROLE

ClearPass - Service Enforcement

Configuration » Services » Edit - HomeLAB - Airwave Login Service

Services - HomeLAB - Airwave Login Service

Summary Service Authentication Roles **Enforcement**

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: HomeLAB - HomeLAB - Airwave Login Policy Modify Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [TACACS Deny Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Tips:Role <i>EQUALS</i> HomeLAB - _AMP_ADMIN_ROLE)	HomeLAB - Airwave Admin Profile
2. (Tips:Role <i>EQUALS</i> HomeLAB - _AMP_VIEWONLY_ROLE)	HomeLAB - Airwave Readonly Profile

Aruba Airwave Authentication TACACS+ via ClearPass

ClearPass - Enforcement Profile Admin

Configuration » Enforcement » Profiles » Edit Enforcement Profile - HomeLAB - Airwave Admin Profile

Enforcement Profiles - HomeLAB - Airwave Admin Profile

Summary Profile Services

Profile:

Name:	HomeLAB - Airwave Admin Profile
Description:	
Type:	TACACS
Action:	Accept
Device Group List:	-

Services:

Privilege Level:	0
Selected Services:	1. AMP:https
Authorize Attribute Status:	ADD
Custom Services:	-

Service Attributes			
Type	Name	=	Value
1. AMP:https	role	=	amp-admin

ClearPass - Enforcement Profile Admin

Configuration » Enforcement » Profiles » Edit Enforcement Profile - HomeLAB - Airwave Admin Profile

Enforcement Profiles - HomeLAB - Airwave Admin Profile

Summary **Profile** Services

Name:	HomeLAB - Airwave Admin Profile		
Description:	<div></div>		
Type:	TACACS		
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop		
Device Group List:	<div></div> <div>--Select--</div>	<div>Remove</div> <div>View Details</div> <div>Modify</div>	Add New Device Group

Aruba Airwave Authentication TACACS+ via ClearPass

ClearPass - Enforcement Profile Admin

- The role "amp-admin" will be enforced, this is the role we early create on the Airware Management Platform

Configuration » Enforcement » Profiles » Edit Enforcement Profile - HomeLAB - Airwave Admin Profile

Enforcement Profiles - HomeLAB - Airwave Admin Profile

Summary Profile **Services**

Privilege Level: 0 (Minimum)



Selected Services: AMP:https [Export All TACACS+ Services Dictionaries](#)

Remove

--Select--

Authorize Attribute Status: ADD

Custom Services: To add new TACACS+ services / attributes, upload the modified dictionary xml - Update TACACS+ Services Dictionary

Service Attributes				
Type	Name	=	Value	
1. AMP:https	role	=	amp-admin	 
2.	Click to add...			

ClearPass - Enforcement Profile Read Only

Configuration » Enforcement » Profiles » Edit Enforcement Profile - HomeLAB - Airwave Readonly Profile

Enforcement Profiles - HomeLAB - Airwave Readonly Profile

Summary Profile **Services**

Profile:

Name: HomeLAB - Airwave Readonly Profile

Description:

Type: TACACS

Action: Accept

Device Group List: -

Services:

Privilege Level: 0

Selected Services: 1. AMP:https

Authorize Attribute Status: ADD

Custom Services: -

Service Attributes				
Type	Name	=	Value	
1. AMP:https	role	=	amp-readonly	

Aruba Airwave Authentication TACACS+ via ClearPass

ClearPass - Enforcement Profile Read Only

Configuration » Enforcement » Profiles » Edit Enforcement Profile - HomeLAB - Airwave Readonly Profile

Enforcement Profiles - HomeLAB - Airwave Readonly Profile

Summary **Profile** Services

Name:	HomeLAB - Airwave Readonly Profile		
Description:	<div></div>		
Type:	TACACS		
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop		
Device Group List:	<div></div> <div>--Select--</div>	<div>Remove</div> <div>View Details</div> <div>Modify</div>	<div>Add New Device Group</div>

ClearPass - Enforcement Profile Read Only

- The role "amp-readonly" will be enforced, this is the role we early create on the Airware Management Platform

Configuration » Enforcement » Profiles » Edit Enforcement Profile - HomeLAB - Airwave Readonly Profile

Enforcement Profiles - HomeLAB - Airwave Readonly Profile

Summary Profile **Services**

Privilege Level:	0 (Minimum)		
Selected Services:	<div>AMP:https</div> <div>--Select--</div>	<div>Remove</div>	<div>Export All TACACS+ Services Dictionaries</div>
Authorize Attribute Status:	ADD		
Custom Services:	To add new TACACS+ services / attributes, upload the modified dictionary xml - Update TACACS+ Services Dictionary		

Service Attributes			
Type	Name	=	Value
1.	AMP:https	role	= amp-readonly
2.	Click to add...		