

Network Configuration Example

Configuring Central Web Authentication
with EX Series Switches and Aruba
ClearPass

Published
2023-08-28

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Network Configuration Example Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass

Copyright © 2023 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide | iv

1

Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass

About This Network Configuration Example | 2

Use Case Overview | 2

Technical Overview | 3

Example: Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass | 5

Requirements | 5

Overview and Topology | 6

Configuration | 7

Verification | 28

Troubleshooting Central Web Authentication | 33

About This Guide

This network configuration example describes how you configure a Juniper Networks EX Series Ethernet Switch, Aruba ClearPass Guest, and Aruba ClearPass Policy Manager to work together to provide central Web authentication for guest endpoints that connect to EX Series switches.

1

CHAPTER

Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass

[About This Network Configuration Example](#) | 2

[Use Case Overview](#) | 2

[Technical Overview](#) | 3

[Example: Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass](#) | 5

[Troubleshooting Central Web Authentication](#) | 33

About This Network Configuration Example

This network configuration example describes how you configure a Juniper Networks EX Series Ethernet Switch, Aruba ClearPass Guest, and Aruba ClearPass Policy Manager to work together to provide central Web authentication for guest endpoints that connect to EX Series switches.

Use Case Overview

Enterprises often have visitors who need temporary access to the network or to the Internet, such as guests or contractors working on campus. It is common for these visitors to use the wired network for access. Enterprises that have access control enabled on switch ports can use central Web authentication (also known as captive portal authentication) to provide the necessary access to these temporary users. In central Web authentication, a user's web browser is redirected to a guest access web portal where the user can provide guest credentials. After the guest web portal authenticates the user, the user is granted limited access to the enterprise network.

Juniper Networks EX Series Ethernet Switches and the Aruba ClearPass Policy Manager platform work together to provide a secure guest access workflow using central Web authentication.

EX Series switches provide carrier-class reliability, security risk management, virtualization, application control, and lower total cost of ownership (TCO). Aruba ClearPass Policy Manager provides role-based and device-based network access control (NAC) for any user across any wired, wireless, and VPN infrastructure. In addition, it provides centralized guest access services that deliver consistent guest workflows and security policy for wired and wireless users. Enterprises with Aruba wireless infrastructure typically deploy Aruba ClearPass to provide NAC services for the wireless infrastructure. Enterprises that also deploy EX Series switches in these environments can leverage the extensive RADIUS capabilities on EX Series switches to integrate with Aruba ClearPass.

RELATED DOCUMENTATION

[Technical Overview | 3](#)

[Example: Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass | 5](#)

[Troubleshooting Central Web Authentication | 33](#)

Technical Overview

Web authentication uses a Web browser as a means for authenticating network users. When a user connects to the network and attempts to open a webpage, Web authentication redirects the webpage request to a login page that requires the user to enter a username and password or to agree to an acceptable use policy. Upon successful authentication, the user is allowed access to the network. Web authentication is useful for providing limited network access to temporary users, such as visitors to an enterprise, who try to access the network using devices that are not 802.1X-enabled. Web authentication can also be used as a fallback authentication method for regular network users who have 802.1X-enabled devices, but fail authentication because of other issues, such as expired network credentials.

Web authentication can be done locally on the switch, but this requires that the Web authentication login pages be configured on each switch used as a network access device. Central Web authentication (CWA) provides efficiency and scaling benefits by redirecting the client's Web browser to a central Web authentication server (CWA server), which handles the complete login process.

An example of a CWA server is Aruba ClearPass Guest. ClearPass Guest is a scalable, easy-to-use guest management solution that delivers secure, automated guest access workflows for enterprise wireless and wired networks and any type of mobile device. As a module within the ClearPass Policy Management platform, ClearPass Guest is fully integrated with the Aruba ClearPass core set of authentication, authorization, accounting, profiling of devices, reporting, and policy enforcement capabilities.

EX Series switches enable the central Web authentication workflow by providing the following features that are fully integrated with Aruba ClearPass Guest and Aruba ClearPass Policy Manager:

- Redirect URL support. EX Series switches can automatically redirect a user's browser to the CWA server login page. The redirect URL can be statically configured on the switch port or it can be dynamically configured on the switch port as part of the authentication process. EX Series switches support a Juniper Networks RADIUS vendor-specific attribute (VSA), Juniper-CWA-Redirect-URL, that enables Aruba ClearPass to pass the dynamic redirect URL to the switch.
- Dynamic firewall filters. EX Series switches provide a built-in firewall filter, JNPR_RSVD_FILTER_CWA. This filter is designed to be applied to guest endpoints before they go through Web authentication. It allows the guest endpoint to access DHCP, DNS, and other essential services required for central Web authentication, while blocking all other access. You can configure Aruba ClearPass to pass the name of this filter to the switch using the standard RADIUS Filter-ID attribute. If you use the JNPR_RSVD_FILTER_CWA filter, the redirect URL must contain the IP address of the CWA server, such as Aruba ClearPass Guest.

Alternatively, you can configure a firewall filter on Aruba ClearPass itself and use the Juniper Networks RADIUS VSA Juniper-Switching-Filter to pass the firewall filter to the switch. The firewall filter must allow traffic to the IP address of the Aruba ClearPass server.

- RADIUS change of authorization (CoA) support. This enables Aruba ClearPass to send a RADIUS CoA to the switch, which instructs the switch to change the dynamic firewall filter or VLAN in use after the endpoint passes central Web authentication.

Central Web authentication is a two-step process in which an endpoint first undergoes MAC RADIUS authentication and then Web authentication as follows:

1. MAC RADIUS authentication—This step allows the guest endpoint to receive an IP address and to access the CWA server while being blocked from most of the network.

By default, EX Series switches automatically attempt MAC RADIUS authentication after 802.1X authentication fails. To support CWA authentication, you must configure Aruba ClearPass to send an access-accept message to the switch if ClearPass is unable to authenticate the endpoint with MAC RADIUS authentication, along with a dynamic firewall filter that permits the endpoint to access required services for CWA authentication. You must also configure Aruba ClearPass to send the redirect URL to the switch, unless you configured the redirect URL locally on the switch.

2. Web authentication—This step allows the guest's credentials to be authenticated and appropriate network access to be granted to the guest.

After MAC RADIUS authentication, the switch automatically starts Web authentication, providing that it has been given a redirect URL and the appropriate firewall filter. When the user opens a Web browser, the switch redirects the Web browser to the Web authentication login page, where the user enters the guest credentials. To enable the guest to access appropriate network resources after successful authentication, you configure Aruba ClearPass to send a RADIUS CoA message that changes the firewall filter applied to the port.

RELATED DOCUMENTATION

[Example: Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass | 5](#)

[Troubleshooting Central Web Authentication | 33](#)

[Use Case Overview | 2](#)

Example: Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass

IN THIS SECTION

- Requirements | 5
- Overview and Topology | 6
- Configuration | 7
- Verification | 28

This configuration example illustrates how to use EX Series switches and Aruba ClearPass to implement central Web authentication of guest users. Specifically, it illustrates how to use the following EX Series switch features in conjunction with Aruba ClearPass:

- The built-in firewall filter `JNPR_RSVD_FILTER_CWA`, which allows a guest endpoint that has not yet been authenticated to access the services required for central Web authentication while blocking access to the rest of the network.
- The Juniper-CWA-Redirect-URL RADIUS VSA, which allows Aruba ClearPass to pass the redirect URL to the switch as part of the authentication process.
- RADIUS CoA support, which allows an EX Series switch to dynamically change the firewall filter in effect for a guest endpoint after the endpoint is authenticated.

This topic covers:

Requirements

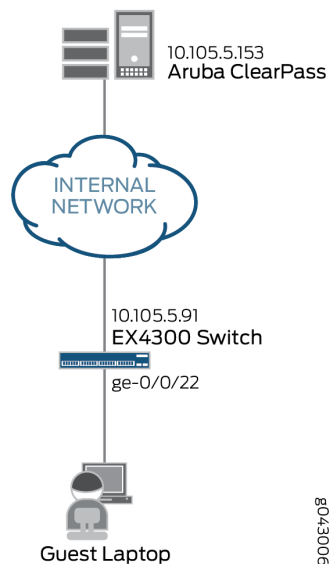
This example uses the following hardware and software components for the policy infrastructure:

- An EX4300 switch running Junos OS Release 15.1R3 or later
- An Aruba ClearPass Policy Manager platform running 6.3.3.63748 or later

Overview and Topology

This network configuration example uses the topology shown in [Figure 1 on page 6](#). A guest laptop connects to port ge-0/0/22 of an EX4300 switch. The Aruba ClearPass server provides both ClearPass Guest and ClearPass Policy Management services.

Figure 1: Topology Used in This Example



Both 802.1X and MAC RADIUS authentication are enabled on port ge-0/0/22. Because the guest laptop does not have a 802.1X client, the switch does not receive any EAPoL packets from the laptop and 802.1X authentication fails. The EX4300 switch automatically tries MAC RADIUS authentication next. A MAC RADIUS enforcement policy in Aruba ClearPass is configured to send a RADIUS access-accept message for unknown clients attempting MAC RADIUS authentication, along with the name of the JNPR_RSVD_FILTER_CWA built-in filter and the redirect URL for the Aruba ClearPass Guest login page.

When the guest user opens a browser and attempts to access a webpage, the EX4300 switch redirects the browser to the Aruba ClearPass Guest login page, where the guest enters the guest credentials. A Web authentication enforcement policy in Aruba ClearPass is configured to add the guest endpoint to the endpoint repository and to send a RADIUS CoA message to the switch. This message tells the switch to change the firewall filter associated with the endpoint to guest_access_policy_1, which is configured on the switch. This filter permits the guest to access everything except the internal network.

Configuration

IN THIS SECTION

- [Configuring the EX4300 Switch | 7](#)
- [Configuring Aruba ClearPass Guest | 12](#)
- [Configuring Aruba ClearPass Policy Manager | 16](#)

This section provides step-by-step instructions for:

Configuring the EX4300 Switch

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter commit from configuration mode.

```
[edit]
set access radius-server 10.105.5.153 dynamic-request-port 3799
set access radius-server 10.105.5.153 secret password
set access radius-server 10.105.5.153 source-address 10.105.5.91
set access profile CP-Test-Profile accounting-order radius
set access profile CP-Test-Profile authentication-order radius
set access profile CP-Test-Profile radius authentication-server 10.105.5.153
set access profile CP-Test-Profile radius accounting-server 10.105.5.153
set access profile CP-Test-Profile radius options nas-identifier 10.105.5.91
set system services web-management http
set system services web-management https system-generated-certificate
set protocols dot1x authenticator authentication-profile-name CP-Test-Profile
set protocols dot1x authenticator interface ge-0/0/22.0 mac-radius
set protocols dot1x authenticator interface ge-0/0/22.0 supplicant multiple
set vlans v100 description "Quarantine VLAN"
set vlans v100 vlan-id 100
set interfaces ge-0/0/22 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/22 unit 0 family ethernet-switching vlan members v100
set firewall family ethernet-switching filter guest_access_policy_1 term Block_Internal from ip-
```

```

destination-address 192.168.0.0/16
set firewall family ethernet-switching filter guest_access_policy_1 term Block_Internal then
discard
set firewall family ethernet-switching filter guest_access_policy_1 term Allow_All then accept

```

Step-by-Step Procedure

The general steps to configure the EX4300 switch are:

- Configure the connection to the Aruba ClearPass Policy Manager.
- Create the access profile used by the 802.1X protocol. The access profile tells the 802.1X protocol which authentication server to use and the authentication methods and order.
- Enable HTTP and HTTPS services.
- Configure the 802.1X protocol.
- Configure the VLAN used by the guest endpoints.
- Configure Ethernet switching on the access port.
- Create the firewall policy that blocks access to the internal network.

To configure the EX4300 switch:

1. Provide the RADIUS server connection information.

```

[edit access]
user@EX4300# set radius-server 10.105.5.153 dynamic-request-port 3799
user@EX4300# set radius-server 10.105.5.153 secret password
user@EX4300# set radius-server 10.105.5.153 source-address 10.105.5.91

```

2. Configure the access profile.

```

[edit access]
user@EX4300# set profile CP-Test-Profile accounting-order radius
user@EX4300# set profile CP-Test-Profile authentication-order radius
user@EX4300# set profile CP-Test-Profile radius authentication-server 10.105.5.153
user@EX4300# set profile CP-Test-Profile radius accounting-server 10.105.5.153
user@EX4300# set profile CP-Test-Profile radius options nas-identifier 10.105.5.91

```

3. Enable HTTP and HTTPS services. These services must be enabled for URL redirection.

```
[edit system services]
user@EX4300# set system services web-management http
user@EX4300# set system services web-management https system-generated-certificate
```

4. Configure the 802.1X protocol to use CP-Test-Profile, and enable the protocol on each access interface. In addition, configure the interfaces to support MAC RADIUS authentication and to allow more than one supplicant, each of which must be individually authenticated.

By default, the switch will first attempt 802.1X authentication. If it receives no EAP packets from the endpoint, indicating that the endpoint does not have an 802.1X supplicant, or if the 802.1X authentication fails, it then tries MAC RADIUS authentication.

```
[edit protocols]
user@EX4300# set dot1x authenticator authentication-profile-name CP-Test-Profile
user@EX4300# set dot1x authenticator interface ge-0/0/22.0 mac-radius
user@EX4300# set dot1x authenticator interface ge-0/0/22.0 supplicant multiple
```

5. Configure the VLAN used in this example.

```
[edit vlans]
user@EX4300# set v100 description "Quarantine VLAN"
user@EX4300# set v100 vlan-id 100
```

6. Configure the access port.

The access port is configured to be in VLAN v100, the quarantine VLAN. This VLAN will be used by the endpoint if Aruba ClearPass does not send dynamic VLAN information when it authenticates the endpoint.

```
[edit interfaces]
user@EX4300# set ge-0/0/22 unit 0 family ethernet-switching interface-mode access
user@EX4300# set ge-0/0/22 unit 0 family ethernet-switching vlan members v100
```

7. Configure a firewall filter, `guest_access_policy_1`, to be used for the endpoint after the guest credentials have been authenticated by Aruba ClearPass Guest.

This filter blocks the endpoint from accessing the internal network (192.168.0.0/16), while permitting access to the Internet.

```
[edit firewall]
user@EX4300# set family ethernet-switching filter guest_access_policy_1 term Block_Internal
from ip-destination-address 192.168.0.0/16
user@EX4300# set family ethernet-switching filter guest_access_policy_1 term Block_Internal
then discard
user@EX4300# set family ethernet-switching filter guest_access_policy_1 term Allow_All then
accept
```

Results

From configuration mode, confirm your configuration by entering the following `show` commands.

```
user@EX4300# show access
radius-server {
  10.105.5.153 {
    dynamic-request-port 3799;
    secret "$9$FYxf3A0Ehrv87y17Vs4DjftZ3Ct0BIcre"; ## SECRET-DATA
    source-address 10.105.5.91;
  }
}
profile CP-Test-Profile {
  accounting-order radius;
  authentication-order radius;
  radius {
    authentication-server 10.105.5.153;
    accounting-server 10.105.5.153;
    options {
      nas-identifier 10.105.5.91;
    }
  }
}
```

```
user@EX4300# show system services
web-management {
  http;
```

```
https {
  system-generated-certificate;
}
}
```

```
user@EX4300# show protocols
dot1x {
  authenticator {
    authentication-profile-name CP-Test-Profile;
    interface {
      ge-0/0/22.0 {
        supplicant multiple;
        mac-radius;
      }
    }
  }
}
```

```
user@EX4300# show interfaces
ge-0/0/22 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members v100;
      }
    }
  }
}
```

```
user@EX4300# show vlans
v100 {
  description "Quarantine VLAN";
  vlan-id 100;
```

```
}
}
```

```
user@EX4300# show firewall
family ethernet-switching {
  filter guest_access_policy_1 {
    term Block_Internal {
      from {
        ip-destination-address {
          192.168.0.0/16;
        }
      }
      then discard;
    }
    term Allow_All {
      then accept;
    }
  }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Configuring Aruba ClearPass Guest

Step-by-Step Procedure

The general steps for configuring Aruba ClearPass Guest are:

- Set up the guest user account.
- Configure the guest login page.

To configure Aruba ClearPass Guest:

1. Log in to ClearPass Guest. For example:

```
https://10.105.5.153/guest/
```

2. Set up the guest user account.

Step-by-Step Procedure

- a. Click **Create New Guest Account**.

- b. Provide the details for the guest user account, as shown below. Be sure to note the password, which is automatically generated.

New Guest Account	
* Guest's Name:	guest2 <small>Name of the guest.</small>
* Company Name:	guestcompany <small>Company name of the guest.</small>
* Email Address:	guest2@guestcompany.com <small>The guest's email address. This will become their username to log into the network.</small>
Account Activation:	Now <small>Select an option for changing the activation time of this account.</small>
Account Expiration:	30 days from now <small>Select an option for changing the expiration time of this account.</small>
* Account Role:	[Guest] <small>Role to assign to this account.</small>
Password:	25938257
* Terms of Use:	<input checked="" type="checkbox"/> I am the sponsor of this account and accept the terms of use
Notes:	<input type="text"/>
<input type="button" value="Create Account"/>	

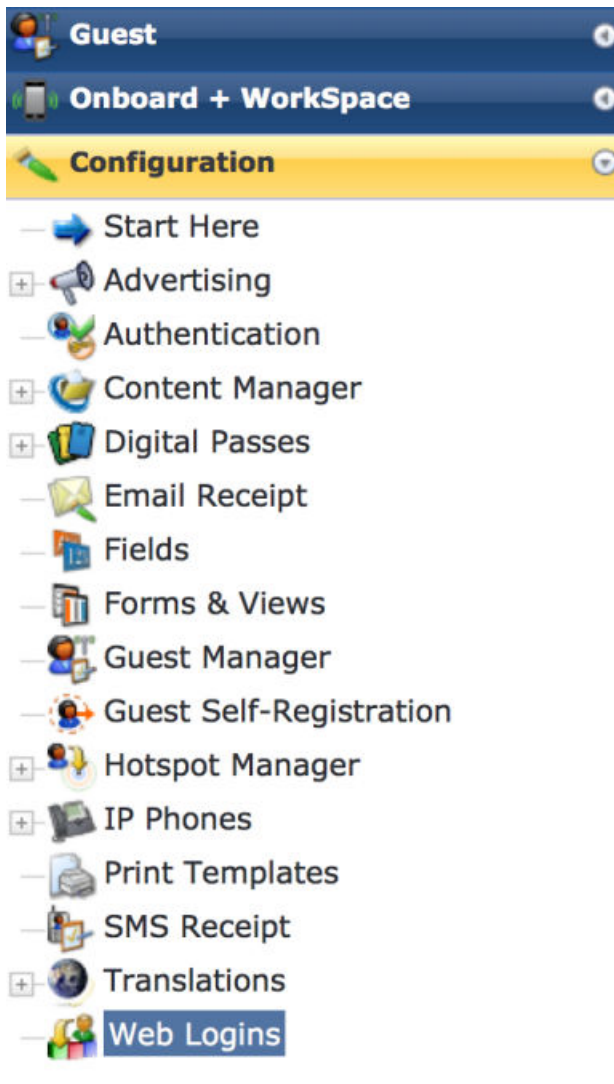
- c. Click **Create Account**.

3. Configure the guest access login page.

Step-by-Step Procedure

- a. Select **Configuration > Web Logins**.

NOTE: If you are using a recent version of Aruba ClearPass Guest, you might need to select **Configuration > Pages > Web Logins**.



- b. In the **Web Logins** page, click **Create a new web login page**.

- c. In the Web Login Editor, provide a name for Web login page you are creating, specify the login page name as it appears in the URL, and set Login Method to **Server-Initiated – Change of authorization (RFC 3576) sent to controller**.

Web Login (new)

Use this form to create a new Web Login.

Web Login Editor	
* Name:	<input type="text" value="Guest Access"/> <small>Enter a name for this web login page.</small>
Page Name:	<input type="text" value="guest-access"/> <small>Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".</small>
Description:	<div style="border: 1px solid #ccc; height: 30px;"></div> <small>Comments or descriptive text about the web login.</small>
* Vendor Settings:	<input type="text" value="Aruba Networks"/> <small>Select a predefined group of settings suitable for standard network configurations.</small>
Login Method:	<input type="text" value="Server-initiated – Change of authorization (RFC 3576) sent to controller"/> <small>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.</small>
Security Hash:	<input type="text" value="Do not check – login will always be permitted"/> <small>Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.</small>

- d. In the Login Form section of the Web Login page, set **Pre-Auth Check** to **None – no extra checks will be made**.

Login Form

Options for specifying the behaviour and content of the login form.

Authentication:	<input type="text" value="Credentials – Require a username and password"/> <small>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.</small>
Prevent CNA:	<input type="checkbox"/> Enable bypassing the Apple Captive Network Assistant <small>The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.</small>
Custom Form:	<input type="checkbox"/> Provide a custom login form <small>If selected, you must supply your own HTML login form in the Header or Footer HTML areas.</small>
Custom Labels:	<input type="checkbox"/> Override the default labels and error messages <small>If selected, you will be able to alter labels and error messages for the current login form.</small>
* Pre-Auth Check:	<input type="text" value="None – no extra checks will be made"/> <small>None – no extra checks will be made before proceeding to the NAS authentication. App Auth – check using Aruba Application Authentication Local – match a local account RADIUS – check using a RADIUS request Single Sign-On – enable SSO for this web login</small>
Terms:	<small>conditions checkbox.</small>

- e. In the Default Destination section, enter a default URL to which the guest gets redirected after successful authentication. In this example, the guest is redirected to the Juniper Networks home page after authentication.

Default Destination	
Options for controlling the destination clients will redirect to after login.	
* Default URL:	<input type="text" value="http://www.juniper.net"/> Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	<input checked="" type="checkbox"/> Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.

Configuring Aruba ClearPass Policy Manager

Step-by-Step Procedure

The general steps for configuring Aruba ClearPass are:

- Modify the Juniper Networks RADIUS dictionary file so that it includes new Juniper Networks RADIUS attributes.
- Add the EX4300 as a network device.
- Create the following enforcement profiles:
 - A profile that is enforced after MAC RADIUS authentication.
 - A profile that is enforced after central Web authentication.
- Create two enforcement policies:
 - A policy that is invoked when MAC RADIUS authentication is used.
 - A policy that is invoked when central Web authentication is used.
- Define the MAC RADIUS authentication service and the Web authentication service.

To configure Aruba ClearPass:

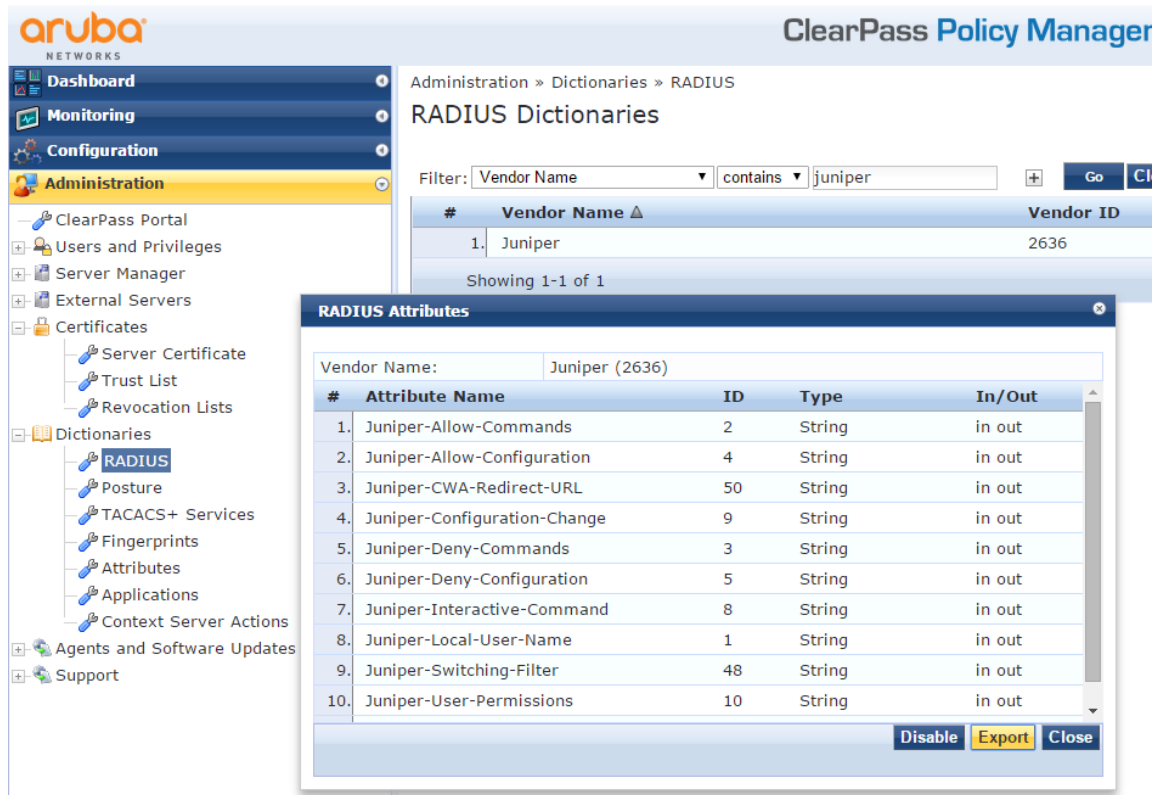
1. Update the Juniper Networks RADIUS dictionary file.

A Juniper Network RADIUS dictionary file comes preinstalled on Aruba ClearPass. Junos OS Release 15.1R3 for EX Series switches adds support for three new Juniper Networks VSAs, which need to be added to the dictionary file.

Step-by-Step Procedure

- a. In Aruba ClearPass, navigate to Administration > Dictionaries > RADIUS.
- b. In the RADIUS Dictionaries window, use the Filter field to search for **Juniper** under Vendor Name.

- c. Click the Juniper dictionary name, and then click **Export** to save the **RadiusDictionary.xml** file to your desktop.



The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, and Administration. The Administration menu is expanded, showing options like ClearPass Portal, Users and Privileges, Server Manager, External Servers, Certificates, Dictionaries, and Agents and Software Updates. The main content area displays 'Administration » Dictionaries » RADIUS' and 'RADIUS Dictionaries'. A filter is set to 'Vendor Name contains juniper'. A table shows one entry: '1. Juniper' with 'Vendor ID 2636'. The 'RADIUS Attributes' dialog box is open, showing 'Vendor Name: Juniper (2636)' and a table of attributes.

#	Attribute Name	ID	Type	In/Out
1.	Juniper-Allow-Commands	2	String	in out
2.	Juniper-Allow-Configuration	4	String	in out
3.	Juniper-CWA-Redirect-URL	50	String	in out
4.	Juniper-Configuration-Change	9	String	in out
5.	Juniper-Deny-Commands	3	String	in out
6.	Juniper-Deny-Configuration	5	String	in out
7.	Juniper-Interactive-Command	8	String	in out
8.	Juniper-Local-User-Name	1	String	in out
9.	Juniper-Switching-Filter	48	String	in out
10.	Juniper-User-Permissions	10	String	in out

- d. Copy the following three attributes, paste them into **RadiusDictionary.xml**, and save the file.

```
<Attribute profile="in out" type="String" name="Juniper-CWA-Redirect-URL" id="50" />
<Attribute profile="in out" type="String" name="Juniper-Switching-Filter" id="48" />
<Attribute profile="in out" type="String" name="Juniper-VoIP-Vlan" id="49" />
```

The dictionary file should look like this when you complete the paste:

```

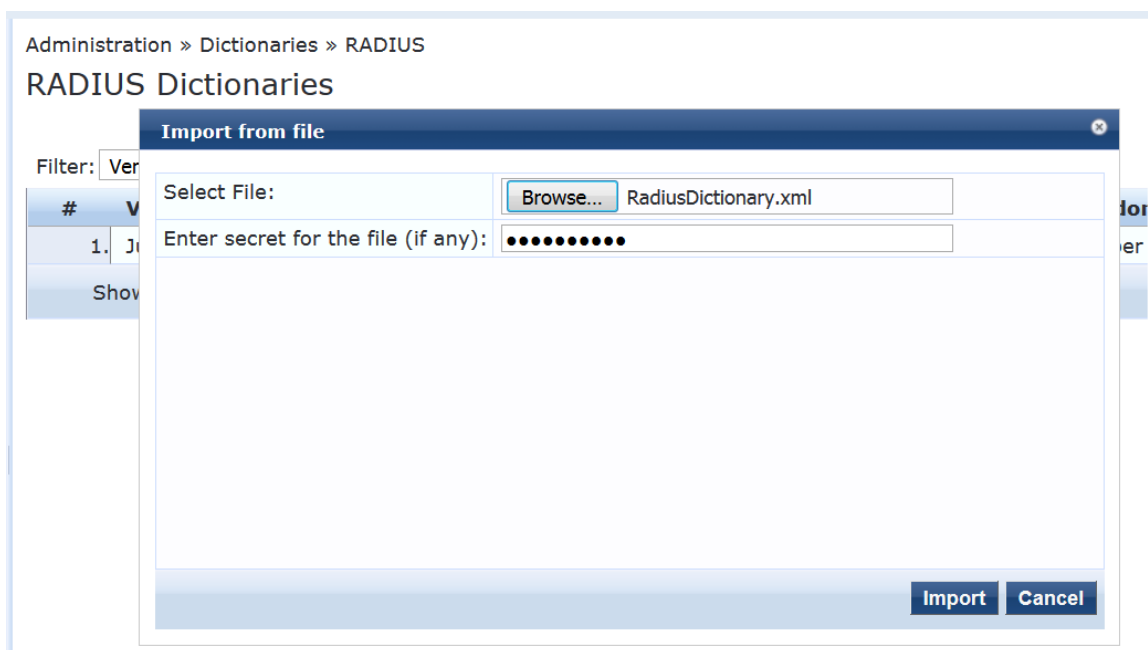
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
  <TipsHeader exportTime="Tue Feb 09 15:30:18 PST 2016" version="6.3"/>
  <Dictionaries>
    <Vendor vendorEnabled="true" prefix="Juniper" name="Radius:Juniper" id="2636">
      <RadiusAttributes>
        <Attribute profile="in out" type="String" name="Juniper-Allow-Commands" id="2"/>
        <Attribute profile="in out" type="String" name="Juniper-Allow-Configuration" id="4"/>
        <Attribute profile="in out" type="String" name="Juniper-Configuration-Change" id="9"/>
        <Attribute profile="in out" type="String" name="Juniper-Deny-Commands" id="3"/>
        <Attribute profile="in out" type="String" name="Juniper-Deny-Configuration" id="5"/>
        <Attribute profile="in out" type="String" name="Juniper-Interactive-Command" id="8"/>
        <Attribute profile="in out" type="String" name="Juniper-Local-User-Name" id="1"/>
        <Attribute profile="in out" type="String" name="Juniper-User-Permissions" id="10"/>
        <Attribute profile="in out" type="String" name="Juniper-CWA-Redirect-URL" id="50" />
        <Attribute profile="in out" type="String" name="Juniper-Switching-Filter" id="48" />
        <Attribute profile="in out" type="String" name="Juniper-VoIP-Vlan" id="49" />
      </RadiusAttributes>
    </Vendor>
  </Dictionaries>
</TipsContents>

```

- e. Import the dictionary file into Aruba ClearPass by clicking



in the RADIUS Dictionaries window and browsing to the file.



- f. After you have imported the file, the Juniper dictionary file should look like this:

Administration » Dictionaries » RADIUS

RADIUS Dictionaries

RADIUS Attributes

Filter

Vendor Name: Juniper (2636) refix

1.	Juniper-Allow-Commands	2	String	in out
2.	Juniper-Allow-Configuration	4	String	in out
3.	Juniper-CWA-Redirect-URL	50	String	in out
4.	Juniper-Configuration-Change	9	String	in out
5.	Juniper-Deny-Commands	3	String	in out
6.	Juniper-Deny-Configuration	5	String	in out
7.	Juniper-Interactive-Command	8	String	in out
8.	Juniper-Local-User-Name	1	String	in out
9.	Juniper-Switching-Filter	48	String	in out
10.	Juniper-User-Permissions	10	String	in out
11.	Juniper-VoIP-Vlan	49	String	in out

Disable
Export
Close


2. Add the EX4300 switch as a network device.

Step-by-Step Procedure

- a. Under Configuration > Network > Devices, click **Add**.

Configuration » Network » Devices

Network Devices



- b. On the Device tab, enter the hostname and IP address of the switch and the RADIUS shared secret that you configured on the switch. Set the Vendor Name field to **Juniper**.

Add Device
✕

Device
SNMP Read Settings
SNMP Write Settings
CLI Settings

Name:	<input type="text" value="Policy-EX4300-01"/>		
IP or Subnet Address:	<input type="text" value="10.105.5.91"/>	(e.g., 192.168.1.10 or 192.168.1.1/24)	
Description:	<input style="height: 20px;" type="text"/>		
RADIUS Shared Secret:	<input type="password" value="....."/>	Verify:	<input type="password" value="....."/>
TACACS+ Shared Secret:	<input type="text"/>	Verify:	<input type="text"/>
Vendor Name:	<input type="text" value="Juniper"/>		
Enable RADIUS CoA:	<input checked="" type="checkbox"/>	RADIUS CoA Port:	<input type="text" value="3799"/>

Attributes
✕

	Attribute	Value	✕
1.	Click to add...		

Add
Cancel

3. Create the enforcement profile to be used for MAC RADIUS authentication.

This profile provides the switch with the name of the built-in firewall filter JNPR_RSVD_FILTER_CWA and the redirect URL for Aruba ClearPass Guest.

Step-by-Step Procedure

- a. Under Configuration > Enforcement > Profiles, click **Add**.
- b. On the Profile tab, set Template to **RADIUS Based Enforcement** and type the profile name, **Guest_Access_Portal_Enforcement**, in the Name field.

Enforcement Profiles

Profile	Attributes	Summary
Template:	RADIUS Based Enforcement	
Name:	Guest_Access_Portal_Enforcement	
Description:		
Type:	RADIUS	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	<input type="text"/> --Select--	<input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/>

c. On the Attributes tab, configure the following attributes:

- **Juniper-CWA-Redirect-URL**—Type the following URL:

```
http://10.105.5.153/guest/guest-access.php?&mac=%{Radius:IETF:Calling-Station-Id}
```

This URL must contain the IP address of the Aruba ClearPass Guest server. It also passes the MAC address of the endpoint to ClearPass Guest (Radius:IETF:Calling-Station-Id).

- **Filter-Id**—Type the following filter name:

```
JNPR_RSVD_FILTER_CWA
```

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Type	Name	Value
1. Radius:Juniper	Juniper-CWA-Redirect-URL	= http://10.105.5.153/guest/guest-access.php?&mac=%{Radius:IETF:Calling-Station-Id}
2. Radius:IETF	Filter-Id	= JNPR_RSVD_FILTER_CWA
3. Click to add...		

4. Configure an enforcement profile to be used for central Web authentication.

This profile is configured as a RADIUS Change of Authorization (CoA) profile. It tells Aruba ClearPass to send a RADIUS CoA to the switch, informing it to change the firewall filter in effect for the endpoint from JNPR_RSVD_FILTER_CWA to guest_access_policy_1.

Step-by-Step Procedure

- a. Under Configuration > Enforcement > Profiles, click **Add**.
- b. On the Profile tab, set Template to **RADIUS Change of Authorization (CoA)** and type the profile name, **Guest_Access_CoA_Profile**, in the Name field.

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Template:	RADIUS Change of Authorization (CoA)	
Name:	Guest_Access_CoA_Profile	
Description:		
Type:	RADIUS_CoA	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	<input type="text"/> <input type="text"/>	<input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/>
	--Select--	

- c. On the Attributes tab, set **Select RADIUS CoA Template** to **IETF - Generic-CoA-IETF** and enter the attributes as shown. All values must be typed in or copied and pasted from this document. The values do not appear in the selection lists.

```

%{Radius:IETF:Calling-Station-Id}
%{Radius:IETF:User-Name}
guest_access_policy_1
  
```

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Select RADIUS CoA Template:	IETF - Generic-CoA-IETF	
Type	Name	Value
1. Radius:IETF	Calling-Station-Id	= %{Radius:IETF:Calling-Station-Id}
2. Radius:IETF	User-Name	= %{Radius:IETF:User-Name}
3. Radius:IETF	Filter-Id	= guest_access_policy_1
4. Click to add...		

5. Configure the MAC RADIUS authentication enforcement policy.

The MAC RADIUS policy tells Aruba ClearPass to apply the **Guest_Access_Portal_Enforcement** profile to all endpoints undergoing MAC RADIUS authentication that are not already known to ClearPass—that is, are not in the endpoint repository.

Step-by-Step Procedure

- a. Under Configuration > Enforcement > Policies, click **Add**.
- b. On the Enforcement tab, type the name of policy (**Juniper-MAC-Auth-Policy**) and set the Default Profile to the predefined profile [**Deny Access Profile**].

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement	Rules	Summary
Name:	Juniper-MAC-Auth-Policy	
Description:		
Enforcement Type:	<input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS+ <input type="radio"/> WEBAUTH (SNMP/Agent/CLI/CoA) <input type="radio"/> Application	
Default Profile:	[Deny Access Profile]	View Details Modify

- c. On the Rules tab, click **Add Rule** and add the rule shown.

This rule permits the Guest_Access_Portal_Enforcement profile to take effect for endpoints that are not known to Aruba ClearPass.

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Authentication	MacAuth	EQUALS	UnknownClient
2. Click to add...			

Enforcement Profiles

Profile Names:

[RADIUS] Guest_Access_Portal_Enforcement

[Move Up](#)
[Move Down](#)
[Remove](#)

--Select to Add--

6. Configure the Web authentication enforcement policy.

This policy takes effect after the guest is redirected to the Aruba ClearPass Guest and ClearPass Guest authenticates the guest. It tells Aruba ClearPass to add the endpoint to the endpoint repository and to apply the Guest_Access_CoA_Profile.

Step-by-Step Procedure

- a. Under Configuration > Enforcement > Policies, click **Add**.
- b. On the Enforcement tab, type the name of the policy (**Guest_Auth_Enforcement_Policy**) and set Default Profile to **[Post Authentication][Update Endpoint Known]**. This is a predefined profile that results in the endpoint being added as a known endpoint in the endpoint repository.

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement	Rules	Summary
Name:	<input type="text" value="Guest_Auth_Enforcement_Policy"/>	
Description:	<input type="text"/>	
Enforcement Type:	<input type="radio"/> RADIUS <input type="radio"/> TACACS+ <input checked="" type="radio"/> WEBAUTH (SNMP/Agent/CLI/CoA) <input type="radio"/> Application	
Default Profile:	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> --Select to Add-- View Details Modify </div> <ul style="list-style-type: none"> --Select to Add-- [Agent] Agent bounce [Agent] Juniper-wireless Aruba 802.1X Wireless No-Action Agent Enforcement [HTTP] [Handle AirGroup Time Sharing] [Post Authentication] [Update Endpoint Known] [Post Authentication] juniper Guest Bandwidth Limit [Post Authentication] juniper Guest Do Expire [Post Authentication] juniper Guest Expire Post Login [Post Authentication] juniper Guest MAC Caching [Post Authentication] juniper Guest Session Limit [RADIUS_CoA] Guest_Access_Profile [RADIUS_CoA] Juniper-wireless Aruba 802.1X Wireless Quarantined Client Aruba Role Enforcement [RADIUS_CoA] [Aerohive - Terminate Session] [RADIUS_CoA] [Aruba Terminate Session] [RADIUS_CoA] [Cisco - Bounce-Host-Port] [RADIUS_CoA] [Cisco - Disable Host-Port] [RADIUS_CoA] [Cisco - Reauthenticate-Session] [RADIUS_CoA] [Cisco - Terminate Session] [RADIUS_CoA] [HP - Terminate Session] [RADIUS_CoA] [Juniper Terminate Session] </div>	

- c. On the Rules tab, click **Add Rule** and add the rule shown.

This rule tells Aruba ClearPass to apply the Guest_Access_CoA_Profile enforcement profile to any endpoint that ClearPass Guest has assigned to role Guest.

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Tips	Role	EQUALS	[Guest]
2. Click to add...			

Enforcement Profiles

Profile Names:

[RADIUS_CoA] Guest Access CoA Profile

Move Up

Move Down

Remove

--Select to Add--

7. Configure the MAC RADIUS authentication service.

The configuration for this service results in MAC RADIUS authentication being performed when the RADIUS User-Name attribute and the Client-MAC-Address attribute received have the same value.

Step-by-Step Procedure

- a. Under Configuration > Services, click **Add**.
- b. On the Services tab, fill out the fields as shown.

Configuration » Services » Edit - JUNOS MAC AUTH

Services - JUNOS MAC AUTH

Summary Service Authentication Roles Enforcement

Name: JUNOS MAC AUTH

Description:

Type: MAC Authentication

Status: Enabled

Monitor Mode: Enable to monitor network access without enforcement

More Options: Authorization Audit End-hosts Profile Endpoints Accounting Proxy

Service Rule

Matches ANY or ALL of the following conditions:

Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS %{Radius:IETF:User-Name}

- c. On the Authentication tab:
 - Delete [MAC AUTH] from the Authentication Methods list and add [EAP MD5] to the list.
 - Select [Endpoints Repository] [Local SQL DB] in the Authentication Sources list.

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary
Authentication Methods:	[EAP MD5]			
Authentication Sources:	[Endpoints Repository] [Local SQL DB]			
Strip Username Rules:	<input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes			

- d. On the Enforcement tab, select **Juniper-MAC-Auth-Policy**.

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	[Sample Allow Access Policy]			Modify
Enforcement Policy Details	<ul style="list-style-type: none"> [AirGroup Enforcement Policy] Juniper_Dot1X_Policy Juniper-MAC-Auth-Policy Juniper-wired 802.1X Wired Enforcement Policy [Sample Allow Access Policy] [Sample Deny Access Policy] 			
Description:				
Default Profile:				
Rules Evaluation Algorithm:	evaluate-all			
Conditions			Enforcement Profil	
1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)			[Allow Access Profile]	

8. Configure the Web-based authentication service.

Step-by-Step Procedure

- a. Under Configuration > Services, click **Add**.
- b. On the Service tab, fill out the fields as shown.

The service rule is the default service rule when you select **Web-based Authentication**. It allows Web-based authentication requests from any client.

Configuration » Services » Add

Services

Service Authentication Roles Enforcement Summary

Type: Web-based Authentication

Name: Guest_WebAuth_Service

Description:

Monitor Mode: Enable to monitor network access without enforcement

More Options: Authorization Posture Compliance

Service Rule

Matches ANY or ALL of the following conditions:

Type	Name	Operator	Value
1. Host	CheckType	MATCHES_ANY	Authentication
2. Click to add...			

- c. On the Authentication tab, set Authentication Sources to **[Guest User Repository][Local SQL DB]**.

Configuration » Services » Add

Services

Service Authentication Roles Enforcement Summary

Authentication Sources:

[Guest User Repository] [Local SQL DB]	Move Up Move Down Remove View Details Modify
--	--

- d. On the Enforcement tab, set Enforcement Policy to **Guest_Auth_Enforcement_Policy**.

Configuration » Services » Add

Services

Service Authentication Roles Enforcement Summary

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

Enforcement Policy: Guest_Auth_Enforcement_Policy [Modify](#)

Enforcement Policy Details

Description:

Default Profile: [Update Endpoint Known]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Tips:Role EQUALS [Guest])	Guest_Access_Profile

Verification

IN THIS SECTION

- [Verifying Central Web Authentication | 28](#)
- [Verifying Status of Authentication Requests on Aruba ClearPass Policy Manager | 31](#)

Confirm that the configuration is working properly.

Verifying Central Web Authentication

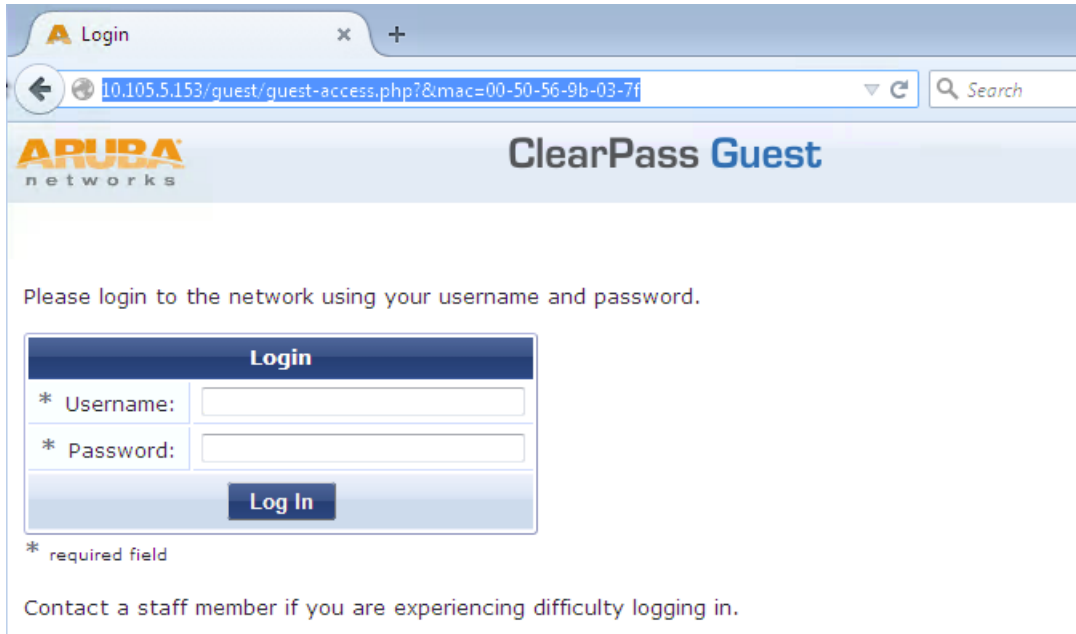
Purpose

Verify that the guest user's browser is redirected to Aruba ClearPass Guest for authentication and that the guest is successfully authenticated after entering the guest credentials.

Action

1. Connect a laptop to port ge-0/0/22 on the EX4300 switch.
2. Open a Web browser on the laptop and attempt to access a webpage.

The ClearPass Guest login page should appear as shown.



ARUBA
networks

ClearPass Guest

Please login to the network using your username and password.

Login

* Username:

* Password:

Log In

* required field

Contact a staff member if you are experiencing difficulty logging in.

- On the EX Series switch, enter the following show command:

```

user@EX4300> show dot1x interface ge-0/0/22 detail
ge-0/0/22.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Mac Radius Authentication Protocol: EAP-MD5
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: not configured
  Number of connected supplicants: 1
    Supplicant: 0050569b037f, 00:50:56:9B:03:7F
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: CWA Authentication
      Authenticated VLAN: v100
  
```

Dynamic Filter: JNPR_RSVD_FILTER_CWA

Session Reauth interval: 3600 seconds

Reauthentication due in 3566 seconds

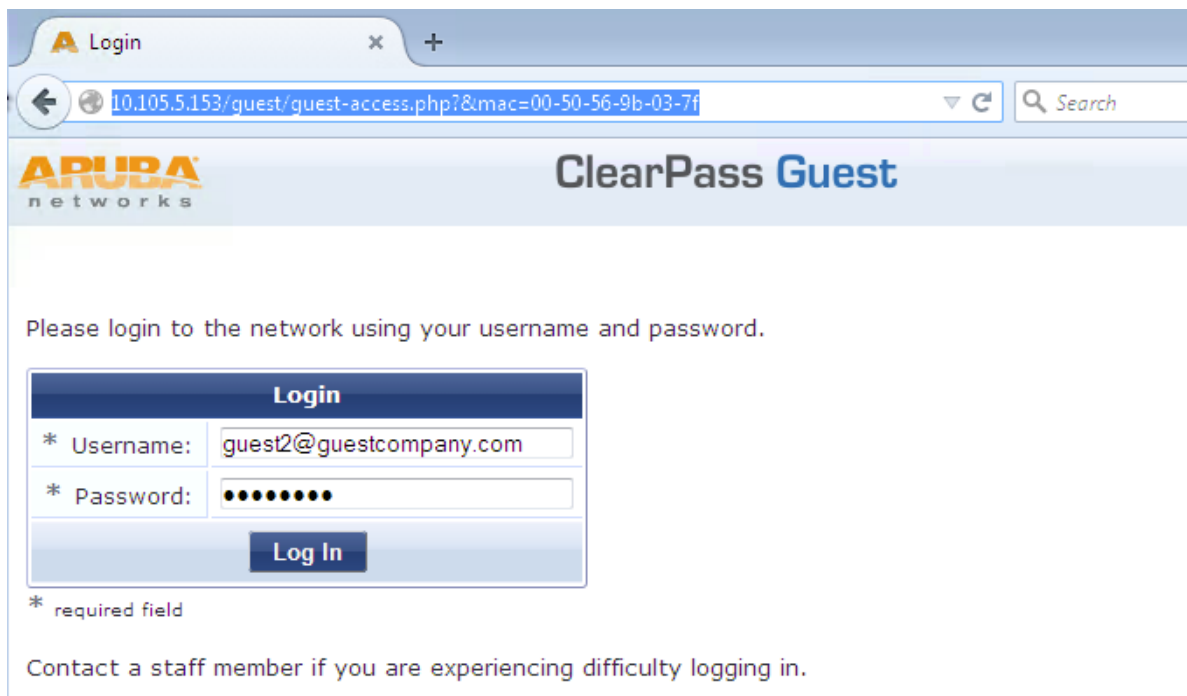
Session Accounting Interim Interval: 600 seconds

Accounting Update due in 566 seconds

CWA Redirect URL : http://10.105.5.153/guest/guest-access.php?&mac=00-50-56-9b-03-7f

The output shows that the endpoint has been authenticated, that the authentication method currently in effect is central Web authentication (CWA Authentication), and that the JNPR_RSVD_FILTER_CWA firewall filter and the redirect URL are also in effect.

4. In the ClearPass Guest login page, enter the guest e-mail address and the automatically generated password that you noted when you configured Aruba ClearPass Guest.



5. After you log in, your browser should be redirected to the Juniper Networks home page, as configured in Aruba ClearPass Guest.
6. On the EX Series switch, enter the following show command:

```
user@EX4300> show dot1x interface ge-0/0/22 detail
ge-0/0/22.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
```

```

Number of retries: 3
Quiet period: 60 seconds
Transmit period: 30 seconds
Mac Radius: Enabled
Mac Radius Restrict: Disabled
Mac Radius Authentication Protocol: EAP-MD5
Reauthentication: Enabled
Configured Reauthentication interval: 3600 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 2
Guest VLAN member: not configured
Number of connected supplicants: 1
  Supplicant: 0050569b037f, 00:50:56:9B:03:7F
    Operational state: Authenticated
    Backend Authentication state: Idle
    Authentication method: Mac Radius
    Authenticated VLAN: v100
    Dynamic Filter: guest_access_policy_1
    Session Reauth interval: 3600 seconds
    Reauthentication due in 3434 seconds
    Session Accounting Interim Interval: 600 seconds
    Accounting Update due in 434 seconds

```

The output shows that the `guest_access_policy_1` firewall filter is now in effect. The switch received the RADIUS CoA from Aruba ClearPass after the endpoint was authenticated by central Web authentication, telling it which firewall filter to use.

Verifying Status of Authentication Requests on Aruba ClearPass Policy Manager

Purpose

Verify that the endpoints are being correctly authenticated and that the correct RADIUS attributes are being exchanged between the switch and Aruba ClearPass.

Action

1. Go to Monitoring > Live Monitoring > Access Tracker to display the status of the authentication requests.

The Access Tracker monitors authentication requests as they occur and reports on their status.

Monitoring » Live Monitoring » Access Tracker

Access Tracker Feb 01, 2016 18:59:49 PST Auto Refresh

[All Requests] cp-campus.englab.juniper.net (10.105.5.153) Last 1 day before Today Edit

Filter: Request ID contains Go Clear Filter Show 10 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	10.105.5.153	WEBAUTH	guest2@guestcompany.	Guest_WebAuth_Servic	ACCEPT	2016/02/01 18:57:36
2.	10.105.5.153	RADIUS	0050569b037f	Juniper_MAC_Auth_Ser	ACCEPT	2016/02/01 18:55:01
3.	10.105.5.153	RADIUS	4067a550a344	Juniper_MAC_Auth_Ser	ACCEPT	2016/02/01 18:54:50

- To get more details on the initial MAC RADIUS authentication request from the endpoint, click the request (line 2 of Access Tracker request table).

Request Details

Summary **Input** **Output** **Accounting** **RADIUS CoA**

Session Identifier: R00002db6-01-56b01a85

Date and Time: Feb 01, 2016 18:55:01 PST

End-Host Identifier: 00-50-56-9b-03-7f

Username: 0050569b037f

Access Device IP/Port: 10.105.5.91:555

System Posture Status: UNKNOWN (100)

Policies Used -

Service: Juniper_MAC_Auth_Service

Authentication Method: EAP-MD5

Authentication Source: None

Authorization Source: [Endpoints Repository]

Roles: [User Authenticated]

Enforcement Profiles: Guest_Access_Portal_Enforcement

Service Monitor Mode: Disabled

Online Status: Online

Showing 2 of 1-10 records Change Status Export Show Logs Close

- To get more details on the Web authentication request from the endpoint, click the request (line 1 of the Access Tracker request table).

Request Details ✕

Summary
Input
Output

Session Identifier:	W00000011-01-56b01b20
Date and Time:	Feb 01, 2016 18:57:36 PST
End-Host Identifier:	0050569b037f
Username:	guest2@guestcompany.com
Access Device IP/Port:	-
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Guest_WebAuth_Service
Authentication Method:	Not applicable
Authentication Source:	[Guest User Repository]
Authorization Source:	[Guest User Repository]
Roles:	[Guest], [User Authenticated]
Enforcement Profiles:	Guest_Access_CoA_Profile
Service Monitor Mode:	Disabled
Online Status:	● Online

◀◀ Showing 1 of 1-10 records ▶▶

Change Status
Export
Show Logs
Close

RELATED DOCUMENTATION

[Troubleshooting Central Web Authentication | 33](#)

[Technical Overview | 3](#)

[Use Case Overview | 2](#)

Troubleshooting Central Web Authentication

IN THIS SECTION

- [Troubleshooting Using Trace Options | 34](#)
- [Troubleshooting the JNPR_RSVD_FILTER_CWA Firewall Filter | 34](#)

This topic describes how you get detailed diagnostic information by enabling tracing of authentication operations on the EX Series switch.

Aruba ClearPass Policy Manager provides additional detailed diagnostic information. See your Aruba ClearPass documentation for more information.

Troubleshooting Using Trace Options

You can enable trace options for the 802.1X protocol. The following set of commands enable the writing of trace logs to a file named **dot1x**:

```
user@Policy-EX4300-01# set protocols dot1x traceoptions file dot1x
user@Policy-EX4300-01# set protocols dot1x traceoptions file size 5m
user@Policy-EX4300-01# set protocols dot1x traceoptions flag all
```

Use the `show log` CLI command to display the contents of the trace log file. For example:

```
user@Policy-EX4300-01> show log dot1x
user@Policy-EX4300-01> show log dot1x | last 10 | refresh
```

You can also display the contents of the trace log file from the UNIX-level shell. For example:

```
user@Policy-EX4300-01> start shell
user@Policy-EX4300-01:RE:0% tail -f /var/log/dot1x
```

Troubleshooting the JNPR_RSVD_FILTER_CWA Firewall Filter

The JNPR_RSVD_FILTER_CWA firewall filter is dynamically installed in the Packet Forwarding Engine (PFE). Because it is not configured through the Junos CLI, you cannot view the filter terms using the CLI.

You can use the Junos OS vty shell command to connect to the PFE to obtain more information about the JNPR_RSVD_FILTER_CWA filter. In the examples below, the vty command is used to see detailed information about the filter JNPR_RSVD_FILTER_CWA that is installed as part of the MAC RADIUS authentication process.

NOTE: The vty command is hidden command and is not supported by JTAC. Because vty commands are undocumented and their use can cause network disruption or operational issues, using vty is not generally recommended.

1. Start vty.

```
user@Policy-EX4300-01> start shell
user@Policy-EX4300-01:RE:0% vty fpc0
```

2. Use the show filter command to determine the index number of the filter on ge-0/0/22.

```
(vty)# sh filter
Program Filters:
-----
   Index   Dir   Cnt   Text   Bss  Name
-----  -
Term Filters:
-----
   Index   Semantic   Name
-----  -
      1   Classic   Client_Policy
      2   Classic   guest_access_policy_1
      3   Classic   test_cwa_ISE
      4   Classic   IPPhone_mac_auth_policy1
      5   Classic   IPPhone_mac_auth_policy_1
  17000   Classic   __default_arp_policer__
  57006   Classic   __jdhcpd__
  57007   Classic   __dhcpv6__
  57008   Classic   __cfm_filter_shared_lc__
  65008   Classic   __jdhcpd_l2_snoop_filter__
12582912   Classic   dot1x_ge-0/0/6
12582913   Classic   dot1x_ge-0/0/8
12582914   Classic   dot1x_ge-0/0/22
46137360   Classic   pfe-cos-cl-553-5-1
46137361   Classic   pfe-cos-cl-554-5-1
46137362   Classic   pfe-cos-cl-555-5-1
```

3. Display the counters associated with the filter.

```
(vty)# sh filter index 12582914 counters
Filter Counters/Policers:
   Index          Packets          Bytes  Name
-----
12582914          0                0  CWA_arp_0050569b037f
12582914          0                0  CWA_destip_0050569b037f
12582914          0                0  CWA_dhcp_0050569b037f
12582914          0                0  CWA_https_0050569b037f
12582914          0                0  CWA_t_dns_0050569b037f
12582914          0                0  CWA_u_dns_0050569b037f
12582914          0                0  dot1x_ge-0/0/22_CWA_http_0050569b037f
```

4. Display the terms of the filter.

```
(vty)# sh filter index 12582914 program
Filter index = 12582914
Optimization flag: 0x0
Filter notify host id = 0
Filter properties: None
Filter state = CONSISTENT
term CWA_destip_0050569b037f
term priority 0
  smac
    0.80.86.155.3.127/48
  ip-destination-address
    10.105.5.153/32

  then
    accept
    count CWA_destip_0050569b037f
term CWA_t_dns_0050569b037f
term priority 0
  smac
    0.80.86.155.3.127/48
  ip-protocol
    6
  destination-port
    53
```



```
then
  accept
  count CWA_t_dns_0050569b037f
term CWA_u_dns_0050569b037f
term priority 0
  smac
    0.80.86.155.3.127/48
  ip-protocol
```

RELATED DOCUMENTATION

[Example: Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass | 5](#)

[Technical Overview | 3](#)

[Use Case Overview | 2](#)