

# ClearPass Policy manager Cisco Switch Setup with CPPM

---



*Technical Note*

---

## Copyright

© 2012 Aruba Networks, Inc. Aruba Networks trademarks include  airwave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners

## Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site::

[http://www.arubanetworks.com/open\\_source](http://www.arubanetworks.com/open_source)

## Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

## Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.



www.arubanetworks.com  
1344 Crossman Avenue  
Sunnyvale, California 94089  
Phone: 408.227.4500  
Fax 408.227.4550

Audience .....	9
Typographic Conventions .....	9
Contacting Support .....	10
<b>1. Introduction.....</b>	<b>11</b>
Assumptions.....	11
Requirements.....	11
Audience .....	11
<b>2. Switch Configuration.....</b>	<b>12</b>
<b>3. 802.1x Service Setup .....</b>	<b>16</b>
<b>4. Cisco Downloadable ACL (DACL).....</b>	<b>19</b>
<b>5. MAC Authentication Service Setup.....</b>	<b>23</b>
<b>6. Adding a Network Device (Switch) .....</b>	<b>25</b>
<b>7. Adding a Test User Account.....</b>	<b>26</b>
<b>8. Testing the 802.1x Service with Access Tracker .....</b>	<b>28</b>
<b>9. Testing the MAC Authentication Service with Access Tracker.....</b>	<b>29</b>
<b>10. Troubleshooting .....</b>	<b>31</b>



Figure 1 CPPM Enforcement Profiles .....	16
Figure 2 Adding a new 802.1x Enforcement Profile.....	17
Figure 3 802.1x Enforcement Profile Attributes tab .....	17
Figure 4 Configuring the VLAN as Value 999 .....	17
Figure 5 Tunnel-Private-Group-Id value is set to 999. ....	18
Figure 6 Adding a Cisco ACL (DAACL) Enforcement Profile.....	19
Figure 7 Adding Enforcement Policies.....	19
Figure 8 Adding Enforcement Policy profile properties.....	20
Figure 9 Creating the 802.1x Wired Service.....	20
Figure 10 Selecting the Authentication Sources: [ Local User Repository].....	21
Figure 11 802.1x Wired Service Enforcement properties.....	21
Figure 12 Reorder Services list.....	22
Figure 13 Adding a non-802.1x MAC authentication Service.....	23
Figure 14 Configuring a non-802.1x MAC Authentication Method and Authentication Source .....	23
Figure 15 Reordering a non-802.1x MAC authentication Service .....	24
Figure 16 Adding a TestRole user.....	26
Figure 17 Adding Local User properties .....	27
Figure 18 Testing a 802.1x Service Access Tracker .....	28
Figure 19 Populating an Access Tracker profile properties.....	28
Figure 20 Access Tracker window .....	29
Figure 21 A non-802.1x network device fails MAC Authentication Service .....	29
Figure 22 Configuring the Endpoints of a non-802.1x network device.....	30
Figure 23 Editing the Endpoint properties of a non-802.1x network device .....	30



Table 1 VLAN numbers ..... 13



## Audience

This ClearPass Policy manager Cisco Switch Setup with CPPM is intended for system administrators and people who are integrating Aruba Networks Wireless Hardware with ClearPass 6.0.1.

## Typographic Conventions

The following conventions are used throughout this manual to emphasize important concepts.

Type Style	Description
<i>Italics</i>	Used to emphasize important items and for the titles of books.
<b>Boldface</b>	Used to highlight navigation in procedures and to emphasize command names and parameter options when mentioned in text.
Sample template code or HTML text	Code samples are shown in a fixed-width font.
<angle brackets>	When used in examples or command syntax, text within angle brackets represents items you should replace with information appropriate to your specific situation. For example: ping <ipaddr> In this example, you would type “ping” at the system prompt exactly as shown, followed by the IP address of the system to which ICMP echo packets are to be sent. Do not type the angle brackets.

## Contacting Support

Main Site	<a href="http://arubanetworks.com">arubanetworks.com</a>
Support Site	<a href="http://support.arubanetworks.com">support.arubanetworks.com</a>
Airheads Social Forums and Knowledge Base and Knowledge Base	<a href="http://community.arubanetworks.com">community.arubanetworks.com</a>
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephones	<a href="http://www.arubanetworks.com/support-services/aruba-support-program/contact-support/">http://www.arubanetworks.com/support-services/aruba-support-program/contact-support/</a>
Software Licensing Site	<a href="https://licensing.arubanetworks.com/">https://licensing.arubanetworks.com/</a>
End of Support information	<a href="http://www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/">www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/</a>
Wireless Security Incident Response Team (WSIRT)	<a href="http://www.arubanetworks.com/support-services/security-bulletins/">http://www.arubanetworks.com/support-services/security-bulletins/</a>

### Support Email Addresses

Americas and APAC	<a href="mailto:support@arubanetworks.com">support@arubanetworks.com</a>
EMEA	<a href="mailto:emea_support@arubanetworks.com">emea_support@arubanetworks.com</a>
WSIRT Email	<a href="mailto:wsirt@arubanetworks.com">wsirt@arubanetworks.com</a>

Please email details of any security problem found in an Aruba product.

---

# 1. Introduction

The purpose of this document is to provide setup instructions for the Cisco 3750 12.2 (58) switch with the ClearPass Policy Manager (CPPM). This includes 802.1x, MAC, and Downloadable Access Control Lists (DACLS) authentications. Voice services will not be covered in this document.

## Assumptions

Verify that a basic configuration of CPPM has been completed (setup and a generic catch-all radius service).

This document discussion uses an Aruba 3200 controller (192.168.99.5) as the DHCP server. Use of a DHCP server setup for the discussed VLANs is required.

Cisco switches support multiple authentication methods and many RADIUS options that are passed to the switch. This document discusses only a small subset of these features.

After each configuration change, exit the configure terminal mode and perform a “write memory” to save the configuration.

## Requirements

- LAN Switch that supports 802.1x and MAC Authentication Bypass
- DHCP Server for the registration VLAN
- Current ClearPass Policy Manager release

## Audience

This document is intended for network administrators deploying a network security solution.

Basic familiarity with most Cisco switches is assumed. For in-depth information about the features and functions of this appliance, refer to the ClearPass User Guide.

---

## 2. Switch Configuration

The first step is to perform the switch configuration. It is assumed that VLAN1 has been created for the switch with a correlating network-accessible IP address. This IP address must communicate with the CPPM Data IP address (unless a single IP address is configured in CPPM, in which case it is the management IP address).

Verify the switch can ping CPPM:

```
CPPM-Demo-3750# ping 192.168.99.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

CPPM-Demo-3750#
```

In the event an error is received, verify the correct ip default-gateway is set and that the firewall is not blocking the switch-to-CPPM communication.

Enable the new access control commands and functions, to include advanced features, using the following command:

```
CPPM-Demo-3750#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CPPM-Demo-3750 (config)# aaa new-model
```

Add CPPM as the RADIUS server with the following commands:

```
CPPM-Demo-3750 (config)# radius server cppm-demo
CPPM-Demo-3750 (config-radius-server)# address ipv4 192.168.99.10
CPPM-Demo-3750 (config-radius-server)# key aruba123
CPPM-Demo-3750 (config-radius-server)# exit
CPPM-Demo-3750 (config)#
```

“radius server” name of server (e.g. cppm-demo) is a new command. Older command uses “radius-server host 192.168.99.10 key aruba123”.

Run the following command to enable 802.1x:

```
CPPM-Demo-3750 (config)# dot1x system-auth-control
```

Use the following commands to set the switch to use RADIUS for AAA Authentication and Accounting:

```
CPPM-Demo-3750 (config)# aaa authentication dot1x default group radius
CPPM-Demo-3750 (config)# aaa authorization network default group radius
CPPM-Demo-3750 (config)# aaa accounting dot1x default start-stop group radius
```

Add a AAA server for dynamic authorization:

```
CPPM-Demo-3750 (config)# aaa server radius dynamic-author
CPPM-Demo-3750 (config-locsvr-da-radius)# client 192.168.99.10 server-key aruba123
CPPM-Demo-3750 (config-locsvr-da-radius)# port 3799
CPPM-Demo-3750 (config-locsvr-da-radius)# auth-type all
CPPM-Demo-3750 (config-locsvr-da-radius)# exit
CPPM-Demo-3750 (config)#
```

The following VLAN numbers will be used:

Table 1 VLAN numbers

VLAN Number	Purpose
999	Users and Access Points
333	Untrusted Devices
200	VoIP Phones
60	Printers
50	Security Network

Use best practices to create standardized naming conventions that describe VLAN purposes and locations as displayed below:

```

CPPM-Demo-3750 (config)# vlan 999
CPPM-Demo-3750 (config-vlan)# name "Users and APs"
CPPM-Demo-3750 (config-vlan)# exit
CPPM-Demo-3750 (config)# vlan 333
CPPM-Demo-3750 (config-vlan)# name "Untrusted Devices"
CPPM-Demo-3750 (config-vlan)# exit
CPPM-Demo-3750 (config)# vlan 200
CPPM-Demo-3750 (config-vlan)# name "VoIP Phones"
CPPM-Demo-3750 (config-vlan)# exit
CPPM-Demo-3750 (config)# vlan 60
CPPM-Demo-3750 (config-vlan)# name "Printers"
CPPM-Demo-3750 (config-vlan)# exit
CPPM-Demo-3750 (config)# vlan 50
CPPM-Demo-3750 (config-vlan)# name "Security Network"
CPPM-Demo-3750 (config-vlan)# exit
CPPM-Demo-3750 (config)#

```

**Note: CPPM-Demo-3750 is also the router.**

Next, create interfaces on each VLAN. If the Cisco switch is not acting as the router (or does not have L3 capability), the VLANs and interface commands must be passed to the router. The run commands are as follows:

```

CPPM-Demo-3750 (config)# interface vlan 999
CPPM-Demo-3750 (config-if)# ip address 192.168.99.1 255.255.255.0
CPPM-Demo-3750 (config-if)# ip helper-address 192.168.99.10
CPPM-Demo-3750 (config-if)# ip helper-address 192.168.99.5
CPPM-Demo-3750 (config-if)# exit
CPPM-Demo-3750 (config)# interface vlan 333
CPPM-Demo-3750 (config-if)# ip address 192.168.33.1 255.255.255.0
CPPM-Demo-3750 (config-if)# ip helper-address 192.168.99.10
CPPM-Demo-3750 (config-if)# ip helper-address 192.168.33.5
CPPM-Demo-3750 (config-if)# exit
CPPM-Demo-3750 (config)# interface vlan 200
CPPM-Demo-3750 (config-if)# ip address 192.168.200.1 255.255.255.0
CPPM-Demo-3750 (config-if)# ip helper-address 192.168.99.10
CPPM-Demo-3750 (config-if)# ip helper-address 192.168.200.5
CPPM-Demo-3750 (config-if)# exit
CPPM-Demo-3750 (config)# interface vlan 60
CPPM-Demo-3750 (config-if)# ip address 192.168.60.1 255.255.255.0
CPPM-Demo-3750 (config-if)# ip helper-address 192.168.99.10
CPPM-Demo-3750 (config-if)# ip helper-address 192.168.99.5

```

```

CPPM-Demo-3750 (config-if)# exit
CPPM-Demo-3750 (config)# interface vlan 50
CPPM-Demo-3750 (config-if)# ip address 192.168.50.1 255.255.255.0
CPPM-Demo-3750 (config-if)# ip helper-address 192.168.99.10
CPPM-Demo-3750 (config-if)# ip helper-address 192.168.99.5
CPPM-Demo-3750 (config-if)# exit

```

**Notes:**

**192.168.99.5 is the DHCP server and will vary based on the local configuration. 192.168.99.10 refers to CPPM for the DHCP request in order for the device to be profiled.**

Verify the RADIUS server settings and applicable VLANs router interfaces for the VLANs have been set prior to configuring a port to perform the 802.1x and MAC authentication bypass (also known as MAC authentication fallback).

Determine the interface type and numbering conventions using the “show interfaces description” command. The following list of interfaces (ports) will be displayed:

```

Fa = FastEthernet or 100Mbps
Gi = GigabitEthernet or 1,000Mbps

```

Use Fa1/0/24, which is the 24<sup>th</sup> copper port on our 3750. Use the following commands for port configuration:

**Note: Interface type and numbering will differ from model to model.**

```

CPPM-Demo-3750 (config)# interface FastEthernet1/0/24
CPPM-Demo-3750 (config-if)# switchport access vlan 333
CPPM-Demo-3750 (config-if)# switchport mode access
CPPM-Demo-3750 (config-if)# authentication order dot1x mab
CPPM-Demo-3750 (config-if)# authentication priority dot1x mab
CPPM-Demo-3750 (config-if)# authentication port-control auto
CPPM-Demo-3750 (config-if)# authentication periodic
CPPM-Demo-3750 (config-if)# authentication timer reauthenticate server
CPPM-Demo-3750 (config-if)# mab
CPPM-Demo-3750 (config-if)# dot1x pae authenticator
CPPM-Demo-3750 (config-if)# dot1x timeout server-timeout 30
CPPM-Demo-3750 (config-if)# dot1x timeout tx-period 10
CPPM-Demo-3750 (config-if)# dot1x timeout supp-timeout 30
CPPM-Demo-3750 (config-if)# dot1x max-req 3
CPPM-Demo-3750 (config-if)# dot1x max-reauth-req 10
CPPM-Demo-3750 (config-if)# spanning-tree portfast
CPPM-Demo-3750 (config-if)# exit

```

Set the port to access mode (untagged) with an untagged VLAN of 333 (the untrusted devices VLAN).

MAC Authentication Bypass (MAB) permits the port to perform MAC authentication if the switch detects that the device is not 802.1x capable.

MAB occurs after 40 seconds:

$(\text{max-reauth-requests} + 1) * \text{tx-period} = 802.1x \text{ authentication timeout.}$

The values provided for these port settings are for lab and evaluation tests only! Consult the Cisco document titled, **Configuring 802.1X Port-Based Authentication**, and work with Cisco Support directly to determine the correct port settings for your environment.

**Note: If CPPM goes offline, all users will gain access to VLAN Number 333.**

In some circumstances, it may be necessary to set the default VLAN to 999.

The following commands must run in order for DACL's to work correctly:

```
CPPM-Demo-3750 (config)# ip dhcp snooping  
CPPM-Demo-3750 (config)# ip device tracking  
CPPM-Demo-3750 (config)# radius-server vsa send authentication
```

### 3. 802.1x Service Setup

The CPPM profiles are applied globally but they must be referenced in an enforcement policy that is associated with a Service to be evaluated. Each Enforcement Profile can have an associated group of Network Access Devices (NADs).

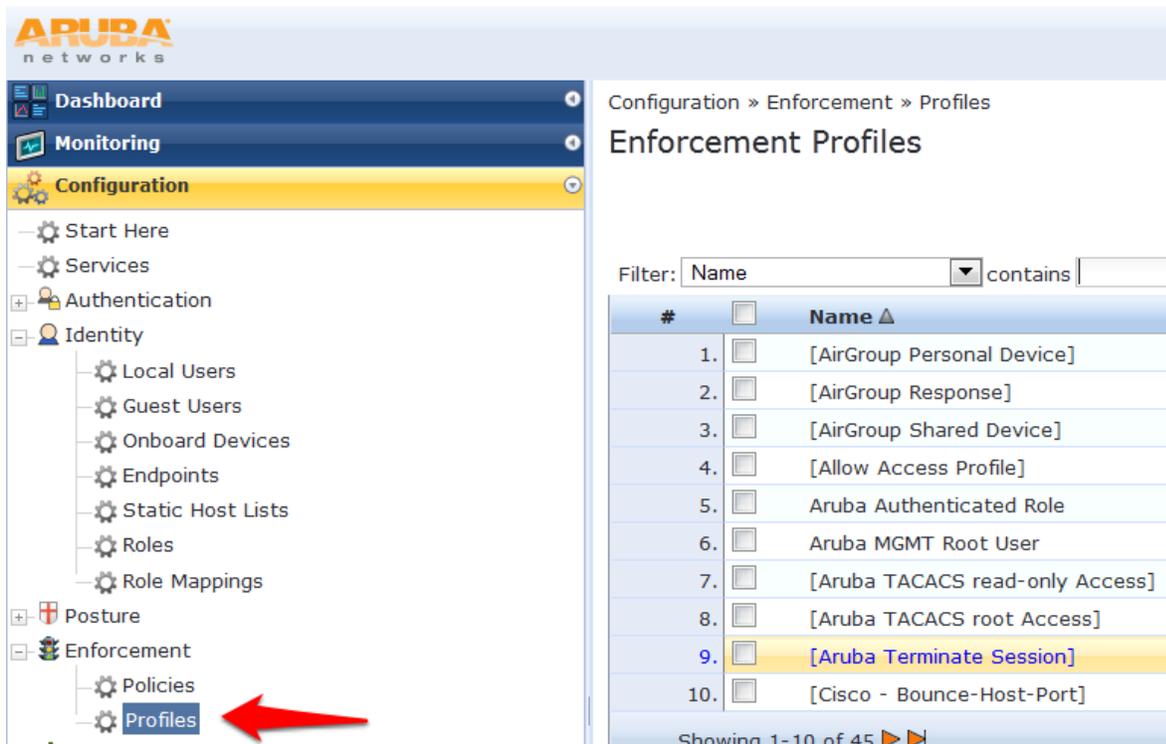
Service setup requires a set of rules known as Enforcement Profiles. One profile will return VLAN 999 and one will return a Cisco DACL.

#### Adding Enforcement Profiles

##### VLAN 999

Navigate to **Configuration->Enforcement->Profiles**.

Figure 1 CPPM Enforcement Profiles



Click **Add Enforcement Profile** in the top right corner of the page.



Enter the profile properties from Figure 1 Adding a new 802.1x Enforcement Profile below.

Figure 2 Adding a new 802.1x Enforcement Profile

Configuration » Enforcement » Profiles » Add Enforcement Profile

### Enforcement Profiles

Profile	Attributes	Summary
Template:	VLAN Enforcement	
Name:	VLAN 999	
Description:	Users and APs	
Type:	RADIUS	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	--Select-- <div style="float: right; margin-top: 5px;">                     Remove View Details Modify                 </div>	

Click **Next** to display the Attributes tab.

Figure 3 802.1x Enforcement Profile Attributes tab

Configuration » Enforcement » Profiles » Edit Enforcement Profile - VLAN 999

### Enforcement Profiles - VLAN 999

Summary	Profile	Attributes
Type	Name	Value
1. Radius:IETF	Session-Timeout	= 10800
2. Radius:IETF	Termination-Action	= RADIUS-Request (1)
3. Radius:IETF	Tunnel-Type	= VLAN (13)
4. Radius:IETF	Tunnel-Medium-Type	= IEEE-802 (6)
5. Radius:IETF	Tunnel-Private-Group-Id	= <span style="border: 1px solid red; padding: 2px;">Enter VLAN</span>
6. Click to add...		

Click Select the **RED** value and enter the VLAN as number 999.

Figure 4 Configuring the VLAN as Value 999

Configuration » Enforcement » Profiles » Edit Enforcement Profile - VLAN 999

### Enforcement Profiles - VLAN 999

Summary	Profile	Attributes
Type	Name	Value
1. Radius:IETF	Session-Timeout	= 10800
2. Radius:IETF	Termination-Action	= RADIUS-Request (1)
3. Radius:IETF	Tunnel-Type	= VLAN (13)
4. Radius:IETF	Tunnel-Medium-Type	= IEEE-802 (6)
5. Radius:IETF	Tunnel-Private-Group-Id	= <span style="border: 1px solid red; padding: 2px;">999</span>
6. Click to add...		

Click the **Save Disk** at the end of the line.

Click **Next** to review the settings and display the Profile Summary.

**Note:** Verify that the Tunnel-Private-Group-Id value is set to 999.

Figure 5 Tunnel-Private-Group-Id value is set to 999.

Configuration » Enforcement » Profiles » Edit Enforcement Profile - VLAN 999

### Enforcement Profiles - VLAN 999

Summary		Profile	Attributes
<b>Profile:</b>			
Name:	VLAN 999		
Description:	Users and APs		
Type:	RADIUS		
Action:	Accept		
Device Group List:	-		
<b>Attributes:</b>			
	Type	Name	Value
1.	Radius:IETF	Session-Timeout	= 10800
2.	Radius:IETF	Termination-Action	= RADIUS-Request (1)
3.	Radius:IETF	Tunnel-Type	= VLAN (13)
4.	Radius:IETF	Tunnel-Medium-Type	= IEEE-802 (6)
5.	Radius:IETF	Tunnel-Private-Group-Id	= 999



999

## 4. Cisco Downloadable ACL (DACL)

Navigate to **Configuration->Enforcement->Profiles**. Click **Add Enforcement Profile**.

Click **Add Enforcement Profile** in the top right corner of the page.



Enter the profile properties from Figure 5 Adding a Cisco ACL (DACL) Enforcement Profile below.

Figure 6 Adding a Cisco ACL (DACL) Enforcement Profile

Configuration » Enforcement » Profiles » Add Enforcement Profile

### Enforcement Profiles

Profile	Attributes	Summary
Template:		Cisco Downloadable ACL Enforcement
Name:		Cisco DACL
Description:		
Type:		RADIUS
Action:		<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop
Device Group List:		--Select--

Click **Next**.

Note the displayed screen has been auto-populated. Click **Next** to accept the default attributes. Select **Click to add**. Add additional profiles as applicable.

Click **Next** to verify the settings.

Click **Save**.

### Adding Enforcement Policies

Enforcement Policies are always associated with a **Service** and a service can only have one policy.

Navigate to **Configuration->Enforcement->Policies**. Click **Add Enforcement Policy**. Enter the profile properties to reflect the options as displayed below:

Figure 7 Adding Enforcement Policies

Configuration » Enforcement » Policies » Add

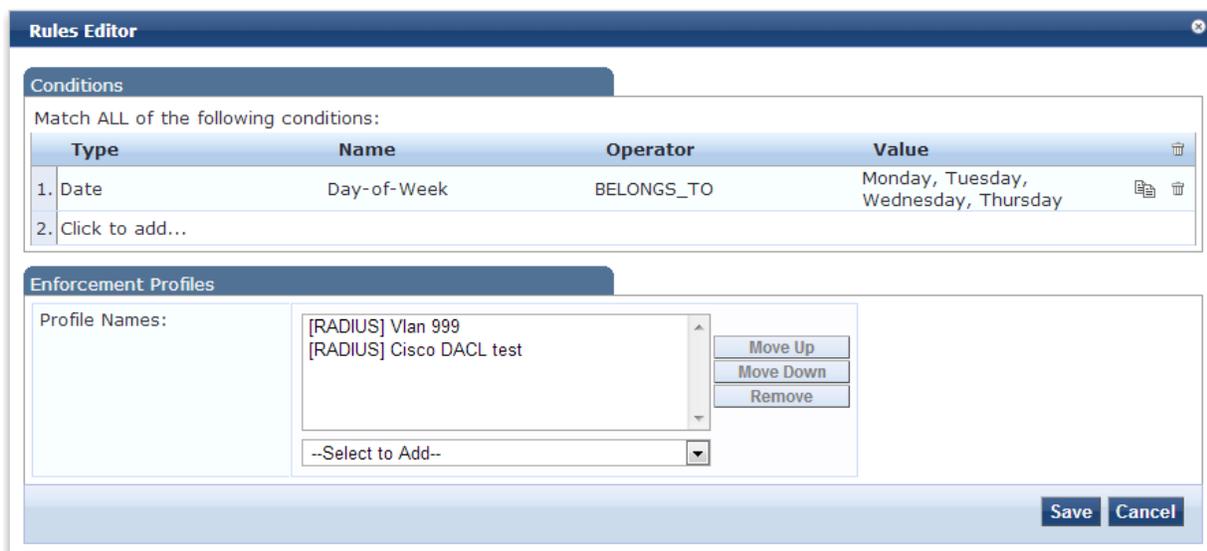
### Enforcement Policies

Enforcement	Rules	Summary
Name:	Wired-Enforcement with DACL	
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:	Cisco DACL test	<a href="#">View Details</a> <a href="#">Modify</a> <a href="#">Add new Enforcement Profile</a>

[Back to Enforcement Policies](#) [Next >](#) [Save](#) [Cancel](#)

Click **Next**. Click **Add Rule**. Enter the profile properties to reflect the options as displayed below:

Figure 8 Adding Enforcement Policy profile properties



Click **Save**.

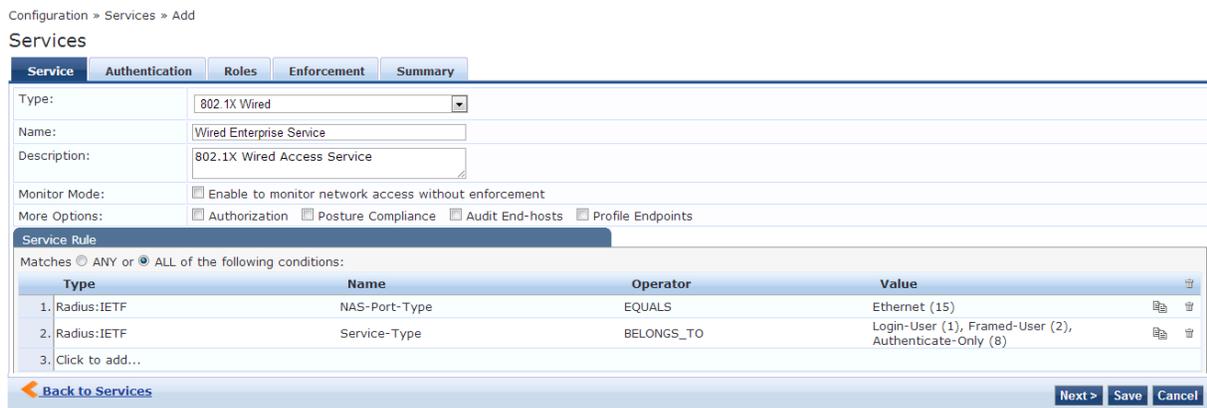
Click **Next**.

Click **Save**.

### Creating the Service

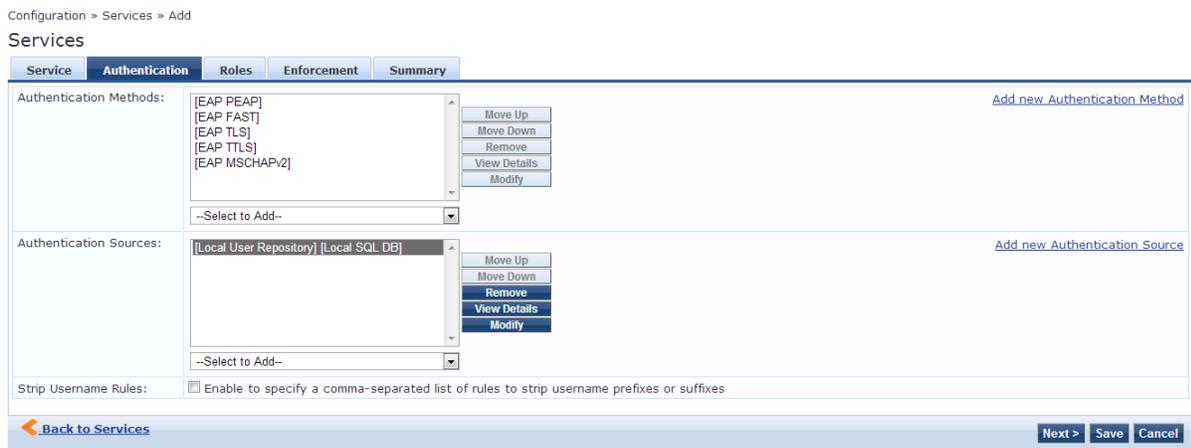
Navigate to **Configuration->Services**. Click **802.1X Wired**. Enter the profile properties to reflect the options as displayed below:

Figure 9 Creating the 802.1x Wired Service



Click **Next**. Select the Authentication Sources: [ Local User Repository]... as displayed below:

Figure 10 Selecting the Authentication Sources: [ Local User Repository]

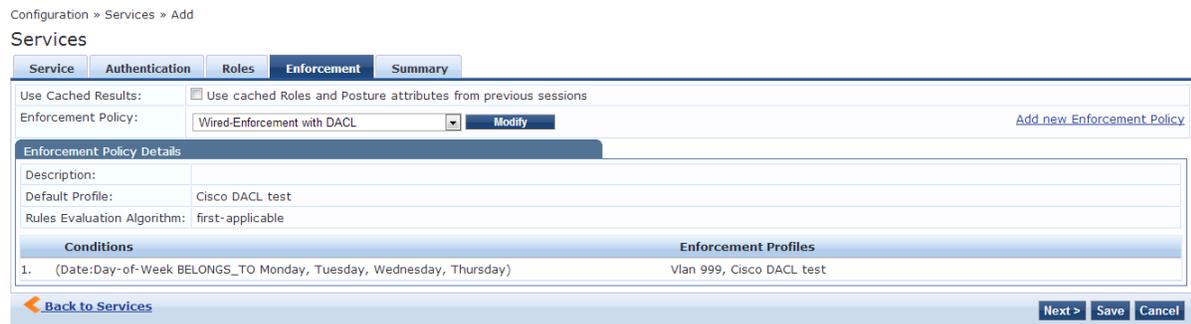


Click **Next**.

**Note:** Role Mapping will not be set up at this time. Click **Next**.

Enter the profile properties to reflect the options as displayed below:

Figure 11 802.1x Wired Service Enforcement properties



Click **Next**. Click **Save**.

### Reorder Services

Reordering is important as CPPM evaluates requests against the service rules of each service configured in the order in which these services are defined. The service associated with the first matching service rule is then associated with this request.

At the **Configuration->Services** tab, navigate to the newly created service and click **Reorder** to the profile properties to reflect as displayed below:

Figure 12 Reorder Services list

Configuration » Services » Reorder

## Reorder Services

Order	Name	Service Details:
1	[Policy Manager Admin Network Login Service]	Name: Wired Enterprise Service
2	Wired Enterprise Service	Template: 802.1X Wired
3	Generic RADIUS Catch All	Type: RADIUS
		Description: 802.1X Wired Access Service
		Status: Enabled
		<b>Service Rule</b>
		( (Radius:IETF:NAS-Port-Type EQUALS Ethernet (15)) AND (Radius:IETF:Service-Type BELONGS_TO Login-User (1), Framed-User (2), Authenticate-Only (8)) ) AND (Connection:Protocol EQUALS RADIUS)

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

[Back to Services](#) [Save](#) [Cancel](#)

## 5. MAC Authentication Service Setup

Previously, the MAC Authentication Bypass was physically enabled via the switch. This configuration setup permits non-802.1x devices to authenticate via their MAC address.

**Note:** MAC addresses are easily falsified and it is recommended that a profiler service is used to verify the MAC address. Profilers inspect the DHCP request for an added level of security.

Navigate to **Configuration->Services**. Click **Add Service**. Enter the profile properties to reflect the options as displayed below:

Figure 13 Adding a non-802.1x MAC authentication Service

Configuration » Services » Add

Services

Service Authentication Roles Enforcement Summary

Type: MAC Authentication

Name: MAC Auth Service

Description: MAC-based Authentication Service

Monitor Mode:  Enable to monitor network access without enforcement

More Options:  Authorization  Audit End-hosts  Profile Endpoints

Service Rule

Matches  ANY or  ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)
3. Connection	Client-Mac-Address	EQUALS	% {Radius:IETF:User-Name}
4. Click to add...			

[Back to Services](#) [Next >](#) [Save](#) [Cancel](#)

Click **Next**. The Authentication Method is preset to MAC AUTH and the Authentication Source is preset to Endpoints Repository displayed:

Figure 14 Configuring a non-802.1x MAC Authentication Method and Authentication Source

Configuration » Services » Add

Services

Service Authentication Roles Enforcement Summary

Authentication Methods: [MAC AUTH] [Add new Authentication Method](#)

Authentication Sources: [Endpoints Repository] [Local SQL DB] [Add new Authentication Source](#)

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

[Back to Services](#) [Next >](#) [Save](#) [Cancel](#)

Click **Next**. Role Mapping will not be set up at this time. Click **Next**.

Click **Next** to accept the default Enforcement Policy.

Click **Next**. Click **Save**.

### Reorder Services

Reordering is important as CPPM evaluates requests against the service rules of each service configured, in the order in which these services are defined. The service associated with the first matching service rule is then associated with this request.

At the **Configuration->Services** tab, navigate to the newly created service and click **Reorder** to the profile properties to reflect as displayed below:

**Note:** When working with multiple 802.1x services, it is important to order them from most specific to least specific with the generic RADIUS catch all service being last.

Figure 15 Reordering a non-802.1x MAC authentication Service

Configuration » Services » Reorder

### Reorder Services

Order	Name	Service Details:
1	[Policy Manager Admin Network Login Service]	Name: MAC Auth Service
2	Wired Enterprise Service	Template: MAC Authentication
3	MAC Auth Service	Type: RADIUS
4	Generic RADIUS Catch All	Description: MAC-based Authentication Service
		Status: Enabled
		<b>Service Rule</b>
		( (Radius:IETF:NAS-Port-Type BELONGS_TO Ethernet (15), Wireless-802.11 (19)) AND (Radius:IETF:Service-Type BELONGS_TO Login-User (1), Call-Check (10)) AND (Connection:Client-Mac-Address EQUALS %{Radius:IETF:User-Name}) ) AND (Connection:Protocol EQUALS RADIUS)

Move Up Move Down

[Back to Services](#) Save Cancel

Click **Save**.

## 6. Adding a Network Device (Switch)

To connect with CPPM using the supported protocols, a Network Access Device (NAD) must belong to the global list of devices in the Policy Manager database.

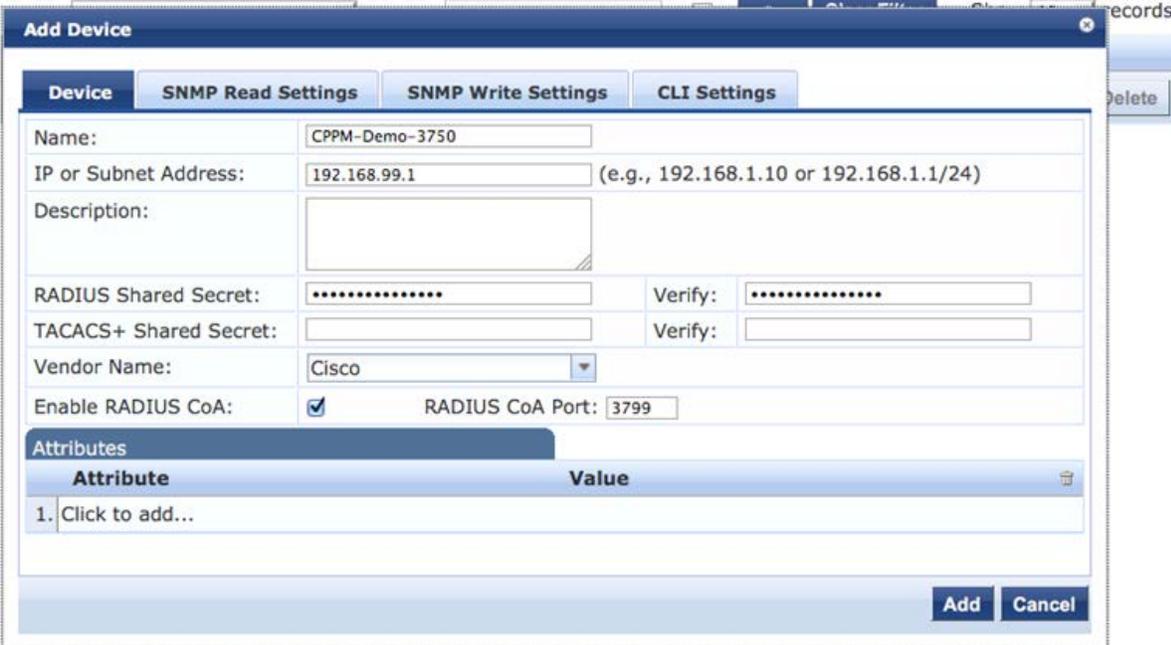
The switch to be used must be set up as a Network Device in CPPM prior to testing the services.

Navigate to **Configuration->Network->Devices**. Click **Add Device**. Enter the profile properties to reflect the options as displayed below (Note: the RADIUS Shared Secret is “aruba123” which was configured earlier on the Cisco switch via the command `client 192.168.99.10 server-key aruba123`):

Configuration » Network » Devices

Network Devices

 Add Device  
 Import Devices  
 Export Devices



Attribute	Value
1. Click to add...	

Click **Add** to save this device to the Network Devices list.

## 7. Adding a Test User Account

CPPM requires a local user account to test the 802.1x service. All local accounts in CPPM must have a Role.

Navigate to **Configuration->Identity->Roles**. Click **Add Roles**. Enter the profile properties to reflect the options as displayed below:

Figure 16 Adding a TestRole user

Configuration » Identity » Roles

Roles

Filter: Name contains Go Clear Filter Show 50 records

# Add New Role

Name: TestRole

Description:

Save Cancel

Add Roles  
Import Roles  
Export Roles

Export Delete

Click **Save**.

To create a user account, navigate to **Configuration->Identity->Local Users**. Click **Add User**.

User ID - test

Password – test123

Checkbox - set to Enable User

Role – TestRole

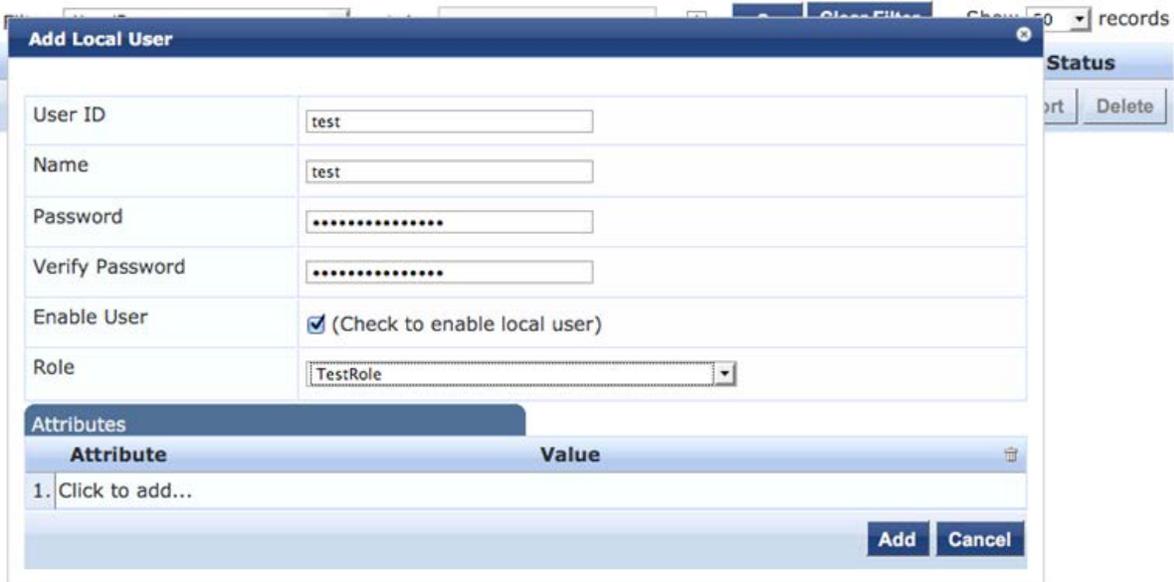
Enter the profile properties to reflect the options as displayed below:

Figure 17 Adding Local User properties

Configuration » Identity » Local Users

## Local Users

-  Add User
-  Import Users
-  Export Users



User ID	test
Name	test
Password	.....
Verify Password	.....
Enable User	<input checked="" type="checkbox"/> (Check to enable local user)
Role	TestRole

Attributes	
Attribute	Value
1. Click to add...	

Click **Add**.

Setup is now complete.

## 8. Testing the 802.1x Service with Access Tracker

Access Tracker provides a real-time display of system activity. It logs authentication attempts received from a list of network devices.

Navigate to **Monitoring & Reporting->Access Tracker**.

Figure 18 Testing a 802.1x Service Access Tracker

Monitoring & Reporting » Live Monitoring » Access Tracker

Access Tracker Aug 17, 2012 06:15:46 PDT Auto Refresh

Data Filter: [All Requests] Server: cppm1 (192.168.99.10)  
Date Range: Last 1 day before Today Edit

Filter: Type contains  Go Clear Filter Show 50 records

Server	Type	User	Service Name	Login	Date and Time
--------	------	------	--------------	-------	---------------

Verify the Auto Refresh is enabled (green) and filters are cleared. Click the AutoRefresh icon/text to change the status as applicable.

**Important!** Log in AFTER the network cable has been plugged in to the test network device.

Enter the log in credentials when prompted. Verify the profile properties are similar to the options as displayed below:

Figure 19 Populating an Access Tracker profile properties

Monitoring & Reporting » Live Monitoring » Access Tracker

Access Tracker Aug 17, 2012 06:24:12 PDT Auto Refresh

Data Filter: [All Requests] Server: cppm1 (192.168.99.10)  
Date Range: Last 1 day before Today Edit

Filter: Type contains  Go Clear Filter Show 50 records

Server	Type	User	Service Name	Login	Date and Time
192.168.99.10	RADIUS	test	Wired Enterprise Service	ACCEPT	2012/08/17 06:23:53
192.168.99.10	RADIUS	#ACSACL#-IP-Cisco_DA	Cisco Downloadable ACL	ACCEPT	2012/08/17 06:23:53

Showing 1-2 of 2

The first entry is the test computer authenticating for network access.

The last entry is the Cisco switch requesting the Downloadable ACL, (DACL) information from CPPM.

If the ACSACL is **RED**, in the second row above, verify the commands are entered as discussed in the Switch Configuration section of this document. If the user authentication fields are **RED**, in the first row above, verify the (enabled) account credentials.

## 9. Testing the MAC Authentication Service with Access Tracker

**Note:** Use a network device that does not support 802.1x.

Navigate to **Monitoring & Reporting->Access Tracker**.

Figure 20 Access Tracker window

Monitoring & Reporting » Live Monitoring » Access Tracker

Access Tracker Aug 17, 2012 06:15:46 PDT Auto Refresh

Data Filter: [All Requests] Server: cppm1 (192.168.99.10)  
Date Range: Last 1 day before Today Edit

Filter: Type contains  Go Clear Filter Show 50 records

Server	Type	User	Service Name	Login	Date and Time
--------	------	------	--------------	-------	---------------

Verify the Auto Refresh is enabled (green) and filters are cleared. Click the AutoRefresh icon/text to change the status as applicable.

Plug in the non-802.1x network device to port 24.

**Note:** the MAC Authentication service request failed.

Figure 21 A non-802.1x network device fails MAC Authentication Service

Monitoring & Reporting » Live Monitoring » Access Tracker

Access Tracker Aug 17, 2012 06:44:36 PDT Auto Refresh

Data Filter: [All Requests] Server: cppm1 (192.168.99.10)  
Date Range: Last 1 day before Today Edit

Filter: Type contains  Go Clear Filter Show 50 records

Server	Type	User	Service Name	Login	Date and Time
192.168.99.10	RADIUS	d8c7c8cdb35e	MAC Auth Service	REJECT	2012/08/17 06:44:25
192.168.99.10	RADIUS	d8c7c8cdb35e	MAC Auth Service	REJECT	2012/08/17 06:43:08
192.168.99.10	RADIUS	test	Wired Enterprise Service	REJECT	2012/08/17 06:23:55
192.168.99.10	RADIUS	test	Wired Enterprise Service	ACCEPT	2012/08/17 06:23:53
192.168.99.10	RADIUS	#ACSACL#-IP-Cisco_DA	Cisco Downloadable ACL	ACCEPT	2012/08/17 06:23:53

Showing 1-5 of 5

This is the expected behavior as the device is unknown.

Unplug the non-802.1x network device.

Navigate to **Configuration->Identity->Endpoints**. Select the MAC address of the non-802.1x device to connect as applicable.

Figure 22 Configuring the Endpoints of a non-802.1x network device

Configuration » Identity » Endpoints

## Endpoints

-  Add Endpoint
-  Import Endpoints
-  Export All Endpoints

Filter:  contains    Show  records

#	<input type="checkbox"/>	MAC Address	Hostname	Category	OS Family	Status	Profiled
1.	<input type="checkbox"/>	001e37d697e3	wnelsen-ap65	Computer	Windows	Unknown	Yes
2.	<input type="checkbox"/>	d8c7c8cdb35e				Unknown	No

Showing 1-2 of 2

Select the status of a device, by checking the box of the desired device, e.g. 'd8c7c7cdb35c' in the screen shot below, to display the Edit Endpoint dialog box.

Change the 'Status' to 'Known client' as displayed below:

Figure 23 Editing the Endpoint properties of a non-802.1x network device

Configuration » Identity » Endpoints

## Endpoints

-  Add Endpoint
-  Import Endpoints
-  Export All Endpoints

Filter:  contains    Show  records

#	<input type="checkbox"/>	MAC Address	Hostname	Category	OS Family	Status	Profiled
1.	<input type="checkbox"/>	001e37d697e3	wnelsen-ap65	Computer	Windows	Unknown	Yes
2.	<input checked="" type="checkbox"/>	d8c7c8cdb35e				Unknown	No

### Edit Endpoint

MAC Address:

Description:

Status:  Known client  Unknown client  Disabled client

Added by: Policy Manager

Attribute	Value
1. Click to add...	

Click **Save**.

Plug in the non-802.1x network device to port 24.

Navigate to **Monitoring & Reporting->Access Tracker**. Note the device is properly authenticated.

---

## 10. Troubleshooting

*Problem:*

I see the Downloadable ACL request is successful, but when I check the ACL for the device on the Cisco switch, it is empty.

*Solution:*

Verify the syntax of the DACL list in CPPM. If there is one ACL in the list that does not match the proper Cisco ACL syntax, then the entire list will be ignored.

*Problem:*

I do not see any incoming requests in Access Tracker.

*Solution:*

Navigate to **Monitoring & Reporting->Event Viewer**. Look for a **Yellow** entry. The most common mistake is either a RADIUS key mismatch or the IP address for the switch is incorrect in **Configuration->Network->Devices**. Another possibility is that your switch is using the wrong VLAN to attempt to communicate with CPPM. If necessary, run the following command in configure terminal mode on the Cisco switch:

```
CPPM-Demo-3750 (config)#ip radius source-interface v lan 999
```

This will force all RADIUS requests to use VLAN 999.