



(/arubapedia/index.php/Main_Page) Welcome to ARUBAPEDIA

Hbharadwaj@arubanetworks.com (/arubapedia/index.php/User:Hbharadwaj@arubanetworks.com)

Talk (/arubapedia/index.php/User_talk:Hbharadwaj@arubanetworks.com)

Preferences (/arubapedia/index.php/Special:Preferences)

Watchlist (/arubapedia/index.php/Special:Watchlist)

Contributions (/arubapedia/index.php/Special:Contributions/Hbharadwaj@arubanetworks.com)

Log out (/arubapedia/index.php?title=Special:UserLogout&returnto=ClearPass+Guest+on+Juniper+WLC)

Page (/arubapedia/index.php/ClearPass_Guest_on_Juniper_WLC)

Discussion (/arubapedia/index.php?title=Talk:ClearPass_Guest_on_Juniper_WLC&action=edit&redlink=1)

Edit (/arubapedia/index.php?title=ClearPass_Guest_on_Juniper_WLC&action=edit)

History (/arubapedia/index.php?title=ClearPass_Guest_on_Juniper_WLC&action=history)

Move (/arubapedia/index.php/Special:MovePage/ClearPass_Guest_on_Juniper_WLC)

Watch (/arubapedia/index.php?

title=ClearPass_Guest_on_Juniper_WLC&action=watch&token=9889d1d69cc94678ba1029e4beb0f45f%2B%5C)

Refresh (/arubapedia/index.php?title=ClearPass_Guest_on_Juniper_WLC&action=purge)

ClearPass Guest on Juniper WLC

Translate this page to de - Deutsch

This is a CLASS-3 (/arubapedia/index.php/Aruba_Data_Policy) Article - PARTNER APPROVED CONTENT
(/arubapedia/index.php/Help:Data_Handling_Procedures)

Contents

- 1 Overview
- 2 Configuration
- 3 Testing

Overview

This page covers some configuration guidance on getting a Juniper WLC (Trapeze) to work with ClearPass Guest to deploy a Guest solution. This document assumes that the reader knows the basics of how to setup ClearPass Guest with more common network devices like Cisco and Aruba, and is familiar with CoAs, Services, and Server-Initiated web login modes of operation. Also outside the scope is basic Juniper WLC configuration beyond the screen shots provided. Explanation of these basics is outside the scope of this document, we will instead focus on nuances that need to be considered for making ClearPass Guest work with a Juniper WLC.

If you read the below knowledge base article from Juniper, you can see that Guest login occurs a bit differently than it does on Aruba and Cisco based network devices:

<http://kb.juniper.net/InfoCenter/index?page=content&id=KB23298> (<http://kb.juniper.net/InfoCenter/index?page=content&id=KB23298>)

The important parts of the flow are here:

1. Users associate to a web portal enabled service and are placed in the WEB-PORTAL state.
2. All user traffic is blocked, except DNS and DHCP requests via the portal ACL, which is in place. The portal ACL should be modified, if SmartPass is used to serve the portal page to the client. The modification should include rules for allowing traffic to the SmartPass IP address and the port which is running the service.
3. HTTP/HTTPS data is redirected to a configured external authentication web server. This is performed by configuring a dedicated ACL rule and setting the web-portal-form attribute in the web portal service profile.
4. The external web server directly interacts with the user web browser to validate credentials, by presenting the Login web page to the user; who is trying to browse the Internet.
5. Once the credentials have been confirmed, the external server sends a CoA request (RFC3576) to the originating Controller. The CoA contains a request for the session username change. The web portal session will become authorized and active at that time. The web portal ACL will be removed to allow normal traffic to take place. Additional CoA attributes can be set by the external web server at the same time.
6. On successful authentication and authorization, the client will be automatically redirected to the web page, which it was initially trying to browse. Optionally, the client can also be sent a logout page, which will explicitly log out the user by setting their Controller session in the WEB-PORTAL state again.

All seems very normal for a server-initiated web login workflow, except for a key nuance in #5 above. The CoA that is sent is not to bounce the user to reauthenticate them, but instead meant to switch the user's state from pre-login to post-login. To do so, we also need to have a custom crafted CoA that has the following information:

1. Trpz-CoA-Replace-User – Trapeze VSA 12
2. Filter-Id – RADIUS Attribute 11

We do not have by default attribute #1 in our Trapeze dictionary and we do not have a CoA that is formatted with this attribute by default, so we must create both. The Trapeze CoA Replace User VSA attribute will be present in the CoA message and its value will be the user name of the user, who was successfully authenticated, and will replace the WEB-PORTAL state user name in the Controller session.

By default, the Filter-Id attribute will be sent with an empty string value, which will clear the portalacl ACL and will allow client traffic to flow normally. You can however set a filter-id to be used for post-auth filtering.

The CoA message will make use of the client MAC address, which is received within the redirect URL, to identify the session. You also have the option to set the username with the CoA.

One extra step here however is that we MUST have a MacAuth request sent before the user gets to the web login page because we need some request to tie the CoA back to that we will send, so, the Juniper WLC MUST be setup to do MacAuth first, with Web fall through. The MacAuth in this situation will always pass, so, Mac-Caching is not an option.

Configuration

The following configuration assumes that you have created a Guest SSID on the WLC, configured to point to a web login page on ClearPass that has been configured as a "server initiated" type of web login, after a MacAuth request. The following are specifics to this network device to make this work.

Step 1: Add the Juniper WLC as a Network Device in CPPM, but set the Vendor to "IETF". This is needed since we will need to build an "IETF-Generic" custom CoA.

Step 2: Add attribute to the Trapeze dictionary. As of the writing of this document, the Trpz-CoA-Replace-User attribute does not exist in the Trapeze Radius dictionary in CPPM. You could manually export the existing dictionary, add this attribute, and then import back into CPPM. This has been done for you, just download the following file, unzip, and import into CPPM in the Administration>Dictionary>RADIUS page. Note, a feature request is on file to add this into the Radius dictionary by default
<https://redmine.amigopod.arubanetworks.com/redmine/issues/26478>
<https://redmine.amigopod.arubanetworks.com/redmine/issues/26478>)).

File:RadiusDictionary.xml.zip (/arubapedia/index.php/File:RadiusDictionary.xml.zip)

Step 3: Create a custom CoA with the following attributes:

Radius:Trapeze	Trpz-CoA-Replace-User	=	%{Authentication:Full-Username}
Radius:IETF	Filter-Id	=	<blank or name of the post-auth ACL that will be used>
Radius:IETF	NAS-IP-Address	=	%{Radius:IETF:NAS-IP-Address}
Radius:IETF	Calling-Station-Id	=	%{Radius:IETF:Calling-Station-Id}
Radius:IETF	Framed-IP-Address	=	%{Connection:Client-IP-Address}

For example:

Configuration » Enforcement » Profiles » Edit Enforcement Profile - Juniper WLC WebAuth

Enforcement Profiles - Juniper WLC WebAuth

Summary	Profile	Attributes
Profile:		
Name:	Juniper WLC WebAuth	
Description:		
Type:	RADIUS_CoA	
Action:	CoA	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:IETF	Framed-IP-Address	= %{Connection:Client-IP-Address}
2. Radius:Trapeze	Trpz-CoA-Replace-User	= %{Authentication:Full-Username}
3. Radius:IETF	Filter-Id	= byod_acl.in
4. Radius:IETF	NAS-IP-Address	= %{Radius:IETF:NAS-IP-Address}
5. Radius:IETF	Calling-Station-Id	= %{Radius:IETF:Calling-Station-Id}

(/arubapedia/index.php/File:juniper-wlc-guest-cppm-1.jpg)

Do this by navigating to Configuration>Enforcement>Profiles and click "Add" in the upper right. Under "Profile" tab, select "Radius Change of Authorization (CoA)" Template, give the profile a name and then click the "Attributes" tab, and select "IETF-Generic-CoA-IETF" template. Once done, add the attributes above and click "Save".

One note on the filter, Juniper WLC require ".in" or ".out" at the end of the name to define direction of the ACL.

Step 4: You should already have at least two services configured to make a server-initiated web login work, a "WebAuth" one that will initiate the CoA and a "Radius" one for Mac Auth, for Mac-Caching and bypassing of web portal for authenticated users that have just been bounced via CoA. Edit the "WebAuth" service. Under the Enforcement tab, create a rule that triggers this new CoA upon user authentication. See condition #1 below as an example (ignore condition #2, not required, part of testing):

Configuration » Services » Edit - JPPSS-BYOD WebAuth

Services - JPPSS-BYOD WebAuth

Summary	Service	Authentication	Authorization	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions				
Enforcement Policy:	JPPSS-BYOD WebAuth Enforcement Modify				Add new Enforcement Policy
Enforcement Policy Details					
Description:					
Default Profile:	Juniper WLC WebAuth				
Rules Evaluation Algorithm:	first-applicable				
Conditions		Enforcement Profiles			
1.	(Tips:Role EQUALS [User Authenticated])	Juniper WLC WebAuth			
2.	(Tips:Role EQUALS [User Authenticated])	JPPSS-BYOD Guest MAC Caching, JPPSS-BYOD Guest Session Limit, JPPSS-BYOD Guest Do Expire, JPPSS-BYOD Guest Expire Post Login, [Update Endpoint Known], [Trapeze - Terminate Session], [Juniper Terminate Session]			

(/arubapedia/index.php/File:juniper-wlc-guest-cppm-3.jpg)

Step 5: As stated above, you must have a MacAuth service that is set to Accept any request. This is mandatory otherwise the CoA will not work. Ignore the mac-caching conditions in this policy example, notice the default enforcement is to Allow.

Configuration » Services » Edit - JPPSS-BYOD Guest MAC Authentication

Services - JPPSS-BYOD Guest MAC Authentication

Summary	Service	Authentication	Authorization	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions				
Enforcement Policy:	JPPSS-BYOD Guest MAC Authentication Poli Modify				Add new Enforcement Policy
Enforcement Policy Details					
Description:	Sample policy for MAC caching specifying a lifetime depending on role				
Default Profile:	[Allow Access Profile]				
Rules Evaluation Algorithm:	first-applicable				
Conditions		Enforcement Profiles			
1.	(Tips:Role EQUALS [Guest]) AND (Endpoint:Username EXISTS) AND (Authorization:[Insight Repository]:Hours-Since-Auth LESS_THAN 8)	JPPSS-BYOD Guest MAC Caching Allow Access Profile			

(/arubapedia/index.php/File:juniper-wlc-guest-cppm-4.jpg)

Step 6: Ensure that your web login page is set to "Login Method" of "Server Initiated". The Vendor in this case really does not matter. You may want to set login delay to 5 seconds to ensure CoA takes place and state is changed on controller before redirecting to welcome/landing page.

Home » Configuration » Web Logins

Web Login (JPPSS-BYOD Login)

Use this form to make changes to the Web Login **JPPSS-BYOD Login**.

Web Login Editor	
* Name:	<input type="text" value="JPPSS-BYOD Login"/> Enter a name for this web login page.
Page Name:	<input type="text" value="byod_login"/> Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	<div style="border: 1px solid #ccc; height: 30px; width: 100%;"></div> Comments or descriptive text about the web login.
* Vendor Settings:	<input type="text" value="Trapeze Networks"/> ▼ Select a predefined group of settings suitable for standard network configurations.
Login Method:	<input type="text" value="Server-initiated — Change of authorization (RFC 3576) sent to controller"/> ▼ Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
Login Form Options for specifying the behaviour and content of the login form.	
Authentication:	<input type="text" value="Credentials – Require a username and password"/> ▼ Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Access Code and Anonymous require the account to have the Username Authentication field set.

(/arubapedia/index.php/File:juniper-wlc-guest-cppm-9.jpg)

Step 7: Ensure Juniper WLC is configured correctly. As stated, the exact config steps are outside the scope of this document, but a couple of important points:

1. Ensure SSID is set for Mac and Web Auth
2. Enable Accounting and Change of Authorization for the Radius server config
3. Disable "Enable Replay Protection" in Radius server config **VERY IMPORTANT**

The screenshot shows the 'AAA Profile Access Properties' dialog box with the 'Accounting' tab selected. The 'Enabled' checkbox is checked. The 'Record Type' is set to 'Start-Stop'. The 'Available AAA Server Groups' list contains 'LOCAL', 'Radius Server Group: sp-radius-server-group', and 'Radius Server Group: webview-default'. The 'Current AAA Server Groups' list contains 'Radius Server Group: Clearpass'. The 'Add', 'Remove', 'Up', and 'Down' buttons are visible between the two lists. The 'Help', 'OK', and 'Cancel' buttons are at the bottom.

AAA Profile Access Properties

AAA Profile Access | Accounting

Accounting

Enabled ☒

Record Type: Start-Stop

Available AAA Server Groups

- LOCAL
- Radius Server Group: sp-radius-server-group
- Radius Server Group: webview-default

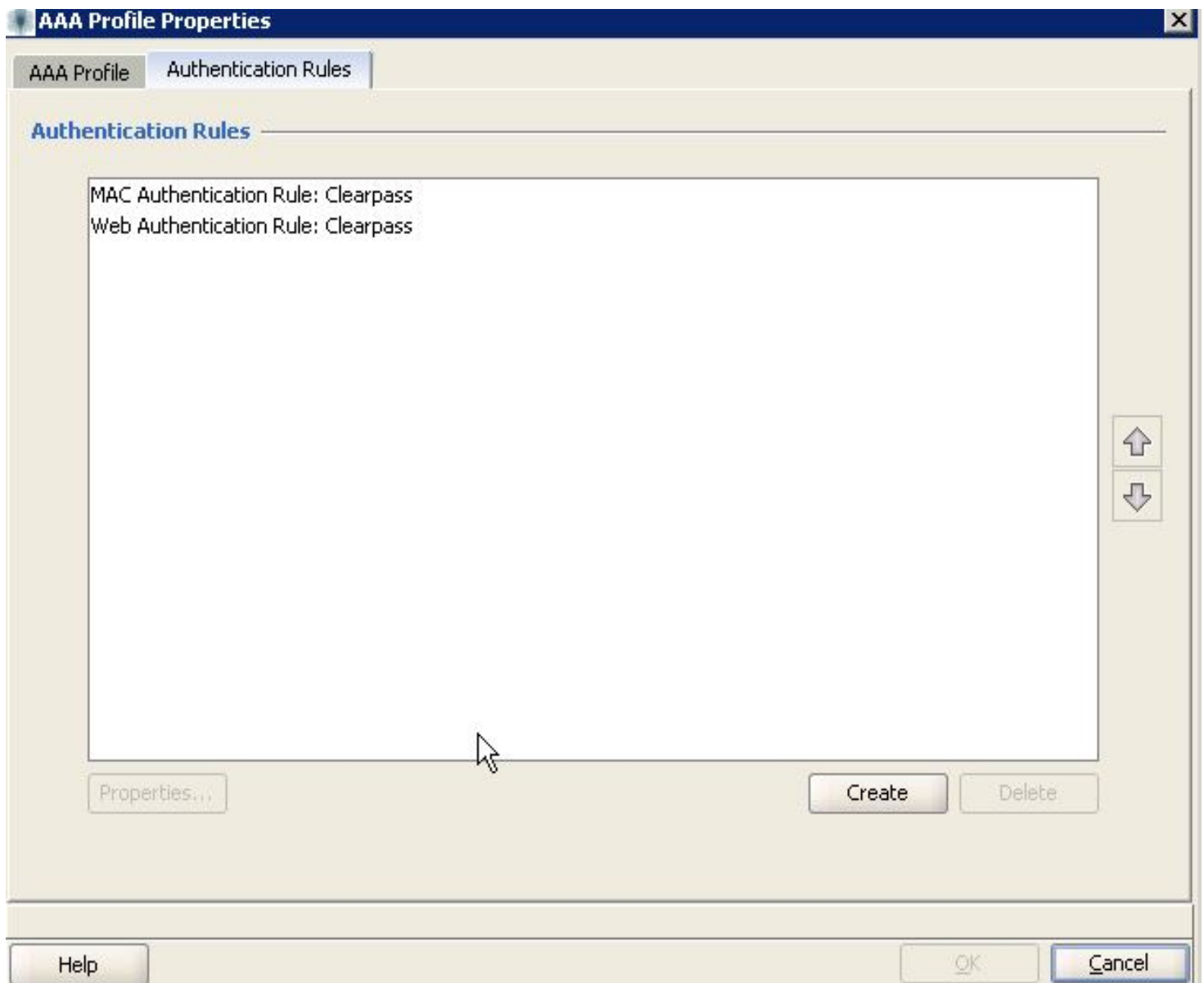
Current AAA Server Groups

- Radius Server Group: Clearpass

Buttons: Add, Remove, Up, Down

Buttons: Help, OK, Cancel

(/arubapedia/index.php/File:juniper-wlc-guest-ring-1.jpg)



(/arubapedia/index.php/File:juniper-wlc-guest-ring-2.jpg)

Configuration - AAA Profiles □

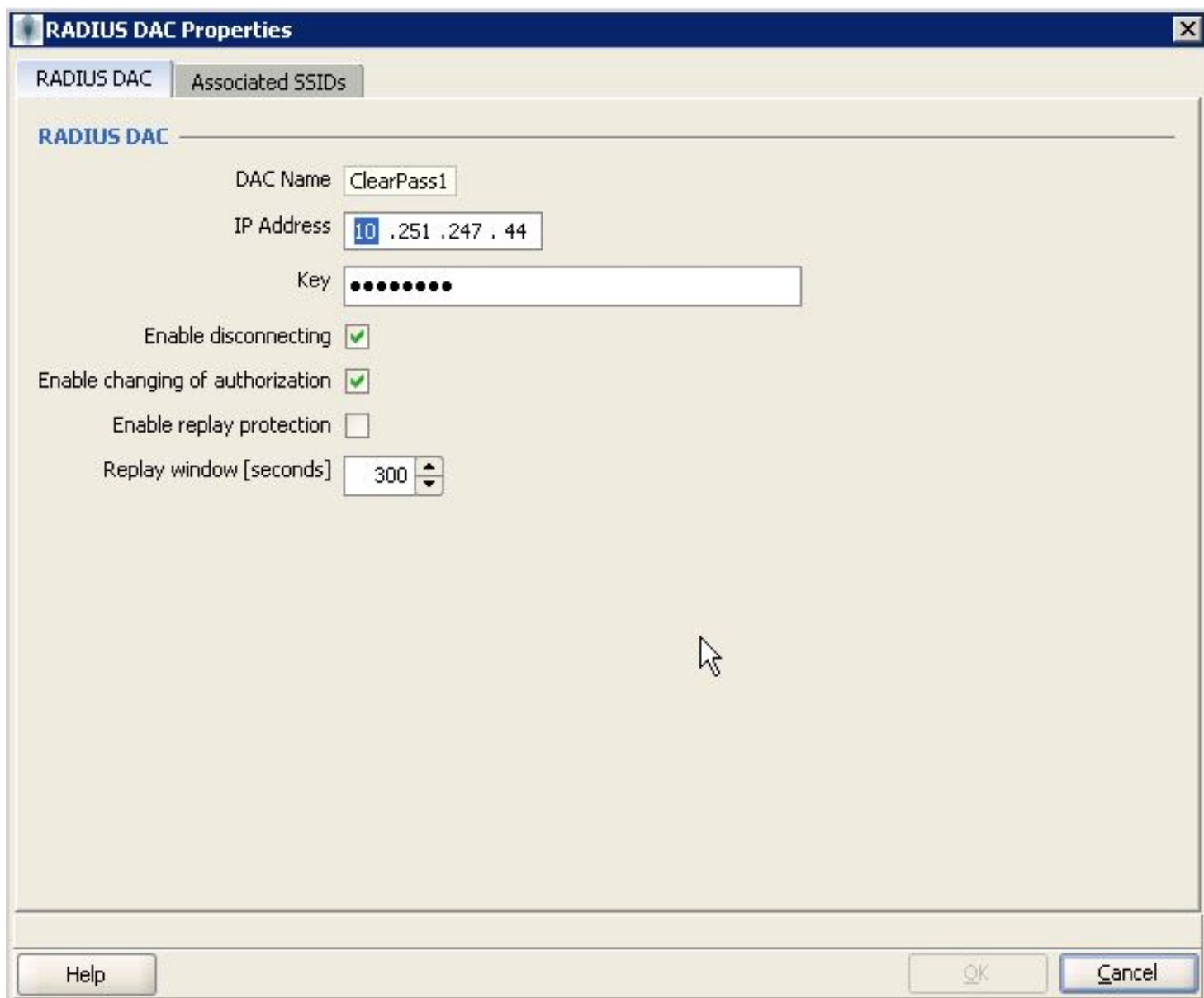
AAA Profiles

#	Name	Authentication Rules	Assigned SSIDs
1	BYOD-Juniper-Clearpass	MAC, Web	JPPSS-BYOD

AAA Profile Access

#	SSID Name	Wired	<input checked="" type="checkbox"/> Accounting Enabled	Accounting Servers	AAA Profile
1	JPPSS-BYOD	No	<input checked="" type="checkbox"/>	Radius Server Group: Cle...	BYOD-Juniper-Clearpass ▼

(/arubapedia/index.php/File:juniper-wlc-guest-ring-3.jpg)



The image shows a Windows-style dialog box titled "RADIUS DAC Properties". It has two tabs: "RADIUS DAC" (selected) and "Associated SSIDs". The "RADIUS DAC" tab contains the following fields and options:

- DAC Name:** A text box containing "ClearPass1".
- IP Address:** A text box containing "10 .251 .247 . 44".
- Key:** A text box containing ten dots (••••••••••).
- Enable disconnecting:** A checkbox that is checked (indicated by a green checkmark).
- Enable changing of authorization:** A checkbox that is checked (indicated by a green checkmark).
- Enable replay protection:** An unchecked checkbox.
- Replay window [seconds]:** A spinner box set to "300".

At the bottom of the dialog are three buttons: "Help", "OK", and "Cancel". A mouse cursor is visible over the "OK" button.

(/arubapedia/index.php/File:juniper-wlc-guest-ring-4.jpg)

File Services Tools Help

Organizer

Configuration - RADIUS

Save Discard

RADIUS

Use System IP Address ☐

RADIUS Servers

#	Name	IP Address	Key	Authentication Port	Accounting Port
1	SmartPass	10 .251 .247 .45	*****	1,812	1,813
2	ClearPass1	10 .251 .247 .44	*****	1,812	1,813

Properties... Delete

RADIUS Server Groups

#	Name	Load Balance	Radius Server List
1	sp-radius-server-group	<input type="checkbox"/>	Server: SmartPass
2	webview-default	<input type="checkbox"/>	Server: ClearPass1
3	Clearpass	<input type="checkbox"/>	Server: ClearPass1

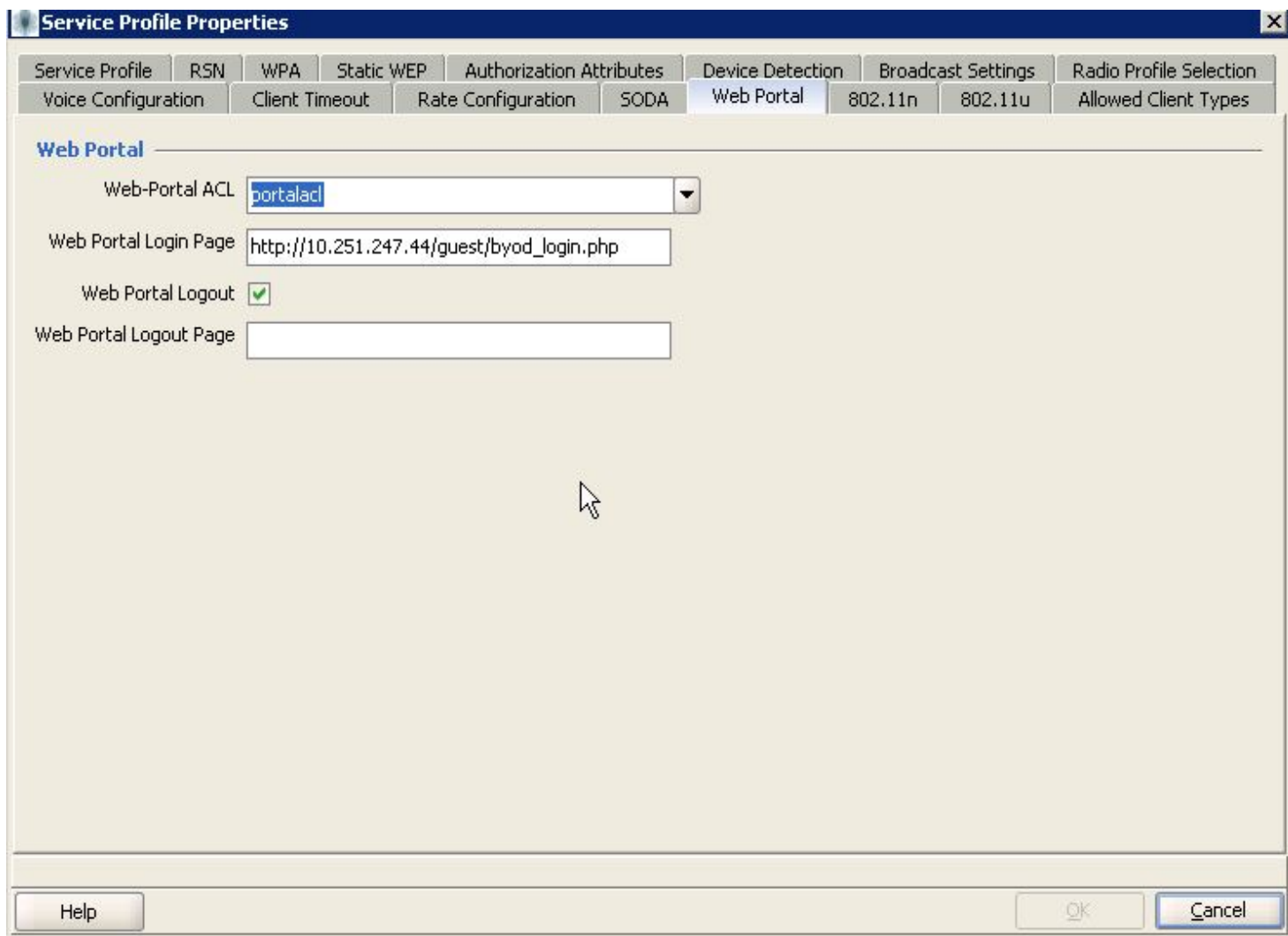
Properties... Delete

RADIUS Dynamic Authorization Clients

#	DAC Name	IP Address	Key	Associated SSIDs
1	SmartPass	10 .251 .247 .45	*****	JPPSS-Guest
2	ClearPass1	10 .251 .247 .44	*****	JPPSS-PT, JPPSS-BYOD

Properties... Delete

(/arubapedia/index.php/File:juniper-wlc-guest-ring-5.jpg)



The image shows a screenshot of the 'Service Profile Properties' dialog box, specifically the 'Web Portal' tab. The dialog has a title bar with a close button. Below the title bar is a tabbed interface with the following tabs: Service Profile, RSN, WPA, Static WEP, Authorization Attributes, Device Detection, Broadcast Settings, Radio Profile Selection, Voice Configuration, Client Timeout, Rate Configuration, SODA, Web Portal (selected), 802.11n, 802.11u, and Allowed Client Types. The 'Web Portal' tab contains the following fields:

- Web-Portal ACL: A dropdown menu showing 'portalacl'.
- Web Portal Login Page: A text box containing 'http://10.251.247.44/guest/byod_login.php'.
- Web Portal Logout: A checkbox that is checked.
- Web Portal Logout Page: An empty text box.

At the bottom of the dialog are three buttons: 'Help', 'OK', and 'Cancel'.

(/arubapedia/index.php/File:juniper-wlc-guest-ring-6.jpg)

Testing


Step 1: Connect a client to the guest SSID. You should see a successful MacAuth request in CPPM:

Request Details

Summary
Input
Output
RADIUS CoA
Accounting
Alerts

Session Identifier:	R000006f4-01-543eda02
Date and Time:	Oct 15, 2014 15:33:06 CDT
End-Host Identifier:	00-EE-BD-5B-97-08
Username:	00-ee-bd-5b-97-08
Access Device IP/Port:	10.119.96.10:39099
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	JPPSS-BYOD Guest MAC Authentication
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Endpoints Repository], [Insight Repository], JPPSS-BYOD MAC-Guest-Check
Roles:	[Guest], [User Authenticated]
Enforcement Profiles:	[Allow Access Profile]
Service Monitor Mode:	Disabled
Online Status:	 Online

Showing 4 of 1-100 records
Change Status
Export
Show Logs
Close

(/arubapedia/index.php/File:juniper-wlc-guest-cppm-5.jpg)


Step 2: Open browser, go through web login process and click login. You should see the WebAuth service entry in Access Tracker and that it initiated the CoA. If you go to the previous Mac Auth entry in Access Tracker, you should see the CoA tab.

Request Details

SummaryInputOutputAlerts

Session Identifier:	W00000055-01-543eda45
Date and Time:	Oct 15, 2014 15:34:13 CDT
End-Host Identifier:	00eebd5b9708
Username:	robbie@aruba.com
Access Device IP/Port:	-
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	JPPSS-BYOD WebAuth
Authentication Method:	Not applicable
Authentication Source:	[Guest User Repository]
Authorization Source:	[Guest User Repository], [Endpoints Repository]
Roles:	[Guest], [User Authenticated]
Enforcement Profiles:	Juniper WLC WebAuth
Service Monitor Mode:	Disabled
Online Status:	 Online

Showing 3 of 1-100 records

Change StatusExportShow LogsClose

(/arubapedia/index.php/File:juniper-wlc-guest-cppm-7.jpg)

Request Details

Summary Input Output **RADIUS CoA** Accounting Alerts

CoA Action# 1

Date and Time	Oct 15, 2014 15:34:16 CDT
Application Name	Policy Manager
RADIUS CoA Action Type	CoA
RADIUS CoA Action Name	Juniper WLC WebAuth
Status Code	1
Status Message	Radius Juniper WLC WebAuth successful for client 00eebd5b9708
RADIUS CoA Attributes	Filter-Id = byod_acl.in Calling-Station-Id = 00-EE-BD-5B-97-08 Trpz-CoA-Replace-User = robbie@aruba.com NAS-IP-Address = 10.119.96.10 Framed-IP-Address = 10.119.124.27

Showing 4 of 1-100 records

Change Status Export Show Logs Close

(/arubapedia/index.php/File:juniper-wlc-guest-cppm-6.jpg)

Retrieved from "https://arubapedia.arubanetworks.com/arubapedia/index.php?title=ClearPass_Guest_on_Juniper_WLC&oldid=115754 (https://arubapedia.arubanetworks.com/arubapedia/index.php?title=ClearPass_Guest_on_Juniper_WLC&oldid=115754)"

Categories (/arubapedia/index.php/Special:Categories): Class3 (/arubapedia/index.php/Category:Class3)
ClearPass (/arubapedia/index.php/Category:ClearPass)

This page was last modified on 19 November 2014, at 15:01.

This page has been accessed 238 times.



(//www.mediawiki.org/)



(http://www.semantic-mediawiki.org/wiki/Semantic_MediaWiki)