Network Configuration Example

Device Profiling with EX Series Switches and Aruba ClearPass Policy Manager

Modified: 2016-07-29

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

Network Configuration Example Device Profiling with EX Series Switches and Aruba ClearPass Policy Manager

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 http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

CHAPTER 1

Device Profiling with EX Series Switches and Aruba ClearPass Policy Manager

About This Network Configuration Example

This network configuration example describes how to configure a Juniper Networks EX Series Ethernet Switch and Aruba ClearPass Policy Manager to work together to authenticate wired endpoints that connect to EX Series switches. Specifically, it shows how to configure an EX Series switch and Aruba ClearPass to profile endpoints as part of the authentication process and use the information collected by device profiling to determine access policy.

Use Case Overview

Juniper Networks EX Series Ethernet Switches are designed to meet the demands of today's high-performance businesses. They enable companies to grow their networks at their own pace, minimizing large up-front investments. Based on open standards, EX Series switches provide the carrier-class reliability, security risk management, virtualization, application control, and lower total cost of ownership (TCO) that businesses need today, while allowing businesses to scale in an economically sensible way for years to come.

Aruba ClearPass Policy Manager is a policy management platform that provides role-based and device-based network access control (NAC) for any user across any wired, wireless, and VPN infrastructure. 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. This integration enables enterprises to deploy consistent security policies across their wired and wireless infrastructure.

Enterprises typically have a variety of users and endpoints, which results in multiple use cases that need to be addressed by their policy infrastructure. Depending on the type of endpoint and how it is being used, an endpoint might be authenticated by 802.1X authentication, MAC RADIUS authentication, or captive portal authentication. The policy infrastructure should enable any device to be connected to any port on the access switch and to be authenticated based on the type of the device, the authorization level of the user, or both.

In this network configuration example, we show how to configure Juniper Networks EX Series switches and Aruba ClearPass Policy Manager to use device profiling as part of the authentication process. Device profiling enables Aruba ClearPass to determine the type of endpoint that is being authenticated—for example, whether it is an access point or a VoIP phone or a Windows computer—and then use that information to enforce access policy appropriate to the device type.

Related Documentation

- Technical Overview on page 7
- Example: Configuring Device Profiling with EX Series Switches and Aruba ClearPass Policy Manager on page 8
- Monitoring Device Profiling on page 36
- Troubleshooting Authentication on page 38

Technical Overview

Aruba ClearPass Profile is a ClearPass Policy Manager module that performs device profiling. Once you enable the module, it automatically collects a variety of data about endpoints, analyzes the data to classify the endpoints, and stores the classifications as device profiles in an endpoint repository. You can then use the device profiles in enforcement policies to control access to your network. For example, you could create an enforcement policy that grants endpoints profiled as VoIP phones access to specific servers in your network. Or you could create an enforcement policy that places all endpoints profiled as access points in a specific VLAN.

A device profile classifies an endpoint according to the following three hierarchical elements:

- Category—This is the broadest classification of a device. It denotes the type of the device—for example, access point, VoIP phone, printer, computer, or smart device.
- Family—Devices within a category are organized into families based on type of OS or type of vendor. For example, when the device category is computer, the family might be Windows, Linux, or Mac OS X. When the device category is smart device, the family might be Apple or Android.
- Name—Devices within a family are further organized by more granular details, such as version. For example, when the device family is Windows, the device name might be Windows 7 or Windows 2008 server.

In addition to the hierarchical classification above, a device profile can contain information such as IP address, hostname, vendor, and time when the device was first discovered or when it was last seen.

To profile devices, Aruba ClearPass Profile uses a number of different types of collectors to collect data on endpoints. For a complete list of the kinds of collectors used, see the Aruba ClearPass documentation. This network configuration example relies on data provided by the DHCP and MAC Organizationally Unique Identitier (OUI) collectors:

- DHCP collector—Collects DHCP attributes such as option55 (parameter request list), option60 (vendor class), and options list from DHCPDiscover and DHCPRequest packets. This information can uniquely fingerprint most endpoints that use DHCP to acquire an IP address on the network. DHCP packets also provide the hostname and IP address of a device.

  For the DHCP collector to be able to collect this information, Aruba ClearPass must receive DHCP packets from the endpoints. DHCP relay on EX Series switches allows a switch to send the initial DHCPDiscover and DHCPRequest packets from endpoints to more than one receiver. Configuring ClearPass as one of these receivers allows ClearPass to listen in on the DHCP message exchange between the DHCP servers and client endpoints and to collect the required information from the DHCP packets.
- MAC OUI collector—Collects the OUI portion of a device's MAC address. The MAC OUI can be used to better classify some endpoints. For example, DHCP fingerprinting can classify an endpoint as a generic Android device, but it cannot provide information

about the vendor. By using the MAC OUI in addition to DHCP fingerprinting, ClearPass Profile can classify an Android device as an HTC Android device, a Samsung Android device, a Motorola Android device, and so on. ClearPass Profile can also use the MAC OUI to profile devices such as printers that might have static IP addresses.

The MAC OUI collector obtains the MAC OUI from the MAC address information included in the RADIUS request packets sent from the EX Series switch on behalf of the endpoint.

Related Documentation

- Example: Configuring Device Profiling with EX Series Switches and Aruba ClearPass Policy Manager on page 8
- Monitoring Device Profiling on page 36
- Troubleshooting Authentication on page 38
- Use Case Overview on page 6

Example: Configuring Device Profiling with EX Series Switches and Aruba ClearPass Policy Manager

This configuration example illustrates how to use the features of EX Series switches and Aruba ClearPass Policy Manager to perform device profiling as part of the endpoint authentication process.

In this example, an organization has four types of endpoints in its wired infrastructure for which it has defined access policies:

- Access points—Endpoints profiled as access points are allowed access to the network and are dynamically assigned to the AP_VLAN VLAN.
- IP phones—Endpoints profiled as IP phones are allowed access to the network. The IPPhone_VLAN is dynamically assigned as the VoIP VLAN.
- Corporate laptops—Endpoints that have an 802.1X supplicant are authenticated by the user credentials. After the user is successfully authenticated, the laptop is granted access to the network and placed in the Windows_VLAN VLAN.
- Noncorporate laptops—Endpoints that do not have an 802.1X supplicant and that are profiled as Windows devices are denied access to the network.

This topic covers:

- Requirements on page 9
- Overview and Topology on page 9
- Configuration on page 10
- Verification on page 30

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

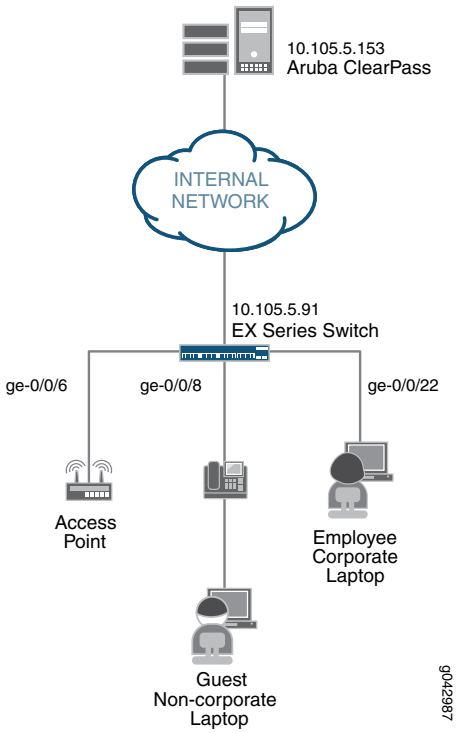
To implement the endpoint access policies, the policy infrastructure is configured as follows:

- All access interfaces on the switch are initially configured to be in VLAN 100, which serves as a remediation VLAN. If an endpoint is not successfully authenticated or is not successfully profiled as one of the supported endpoints, it remains in the remediation VLAN.
- Endpoints that have an 802.1X supplicant are authenticated by using 802.1X PEAP authentication. For more information on 802.1X PEAP authentication, see *Configuring 802.1X PEAP and MAC RADIUS Authentication with EX Series Switches and Aruba ClearPass Policy Manager*.
- Endpoints that do not have an 802.1X supplicant are authenticated using MAC RADIUS authentication and are profiled to determine what type of device they are. These endpoints undergo a two-step authentication process:

  1. The first step occurs after an endpoint first connects to the switch but before it has been profiled by Aruba ClearPass Profile. After it connects, the endpoint is authenticated using MAC RADIUS authentication. Aruba ClearPass applies an enforcement policy that instructs the switch to grant the endpoint access to the Internet but prevents it from accessing the internal network.
  2. The second step occurs after an endpoint has been successfully profiled. After being authenticated in the first step, the endpoint contacts a DHCP server to request an IP address. The switch relays the DHCP messages sent by the endpoint to the DHCP server to Aruba ClearPass as well, which allows ClearPass to profile the endpoint. After it has profiled the endpoint and added the endpoint to its endpoint repository, ClearPass sends a RADIUS Change of Authorization (CoA) message to the switch, telling it to terminate the session. The switch then attempts reauthentication on behalf of the endpoint. Because the endpoint now exists in the endpoint repository, Aruba ClearPass is able to apply an enforcement policy appropriate to the device type when it authenticates the endpoint. For example, if the endpoint is an access point, ClearPass applies the enforcement policy that dynamically assigns the access point to the AP_VLAN VLAN.

Figure 1 on page 10 shows the topology used in this example.

Figure 1: Topology Used in This Example



Configuration

This section provides step-by-step instructions for:

- Configuring the EX4300 Switch on page 10
- Configuring Aruba ClearPass Policy Manager on page 18

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 protocols dot1x authenticator authentication-profile-name CP-Test-Profile
set protocols dot1x authenticator interface ge-0/0/6.0 mac-radius
set protocols dot1x authenticator interface ge-0/0/6.0 supplicant multiple
set protocols dot1x authenticator interface ge-0/0/8.0 mac-radius
```

```
set protocols dot1x authenticator interface ge-0/0/8.0 supplicant multiple
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 AP_VLAN vlan-id 130
set vlans IPPhone_VLAN vlan-id 120
set vlans Windows_VLAN vlan-id 150
set vlans v100 description "Remediation VLAN"
set vlans v100 vlan-id 100
set interfaces ge-0/0/6 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/6 unit 0 family ethernet-switching vlan members v100
set interfaces ge-0/0/8 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/8 unit 0 family ethernet-switching vlan members v100
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 interfaces irb unit 100 family inet address 10.10.100.1/24
set interfaces irb unit 120 family inet address 10.10.120.1/24
set interfaces irb unit 130 family inet address 10.10.130.1/24
set interfaces irb unit 150 family inet address 10.10.150.1/24
set vlans AP_VLAN l3-interface irb.130
set vlans IPPhone_VLAN l3-interface irb.120
set vlans Windows_VLAN l3-interface irb.150
set vlans v100 l3-interface irb.100
set forwarding-options dhcp-relay server-group dhcp-dot1x 10.10.10.10
set forwarding-options dhcp-relay server-group dhcp-dot1x 10.105.5.153
set forwarding-options dhcp-relay active-server-group dhcp-dot1x
set forwarding-options dhcp-relay group all interface irb.100
set forwarding-options dhcp-relay group all interface irb.120
set forwarding-options dhcp-relay group all interface irb.130
set forwarding-options dhcp-relay group all interface irb.150
set firewall family ethernet-switching filter Internet_Only_Access term Allow_DHCP
from destination-port 67
set firewall family ethernet-switching filter Internet_Only_Access term Allow_DHCP
from destination-port 68
set firewall family ethernet-switching filter Internet_Only_Access term Allow_DHCP
from ip-protocol udp
set firewall family ethernet-switching filter Internet_Only_Access term Allow_DHCP
then accept
set firewall family ethernet-switching filter Internet_Only_Access term Allow_DNS from
 destination-port 53
set firewall family ethernet-switching filter Internet_Only_Access term Allow_DNS from
 ip-protocol udp
set firewall family ethernet-switching filter Internet_Only_Access term Allow_DNS from
 ip-protocol tcp
set firewall family ethernet-switching filter Internet_Only_Access term Block_Internal
from ip-destination-address 192.168.0.0/16
set firewall family ethernet-switching filter Internet_Only_Access term Block_Internal
then discard
set firewall family ethernet-switching filter Internet_Only_Access 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 and authentication methods to use and the order of the authentication methods.
- Configure the 802.1X protocol.
- Configure the VLANs.
- Configure Ethernet switching on the access ports.
- Configure integrated routing and bridging (IRB) interfaces and assign them to the VLANs.
- Configure DHCP relay to send DHCP packets to Aruba ClearPass so that it can perform device profiling.
- 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@Policy-EX4300-01# set radius-server 10.105.5.153 dynamic-request-port
3799
user@Policy-EX4300-01# set radius-server 10.105.5.153 secret password
user@Policy-EX4300-01# set radius-server 10.105.5.153 source-address 10.105.5.91
```

2. Configure the access profile.

```
[edit access]
user@Policy-EX4300-01# set profile CP-Test-Profile accounting-order radius
user@Policy-EX4300-01# set profile CP-Test-Profile authentication-order radius
user@Policy-EX4300-01# set profile CP-Test-Profile radius authentication-server
 10.105.5.153
user@Policy-EX4300-01# set profile CP-Test-Profile radius accounting-server
10.105.5.153
user@Policy-EX4300-01# set profile CP-Test-Profile radius options nas-identifier
 10.105.5.91
```

3. Configure 802.1X 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, it then tries MAC RADIUS authentication.

```
[edit protocols]
user@Policy-EX4300-01# set dot1x authenticator authentication-profile-name
CP-Test-Profile
user@Policy-EX4300-01# set dot1x authenticator interface ge-0/0/6.0 mac-radius
user@Policy-EX4300-01# set dot1x authenticator interface ge-0/0/6.0 supplicant
 multiple
```

```
user@Policy-EX4300-01# set dot1x authenticator interface ge-0/0/8.0 mac-radius
user@Policy-EX4300-01# set dot1x authenticator interface ge-0/0/8.0 supplicant
 multiple
user@Policy-EX4300-01# set dot1x authenticator interface ge-0/0/22.0
mac-radius
user@Policy-EX4300-01# set dot1x authenticator interface ge-0/0/22.0 supplicant
 multiple
```

4. Configure the VLANs used in this example.

```
[edit vlans]
user@Policy-EX4300-01# set AP_VLAN vlan-id 130
user@Policy-EX4300-01# set IPPhone_VLAN vlan-id 120
user@Policy-EX4300-01# set Windows_VLAN vlan-id 150
user@Policy-EX4300-01# set v100 description "Remediation VLAN"
user@Policy-EX4300-01# set v100 vlan-id 100
```

   Note that for dynamic VLAN assignment to work, the VLAN must exist on the switch before authentication is attempted. If the VLAN doesn't exist, authentication fails.

5. Configure the access ports.

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

```
[edit interfaces]
user@Policy-EX4300-01# set ge-0/0/6 unit 0 family ethernet-switching
interface-mode access
user@Policy-EX4300-01# set ge-0/0/6 unit 0 family ethernet-switching vlan
members v100
user@Policy-EX4300-01# set ge-0/0/8 unit 0 family ethernet-switching
interface-mode access
user@Policy-EX4300-01# set ge-0/0/8 unit 0 family ethernet-switching vlan
members v100
user@Policy-EX4300-01# set ge-0/0/22 unit 0 family ethernet-switching
interface-mode access
user@Policy-EX4300-01# set ge-0/0/22 unit 0 family ethernet-switching vlan
members v100
```

6. Configure IRB interfaces and assign them to the VLANs.

```
[edit interfaces]
user@Policy-EX4300-01# set irb unit 100 family inet address 10.10.100.1/24
user@Policy-EX4300-01# set irb unit 120 family inet address 10.10.120.1/24
user@Policy-EX4300-01# set irb unit 130 family inet address 10.10.130.1/24
user@Policy-EX4300-01# set irb unit 150 family inet address 10.10.150.1/24

[edit vlans]
user@Policy-EX4300-01# set v100 l3-interface irb.100
user@Policy-EX4300-01# set IPPhone_VLAN l3-interface irb.120
user@Policy-EX4300-01# set AP_VLAN l3-interface irb.130
user@Policy-EX4300-01# set Windows_VLAN l3-interface irb.150
```

7. Configure DHCP relay to forward DHCP request packets to Aruba ClearPass.

```
[edit forwarding-options]
user@Policy-EX4300-01# set dhcp-relay server-group dhcp-dot1x 10.10.10.10
user@Policy-EX4300-01# set dhcp-relay server-group dhcp-dot1x 10.105.5.153
```

```
user@Policy-EX4300-01# set dhcp-relay active-server-group dhcp-dot1x
user@Policy-EX4300-01# set dhcp-relay group all interface irb.100
user@Policy-EX4300-01# set dhcp-relay group all interface irb.120
user@Policy-EX4300-01# set dhcp-relay group all interface irb.130
user@Policy-EX4300-01# set dhcp-relay group all interface irb.150
```

NOTE: In this configuration example, Layer 3 interfaces for the endpoint VLANs are configured on the access switch in order to demonstrate the DHCP relay configuration. In a typical enterprise deployment, however, the Layer 3 interfaces for the endpoint VLANs are configured on an aggregation or core layer switch. In such a deployment, DHCP relay on the aggregation or core switch should be configured to forward the DHCP requests from the endpoints to Aruba ClearPass.

8. Configure a firewall filter, Internet_Only_Access, to be used for devices that have been authenticated by MAC RADIUS authentication but have not yet been profiled.

   This filter blocks an endpoint from accessing the internal network (192.168.0.0/16).

```
[edit firewall]
user@Policy-EX4300-01# set family ethernet-switching filter Internet_Only_Access
 term Allow_DHCP from destination-port 67
user@Policy-EX4300-01# set family ethernet-switching filter Internet_Only_Access
 term Allow_DHCP from destination-port 68
user@Policy-EX4300-01# set family ethernet-switching filter Internet_Only_Access
 term Allow_DHCP from ip-protocol udp
user@Policy-EX4300-01# set family ethernet-switching filter Internet_Only_Access
 term Allow_DHCP then accept
user@Policy-EX4300-01# set family ethernet-switching filter Internet_Only_Access
 term Allow_DNS from destination-port 53
user@Policy-EX4300-01# set family ethernet-switching filter Internet_Only_Access
 term Allow_DNS from ip-protocol udp
user@Policy-EX4300-01# set family ethernet-switching filter Internet_Only_Access
 term Allow_DNS from ip-protocol tcp
user@Policy-EX4300-01# set family ethernet-switching filter Internet_Only_Access
 term Block_Internal from ip-destination-address 192.168.0.0/16
user@Policy-EX4300-01# set family ethernet-switching filter Internet_Only_Access
 term Block_Internal then discard
user@Policy-EX4300-01# set family ethernet-switching filter Internet_Only_Access
 term Allow_All then accept
```

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

```
user@Policy-EX4300-01# show access
radius-server {
    10.105.5.153 {
        dynamic-request-port 3799;
        secret "$9$FYxf3A0Ehrv87yl7Vs4DjfTz3Ct0BIcre"; ## 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@Policy-EX4300-01# show protocols
dot1x {
    authenticator {
        authentication-profile-name CP-Test-Profile;
        interface {
            ge-0/0/6.0 {
               supplicant multiple;
               mac-radius;
            }
            ge-0/0/8.0 {
                supplicant multiple;
                mac-radius;
            }
            ge-0/0/22.0 {
                supplicant multiple;
                mac-radius;
             }
        }
    }
}

user@Policy-EX4300-01# show interfaces
ge-0/0/6 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members v100;
            }
        }
    }
}
ge-0/0/8 {
    unit 0 {
        family ethernet-switching;
            vlan {
                members v100;
            }
        }
    }
}
ge-0/0/22 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members v100;
            }
        }
    }
}
irb {
```

```
    unit 100 {
        family inet {
            address 10.10.100.1/24;
        }
    }
    unit 120 {
        family inet {
            address 10.10.120.1/24;
        }
    }
    unit 130 {
        family inet {
            address 10.10.130.1/24;
        }
    }
    unit 150 {
        family inet {
            address 10.10.150.1/24;
        }
    }
}


user@Policy-EX4300-01# show vlans
AP_VLAN {
    vlan-id 130;
    l3-interface irb.130;
}
IPPhone_VLAN {
    vlan-id 120;
    l3-interface irb.120;
}
Windows_VLAN {
    vlan-id 150;
    l3-interface irb.150;
}
v100 {
    description "Remediation VLAN";
    vlan-id 100;
    l3-interface irb.100;
}


user@Policy-EX4300-01# show forwarding-options
dhcp-relay {
    server-group {
        dhcp-dot1x {
            10.10.10.10;
            10.105.5.153;
        }
    }
    active-server-group dhcp-dot1x;
    group all {
        interface irb.100;
        interface irb.120;
        interface irb.130;
        interface irb.150;
    }
}
```

```
user@Policy-EX4300-01# show firewall
family ethernet-switching {
    filter Internet_Only_Access {
        term Allow_DHCP {
            from {
                destination-port [ 67 68 ];
                ip-protocol udp;
            }
            then accept;
        }
        term Allow_DNS {
            from {
                destination-port 53;
                ip-protocol [ udp tcp ];
            }
        }
        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 Policy Manager

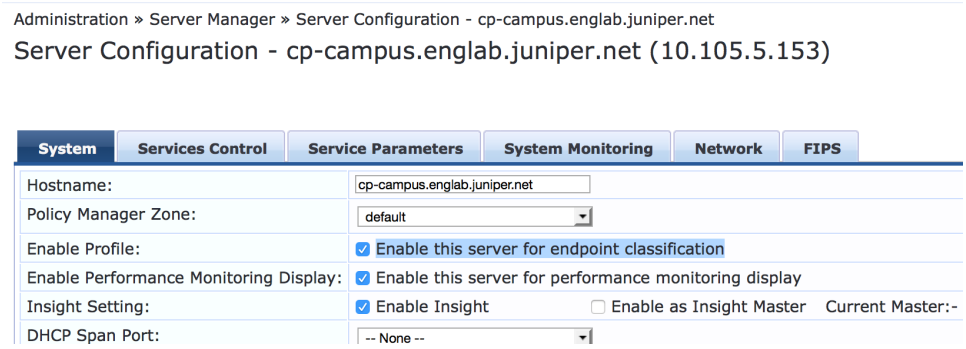
Step-by-Step Procedure

The general steps for configuring Aruba ClearPass are:

- Enable device profiling.
- Modify the Juniper Networks RADIUS dictionary file so that it includes some additional Juniper Networks RADIUS attributes used in this configuration example.
- Add the EX4300 as a network device.
- Ensure that the server certificate used for 802.1X PEAP authentication has been installed.
- Add the local user used in this example for 802.1X authentication.
- Create the following enforcement profiles:
  - Employee_Windows_Profile that places endpoints in VLAN 150.
  - IPPhone_Profile that defines VLAN 120 as the VoIP VLAN.
  - AccessPoint_Profile that places endpoints in VLAN 130.
  - Internet_Access_Only_Profile that specifies the firewall filter Internet_Only_Access be used for devices that have not yet been profiled.
- Create two enforcement policies:
  - A policy that is invoked when MAC RADIUS authentication is used.
  - A policy that is invoked when 802.1X authentication is used.
- Define the MAC RADIUS authentication service and the 802.1X authentication service.
- Ensure that the MAC RADIUS authentication service is evaluated before the 802.1X authentication service.

To configure Aruba ClearPass:

1. Enable device profiling.
   a. Under Administration > Server Manager > Server Configuration, click the name of the Aruba ClearPass server.
   b. In the System tab, click **Enable this server for endpoint classification**.



2. Update the Juniper Networks RADIUS dictionary file.

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

   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** and save the **RadiusDictionary.xml** file to your desktop.

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

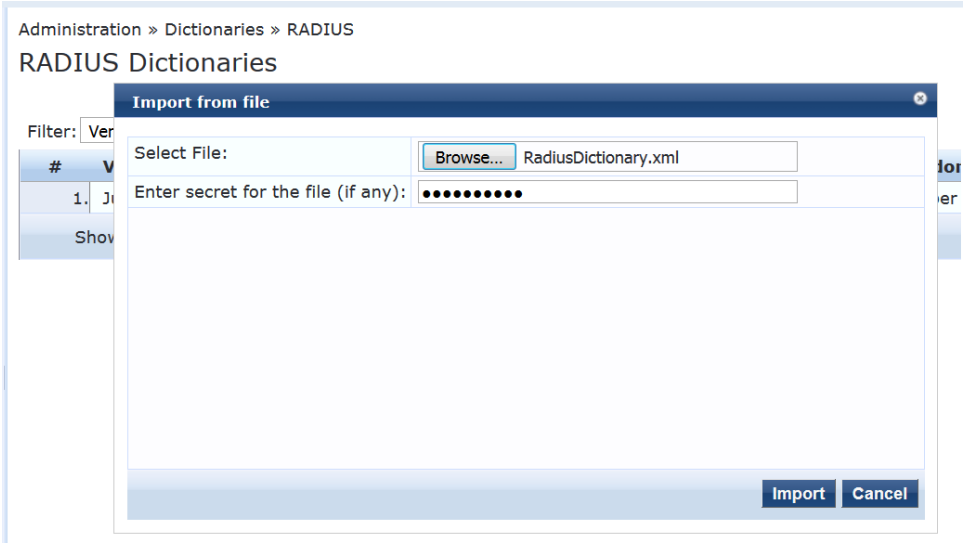
```
<Attribute profile="in out" type="String" name="Juniper-CWA-Redirect-URL"
id="50" />
<Attribute profile="in out" type="String" name="Juniper-Switching-Filter"
```

```
id="48" />
<Attribute profile="in out" type="String" name="Juniper-VoIP-Vlan" id="49"
/>
```

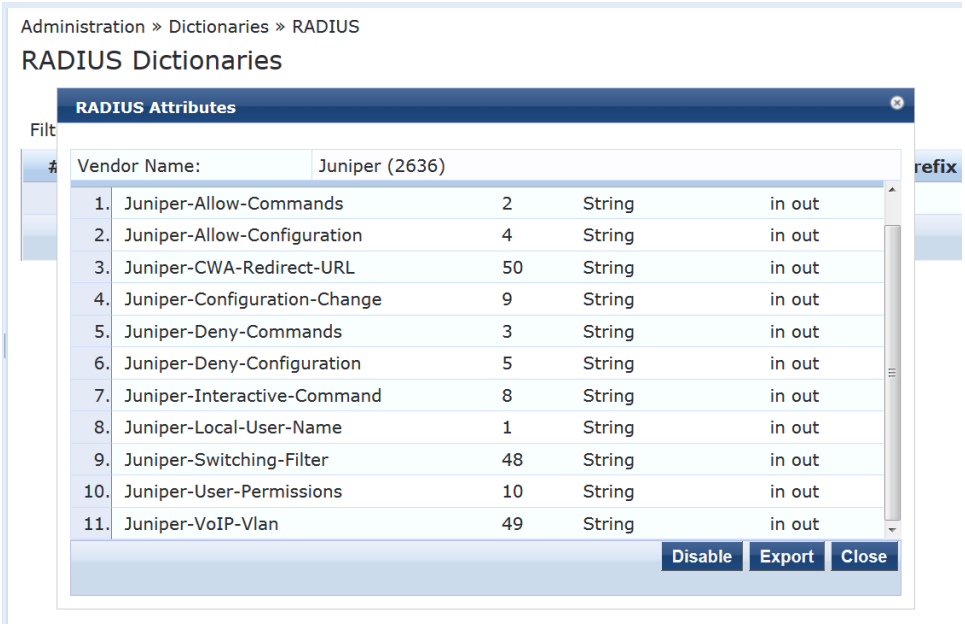
The dictionary file should look like this when you complete the paste:

```
<?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 **RadiusDictionary.xml** into Aruba ClearPass by clicking Import in the RADIUS Dictionaries window and browsing to the file.

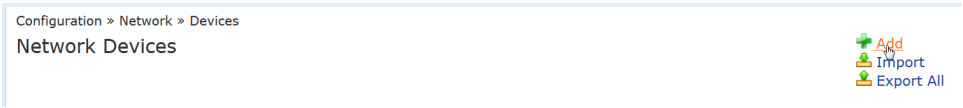


f. After you have imported the file, the Juniper dictionary file should look like this:

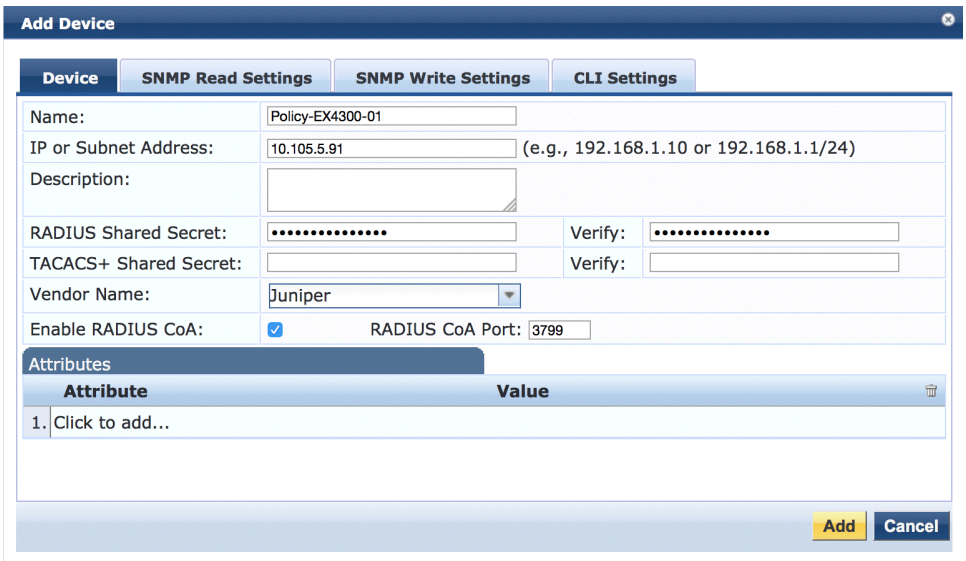


3. Add the EX4300 switch as a network device.

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

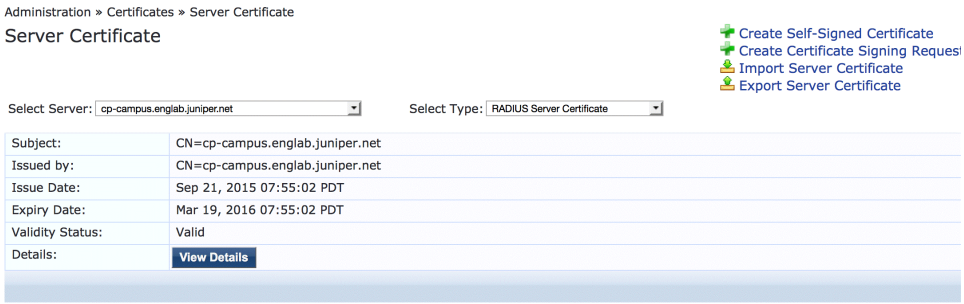


   b. On the Device tab, enter the hostname and IP address of the switch and the RADIUS shared secret that you configured on the switch. Set the Vendor Name field to **Juniper**.



4. Ensure that a server certificate for 802.1X PEAP authentication exists.

Under Administration > Certificates > Server Certificate, verify that Aruba ClearPass has a valid server certificate installed. If it does not, add a valid server certificate. The Aruba ClearPass documentation and your Certificate Authority can provide more details on how to obtain certificates and import them into ClearPass.

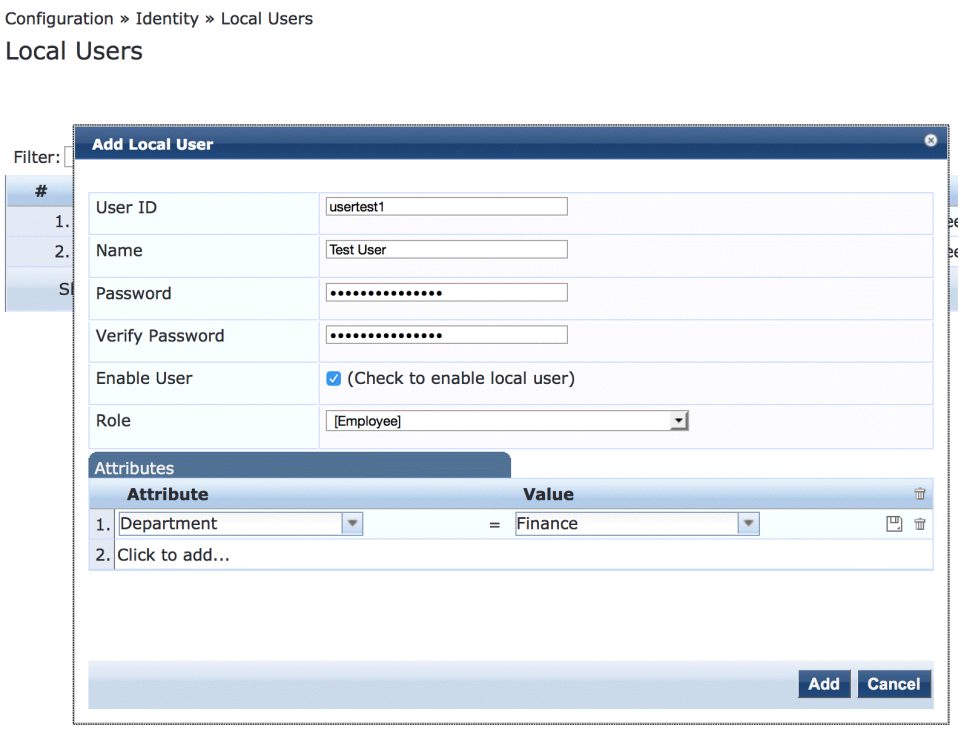


5. Add a test user to the local user repository.

   This user will be used to verify 802.1X authentication.

   a. Under Configuration > Identity > Local Users, click **Add**.

   b. In the Add Local User window, enter the user ID (**usertest1**), username (**Test User**), and password. Then select **Employee** as the user role. Under Attributes, select the **Department** attribute and type **Finance** under Value.

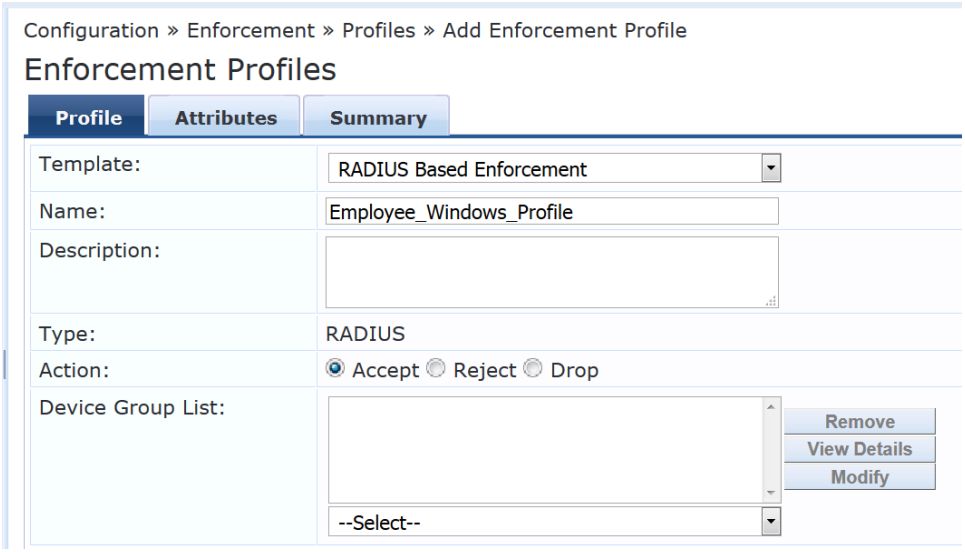


6. Configure an enforcement profile for employee Windows laptops or desktops that authenticate using 802.1X.

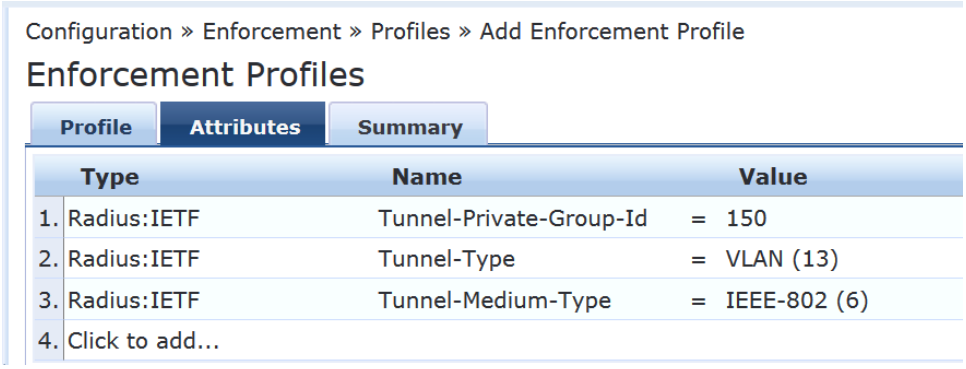
This profile places the endpoints in VLAN 150.

a. Under Configuration > Enforcement > Profiles, click **Add**.

b. On the Profile tab, set Template to **RADIUS Based Enforcement** and type the profile name, **Employee_Windows_Profile**, in the Name field.



c. On the Attributes tab, configure the attributes as shown.



7. Configure an access point enforcement profile, which places access points in VLAN 130.

   Use the same basic procedure to create this profile as you used in the previous step. After you complete the profile, the information on the Summary tab will appear as shown.

Configuration » Enforcement » Profiles » Edit Enforcement Profile - AccessPoint_Profile

Enforcement Profiles - AccessPoint_Profile

Summary | Profile | Attributes

Profile:

Name:	AccessPoint_Profile
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
2.	Radius:IETF	Tunnel-Private-Group-Id	=	130
3.	Radius:IETF	Tunnel-Type	=	VLAN (13)

8. Configure an IP phone enforcement profile.

   This profile instructs Aruba ClearPass to return VLAN 120 as the VLAN that should be used as the VoIP VLAN. The Juniper Networks RADIUS dictionary defines a special RADIUS attribute to use for this purpose. Select **RADIUS-Juniper** for the attribute type and **Juniper-VoIP-Vlan** as the attribute name.

   After you complete the profile, the information on the Summary tab will appear as shown.

Configuration » Enforcement » Profiles » Edit Enforcement Profile - IPPhone_Profile

Enforcement Profiles - IPPhone_Profile

Summary | Profile | Attributes

Profile:

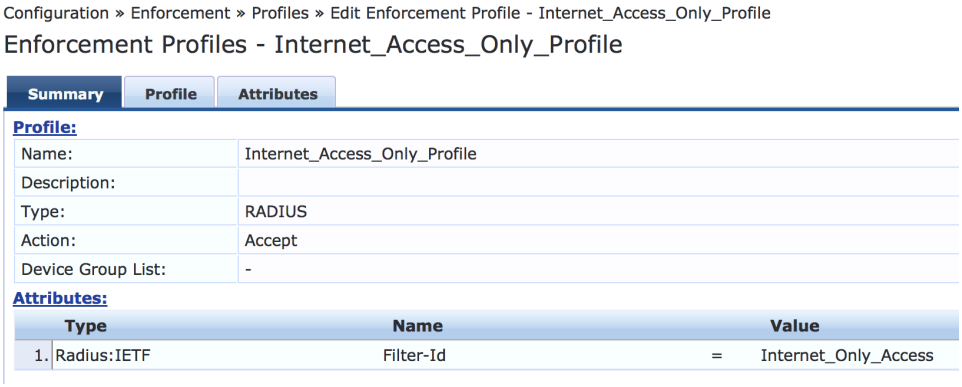
Name:	IPPhone_Profile
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Juniper	Juniper-VoIP-Vlan	=	120

9. Configure an Internet access only enforcement profile.

   This enforcement profile tells Aruba ClearPass to return the name of the firewall filter Internet_Only_Access, which is the firewall filter you configured on the switch that blocks access to the internal network. After you complete this profile, the information on the Summary tab will appear as shown.

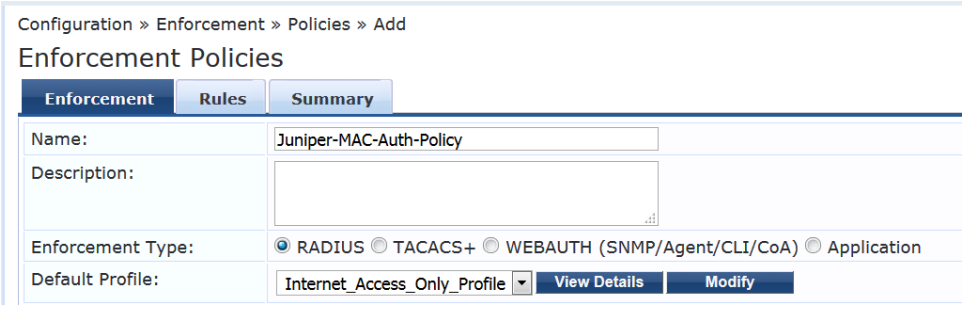


10. Configure the MAC RADIUS authentication enforcement policy.

    For endpoints being authenticated by MAC RADIUS authentication, this policy tells Aruba ClearPass to apply enforcement policies according to the device profile. The AccessPoint_Profile is applied to endpoints profiled as access points, and the IPPhone_Profile is applied to endpoints profiled as VoIP phones. The predefined enforcement policy Deny Access Profile is applied to endpoints profiled as Windows devices. This enforces the organization access policy that only laptops with an 802.1X supplicant are allowed access to the network. For all other endpoints, including endpoints that have not yet been profiled, the Internet_Access_Only profile will be applied.

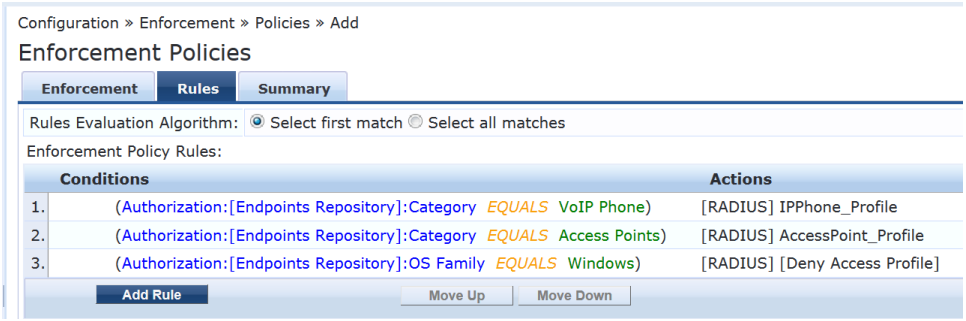
    a. Under Configuration > Enforcement > Policies, click **Add**.

    b. On the Enforcement tab, type the name of the policy (**Juniper-MAC-Auth-Policy**) and set Default Profile to **Internet_Access_Only**.



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

       You must add the rules sequentially by clicking **Save** before you create the next rule.

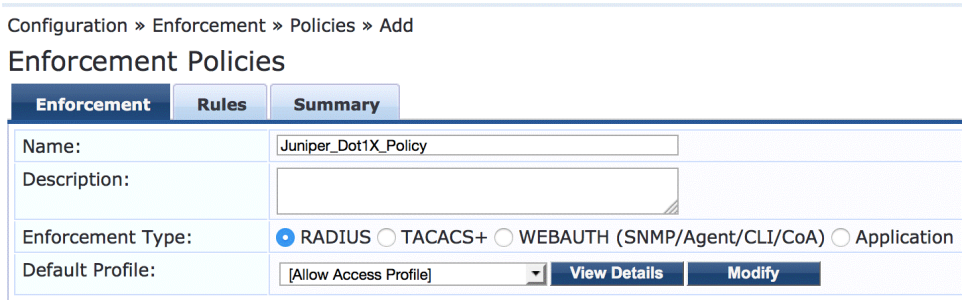


11. Configure the 802.1X enforcement policy.

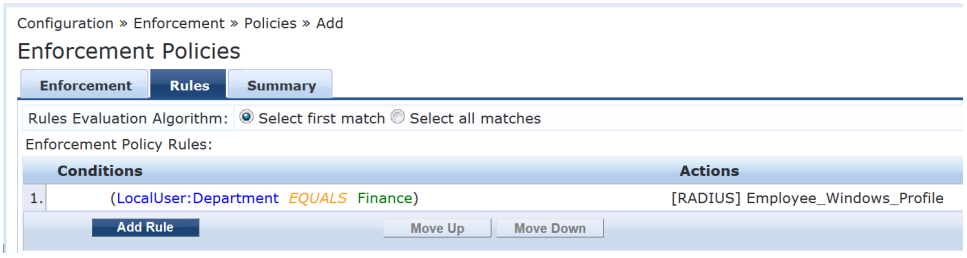
    This policy tells Aruba ClearPass to use the Employee_Windows_Profile enforcement profile if a user is successfully authenticated as a member of the finance department.

    a. Under Configuration > Enforcement > Policies, click **Add**.

    b. On the Enforcement tab, type the name of the policy (**Juniper_Dot1X_Policy**) and set Default Profile to **[Allow Access Profile]**. (This is a predefined profile.)



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

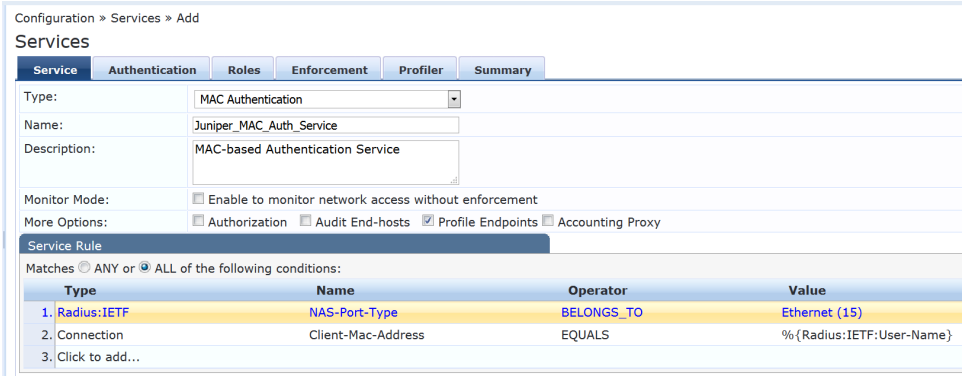


12. Configure the MAC RADIUS authentication service.

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.

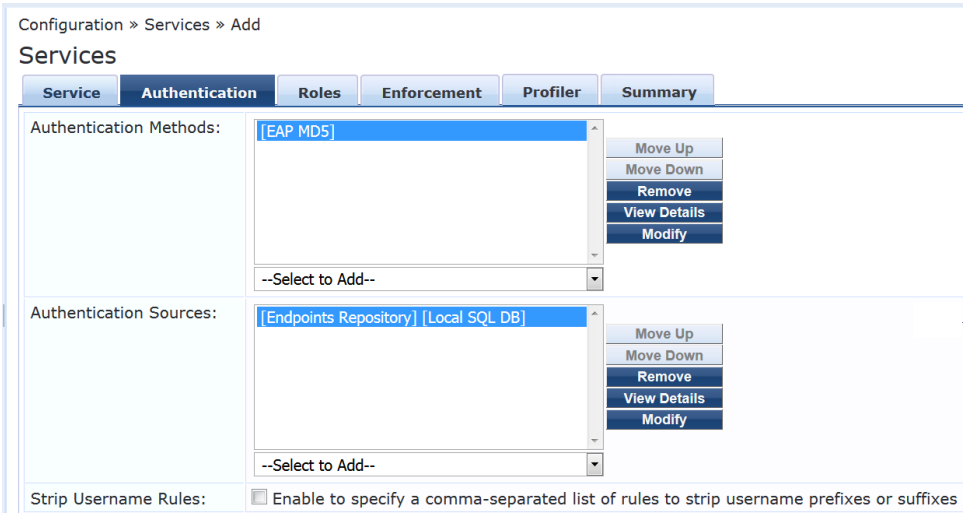
a. Under Configuration > Services, click **Add**.

b. On the Services tab, fill out the fields as shown. Be sure to select the **Profile Endpoints** option.

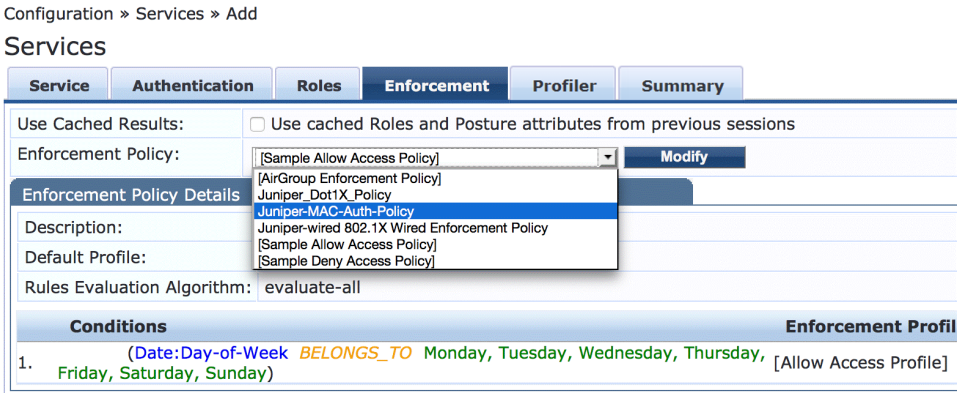


c. On the Authentication tab:

- 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.



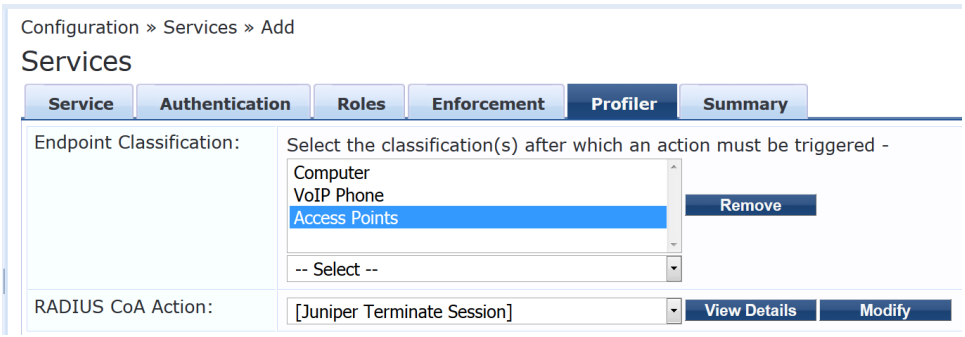
d. On the Enforcement tab, select **Juniper-MAC-Auth-Policy**.



e. On the Profiler tab:

- Add **Computer**, **VoIP Phone**, **Access Points** to the Endpoint Classification list.
- Select **[Juniper Terminate Session]** from the RADIUS CoA Action list.

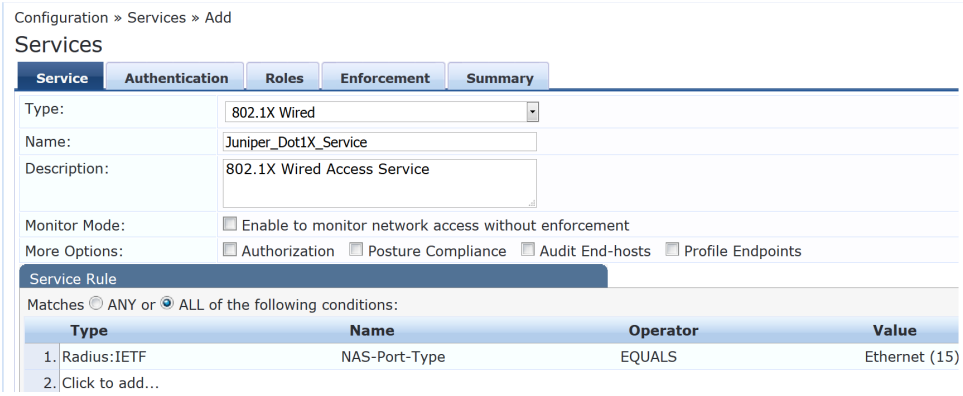
This configuration causes endpoints to go through reauthentication after they are profiled and added to the endpoint repository. Before an endpoint is profiled, the Internet_Access_Only_Profile enforcement profile is in effect for the authenticated user session. (This profile is the default profile for the MAC authentication policy configured in Step 10.) After Aruba ClearPass successfully classifies a device, it sends a RADIUS CoA to the switch, which causes the switch to terminate the session. The switch then attempts to reauthenticate the endpoint. Because the endpoint's device profile is now in the endpoint repository, the appropriate device enforcement profile will be applied when the endpoint is authenticated.



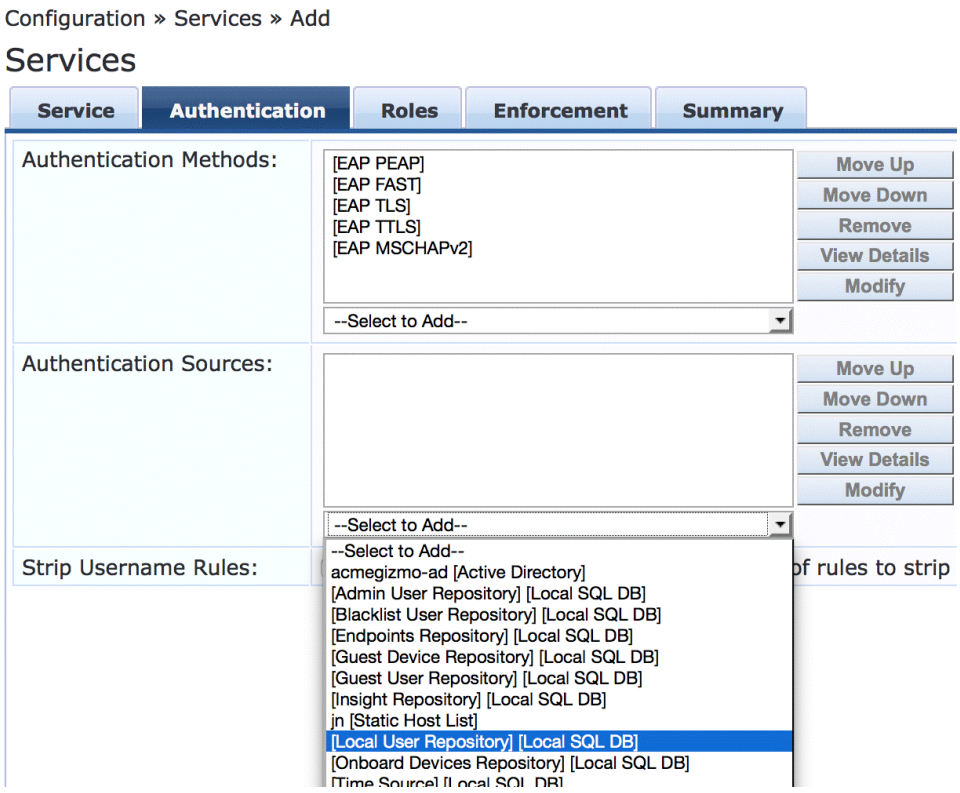
13. Configure the 802.1X authentication service.

a. Under Configuration > Services, click **Add**.

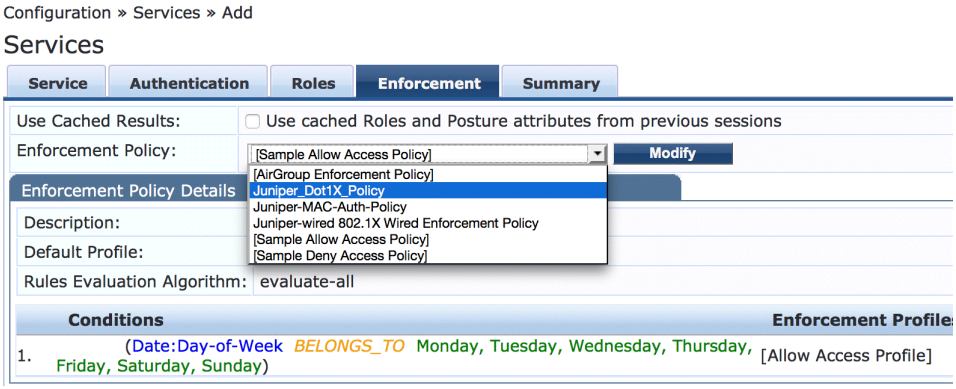
b. On the Service tab, fill out the fields as shown.



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



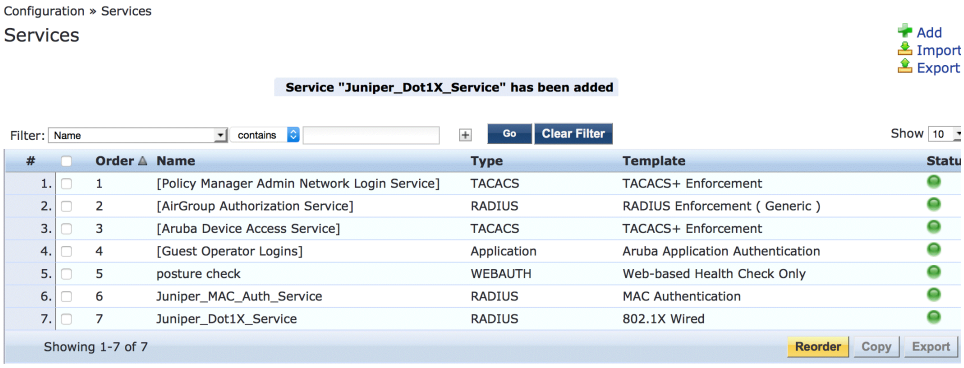
d. On the Enforcement tab, set Enforcement Policy to **Juniper_Dot1X_Policy**.



14. Verify that the MAC RADIUS authentication service policy is evaluated before the 802.1X authentication service policy.

    Because Aruba ClearPass is configured to recognize MAC RADIUS authentication requests by the RADIUS User-Name attribute and the Client-MAC-Address attribute having the same value, it is more efficient to have the MAC RADIUS service policy evaluated first.

    In the Services main window, verify that **Juniper-MAC-Auth-Policy** appears before **Juniper-MAC_Dot1X_Policy** in the services list, as shown. If it does not, click **Reorder** and move **Juniper-MAC-Auth-Policy** above **Juniper-MAC_Dot1X_Policy**.



Verification

Confirm that the configuration is working properly.

- Verifying 802.1X Authentication on the EX4300 Switch on page 30
- Verifying the Access Point Authentication on the EX4300 Switch on page 31
- Verifying the VoIP Phone and Non-corporate Laptop Authentication on the EX4300 Switch on page 32
- Verifying the Status of Authentication Requests on Aruba ClearPass Policy Manager on page 34

Verifying 802.1X Authentication on the EX4300 Switch

Purpose Verify that the test user, usertest1, is being authenticated and placed in the correct VLAN.

To perform this procedure, you must have a Windows device with an active 802.1X supplicant that passes the authentication information for usertest1. For information on how to configure a Windows 7 supplicant for 802.1X PEAP authentication, see *Configuring 802.1X PEAP and MAC RADIUS Authentication with EX Series Switches and Aruba ClearPass Policy Manager*.

Action

1. Connect the Windows 7 laptop to ge-0/0/22 on the EX4300 switch.
2. On the switch, type the following command:

```
user@Policy-EX4300-01> show dot1x interface ge-0/0/22.0
802.1X Information:
Interface    Role       State       MAC address       User
ge-0/0/22.0  Authenticator Authenticated 00:50:56:9B:03:7F  usertest1
```

3. For more details, including the dynamic VLAN assignment, type:

```
user@Policy-EX4300-01> show dot1x interface ge-0/0/22.0 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: Disabled
  Mac Radius Restrict: Disabled
  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: usertest1, 00:50:56:9B:03:7F
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Radius
      Authenticated VLAN: Windows_VLAN
      Session Reauth interval: 3600 seconds
      Reauthentication due in 2682 seconds
      Session Accounting Interim  Interval: 600 seconds
      Accounting Update  due in 282 seconds
```

The output shows that usertest1 has been successfully authenticated and placed in Windows_VLAN VLAN.

Verifying the Access Point Authentication on the EX4300 Switch

Purpose Verify that the access point has been successfully authenticated and placed in the correct VLAN.

Action

1. Connect an access point to ge-0/0/6 on the EX4300 switch.
2. On the switch, type the following command:

```
user@Policy-EX4300-01> show dot1x interface ge-0/0/6
ge-0/0/6.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  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: c46413c07cda, C4:64:13:C0:7C:DA
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Mac Radius
      Authenticated VLAN: AP_VLAN
      Session Reauth interval: 3600 seconds
      Reauthentication due in 1669 seconds
      Session Accounting Interim  Interval: 600 seconds
      Accounting Update  due in 379 seconds
```

The output shows that the access point has been authenticated and placed in the AP_VLAN VLAN.

Verifying the VoIP Phone and Non-corporate Laptop Authentication on the EX4300 Switch

Purpose Verify that the VoIP phone has been successfully authenticated and that the non-corporate laptop has not been authenticated.

Action

1. Connect a VoIP phone to ge-0/0/8 on the EX4300 switch, and connect a laptop that does not have an enabled 802.1X supplicant to the Ethernet port on the phone.

2. To verify the authentication state of the devices, type the following command on the switch:

```
user@Policy-EX4300-01> show dot1x interface ge-0/0/8
ge-0/0/8.0
  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: 2
    Supplicant: 08173515ec53, 08:17:35:15:EC:53
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Mac Radius
     Authenticated VLAN: IPPhone_VLAN
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3591 seconds
      Session Accounting Interim  Interval: 600 seconds
      Accounting Update  due in 591 seconds
    Supplicant: No User, D0:67:E5:50:E3:DD
      Operational state: Connecting
      Backend Authentication state: Idle
      Authentication method: None
      Session Reauth interval: 0 seconds
      Reauthentication due in 0 seconds
      Session Accounting Interim  Interval: 600 seconds
      Accounting Update  due in 0 seconds
```

The output shows that two supplicants are attached to the port, each identified by MAC address. The VoIP phone has been successfully authenticated and placed in IPPhone_VLAN. The laptop is in a connecting state, not authenticated state, indicating that it has failed to be authenticated.

3. To verify that IPPhone_VLAN VLAN has been assigned as the VoIP VLAN, type the following command:

```
user@Policy-EX4300-01> show ethernet-switching interface ge-0/0/8
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down,
                         MMAS - Mac-move action shutdown,
                         SCTL - shutdown by Storm-control )

Logical     Vlan         TAG  MAC    STP       Logical         Tagging
interface   members           limit  state     interface flags
ge-0/0/8.0                   65535                            tagged,untagged
```

```
default      1    65535  Forwarding                untagged
IPPhone_VLAN 120  65535  Forwarding                tagged
```

IPPhone_VLAN is shown as a tagged VLAN, indicating that it is the VoIP VLAN.

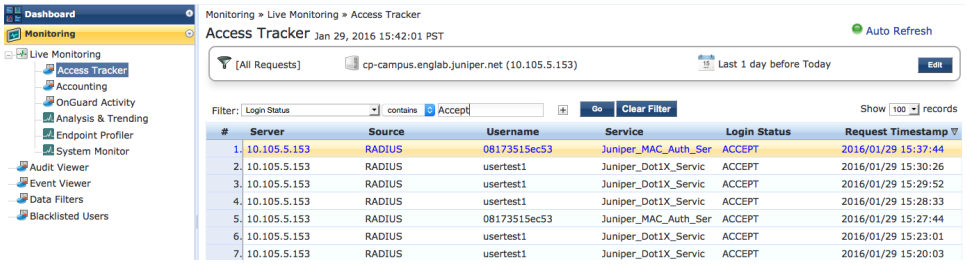
Verifying the Status of Authentication Requests on Aruba ClearPass Policy Manager

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

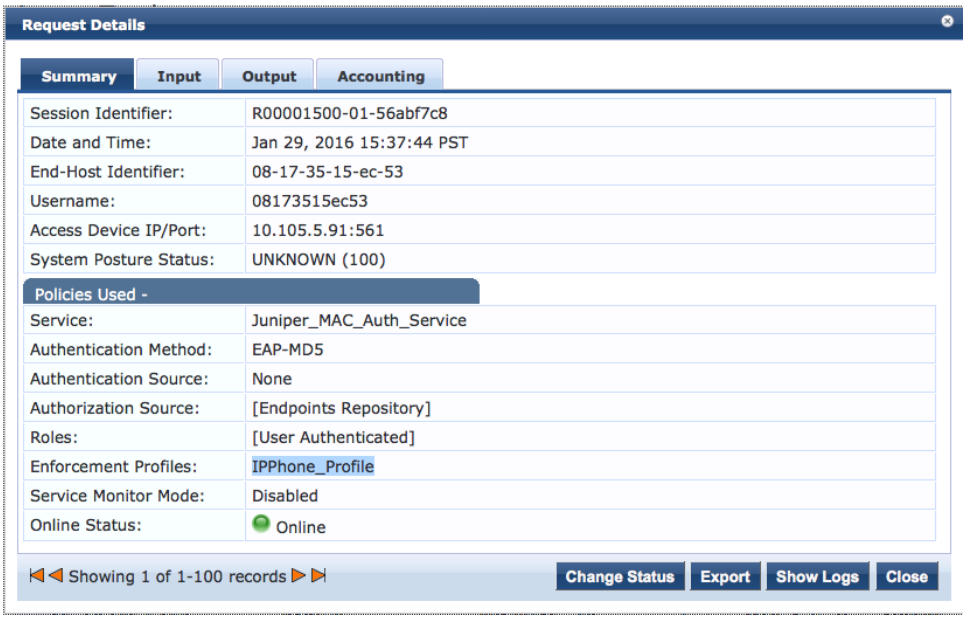
Action

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

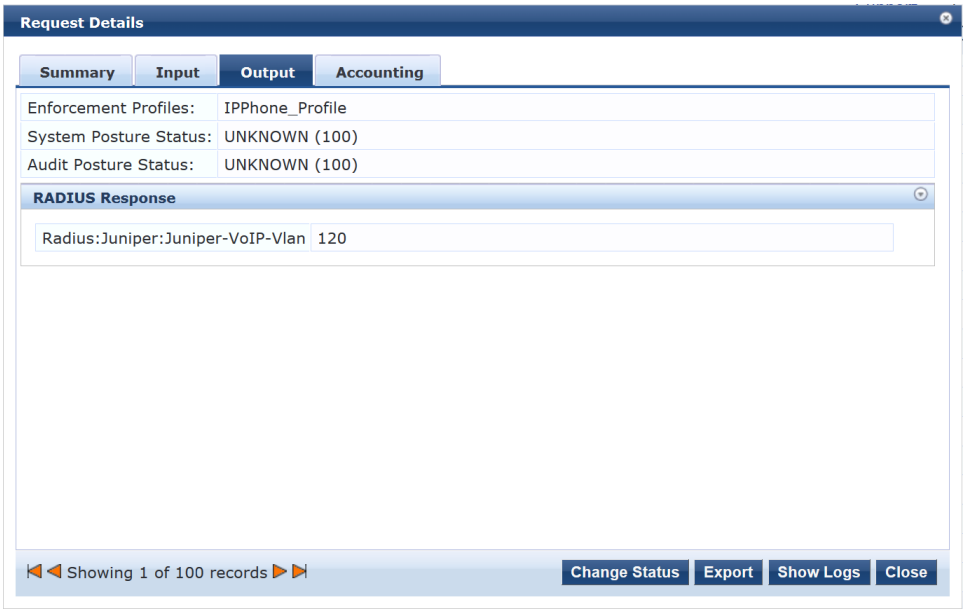
   The Access Tracker monitors authentication requests as they occur and reports on their status.



2. To get more details on a particular authentication request, click on the request.



3. To verify the RADIUS attributes that Aruba ClearPass sent back to the switch for this request, click the **Output** tab.



Meaning The authentication request from the IP phone was successful and the correct information about the VoIP VLAN was returned to the switch.

Related Documentation

- Monitoring Device Profiling on page 36
- Troubleshooting Authentication on page 38
- Technical Overview on page 7
- Use Case Overview on page 6

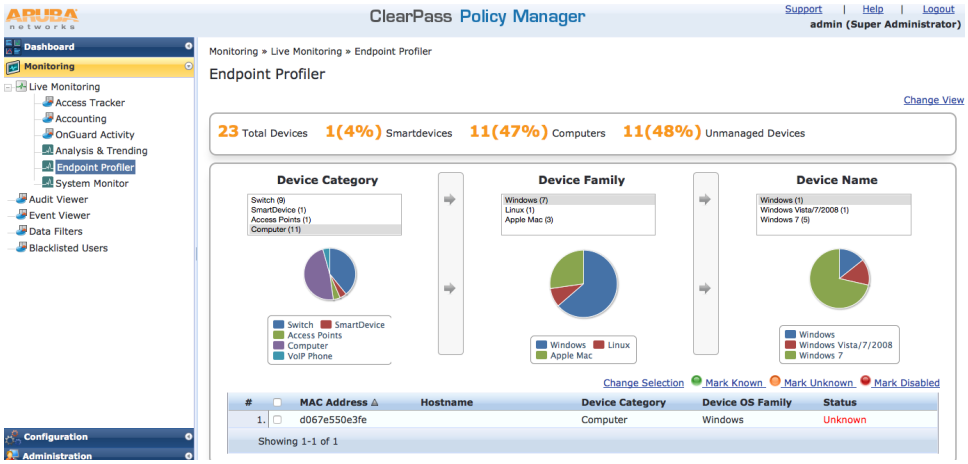
Monitoring Device Profiling

You can view the devices that Aruba ClearPass Profile has discovered and maintains in its endpoint repository, obtaining information on the total number of devices profiled, the kinds of devices, and device-specific data, such as the device vendor, device hostname, and timestamp when the device was added to the repository.

1. In Aruba ClearPass, select **Monitoring** > Live Monitoring > Endpoint Profiler.

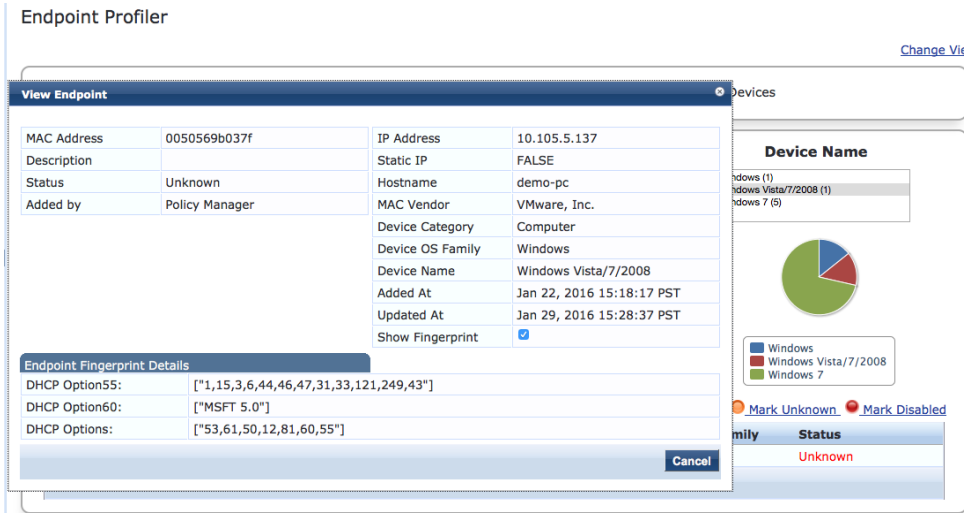
   The initial Endpoint Profiler window provides an overview of the endpoints in its repository, grouping devices within the device category, device family, and device

name hierarchies. The table at the bottom of the window lists the endpoints that are in the currently selected device name group.



2. To display more information about an individual endpoint, click on the endpoint in the table.

   In the View Endpoint window, you can display the information ClearPass Profile used to profile the device by selecting the **Show Fingerprint** option. In the following example, ClearPass Profile used information obtained from various DHCP options in the DHCP messages to profile the device.



Related Documentation

- Example: Configuring Device Profiling with EX Series Switches and Aruba ClearPass Policy Manager on page 8
- Troubleshooting Authentication on page 38
- Technical Overview on page 7
- Use Case Overview on page 6

Troubleshooting Authentication

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 the Aruba ClearPass documentation for more information.

You can enable trace options for the 802.1X protocol. The following set of commands enables 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
```

Related Documentation

- Example: Configuring Device Profiling with EX Series Switches and Aruba ClearPass Policy Manager on page 8
- Monitoring Device Profiling on page 36
- Technical Overview on page 7
- Use Case Overview on page 6