Identify Engines Ignition Server
Ethernet Routing Switch
5500 5600 4500 2500
Engineering

> Device Authentication using Identity Engines Ignition Server Technical Configuration Guide

Enterprise Solutions Engineering
Document Date: April 2010
Document Number: NN48500-586
Document Version: 2.0

Abstract

This Technical Configuration Guide outlines the configuration steps required to create an authenticated network infrastructure for biomedical devices that are Ethernet attached. The main components include both the Ethernet edge switches and the Network Access Control infrastructure provided by Avaya's Identity Engines portfolio.

The audience for this Technical Configuration Guide is intended to be Avaya Sales teams, Partner Sales teams and end-user customers.

Revision Control

No	Date	Version	Revised by	Remarks
1	09/09/2009	1.0	JVE	Modifications to Software Baseline section
2	27/04/2010	2.0	JVE	Added Internal Device configuration

Table of Contents

Conventions

This section describes the text, image, and command conventions used in this document.

Symbols:

👍 Tip – Highlights a configuration or technical tip.

ⓘ Note – Highlights important information to the reader.

☠ Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

Text:

Bold text indicates emphasis.

Italic text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

```
ERS5520-48T# show running-config
```

Output examples from Avaya devices are displayed in a Lucinda Console font:

```
ERS5520-48T# show running-config

! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 5520-24T-PWR
! Software version = v5.0.0.011
enable
configure terminal
```

1. Overview: Medical Device Authentication using Identify Engines

This document provides the framework for implementing device level authentication controls. Future documents will build on this as a base to further define pre-canned solutions that utilize device level authentication.

1.1 Access Layer

Any of the following access layer switches that can be used with Ignition Server for device authentication. However, only the ERS5500 or ERS5600 series can be used if User Access Policies are also required allowing the RADIUS server to tell the switch what policy to apply for a specific user or device.

- ERS5500
- ERS5600
- ERS4500
- ERS2400

1.2 Ignition Server – Biomedical Device Authentication

For the Ignition Server to authenticate biomedical devices from an EAP authenticator, it must know the device identity (typically the MAC address). In an existing network consisting of many biomedical devices, most likely each device identity will not be known, thus making it very difficult to authorize each device based solely on the full MAC address. Avaya's Ignition Server can be configured for device authentication using just the prefix of the biomedical manufacturer's vendor MAC. In turn, the Ignition Server can keep a data base of the full MAC address of each device once it is authenticated by the Ignition Server.

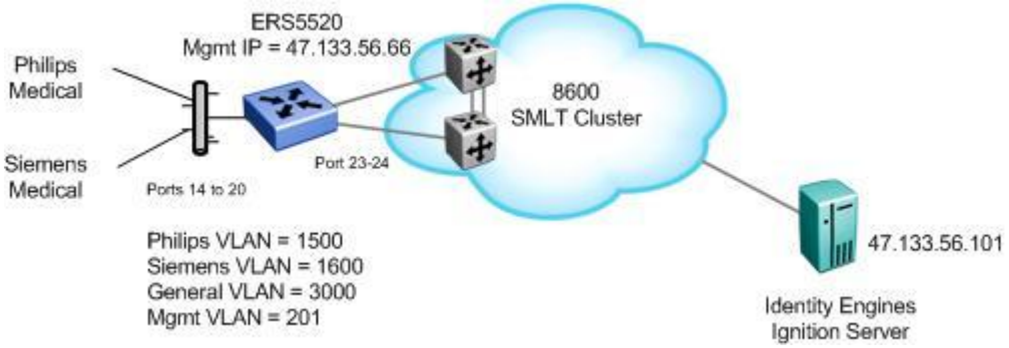
The following is a list of top biomedical manufacturers vendor MAC's.

Prefix	Vendor
00095C	Philips Medical System – Cardiac and Monitoring System
00251B	Philips CareServant
001865	Siemens Medical Solutions Diagnostics Manufacturing (formerly Bayer Diagnostics Sudbury Ltd)
0030E6	Draeger Medical Systems, Inc. (was: SIEMENS MEDICAL SYSTEMS)
0003B1	Hospira Inc. (was: Abbott Laboratories)
001AFA	Welch Allyn, Inc.

1.3 Configuration Examples

Although any Avaya switch as shown in Section 1.1 could be used, for this example, we will use an ERS5520 for allow for both device authentication with or without policy.

1.4 Biomedical Device Authentication using Identify Engines Ignition Server and ERS5500



For this example, we will demonstrate how to configure the Ethernet Routing Switch 5500 and Ignition Server to allow for device authentication based on the biomedical manufacturer vendor MAC address. This will allow authentication and VLAN separation of manufacturer traffic. All that is required is the first three digits of the vendor MAC address for the Ignition Server to authenticate the device and then tell the EAP authenticator (ERS 5520 in this example) what VLAN to place the biomedical device in (we will use Philips and Siemens for this example).

The Ethernet Routing Switch 5500 can be configured to accept both EAP and non-EAP (NEAP) on the same port. In regards to non-EAP, the switch can be configured to accept a password format using any combination of IP address and MAC address with or without port number. By default, the password format is set for IP address, MAC address, and port number. For this example, Ignition Server will be configured for device authentication so it is not important how the password format is configured on the ERS 5520. However, it is suggested to use a password format of MAC address so that if the complete MAC address is known, we can use user authentication versus device authentication on Ignition server.

Overall, we will configured the following

- Enable NEAP on ports 14 to 20 of ERS5520 using the non-EAP password format of MAC address only
- Add VLAN 1500 for the Philips devices
- Add VLAN 1600 for the Siemens devices
- Add VLAN 3000 as the default VLAN everyone connects to until authenticated by Ignition Server
- Configure the Ethernet Routing Switch 5520 and Ignition server with shared key set to *nortel*

- Add the recommended settings for connectivity to an SMLT Cluster – VLACP and Multilink Trunking (MLT) with Spanning Tree disabled on the uplink core ports 23 and 24

1.4.1 ERS Switch Configuration

1.4.1.1 Go to configuration mode.

ERS5520-1 Step 1 - Enter configuration mode

```
5520-24T-PWR> enable
5520-24T-PWR# configure terminal
5520-24T-PWR(config)# cmd-interface cli
5520-24T-PWR(config)# banner disable
5520-24T-PWR(config)# snmp-server name 5520-24T-1
```

1.4.1.2 Create VLAN's

ERS5520-1 Step 1 – Create VLAN's 201, 1500, 1600, and 3000

```
5520-24T-1(config)# vlan create 201 name mgmt type port
5520-24T-1(config)# vlan create 1500 name philips type port
5520-24T-1(config)# vlan create 1600 name siemens type port
5520-24T-1(config)# vlan create 3000 name general type port
```

ERS5520-1 Step 2 – Enable VLAN tagging on all appropriate ports

```
5520-24T-1(config)# vlan port 23-24 tagging tagall
```

ERS5520-1 Step 3 – Set VLAN configuration control to automatic, add VLAN port members, and set the management VLAN to VLAN 201

```
5520-24T-1(config)# vlan configcontrol automatic
5520-24T-1(config)# vlan members add 201 23-24
5520-24T-1(config)# vlan members add 1500 23-24
5520-24T-1(config)# vlan members add 1600 23-24
5520-24T-1(config)# vlan members add 3000,14-20,23-24
5520-24T-1(config)# vlan mgmt 201
```

ERS5520-1 Step 4 – Remove port members from the default VLAN

```
5520-24T-1(config)# vlan members remove 1 14-20,23-24
```

Please note that the non-EAP devices must be a member of a VLAN for the switch to authenticate the devices. You can either leave port member 14-20 in VLAN 1 or create a separate VLAN and add the port members as we have done by creating VLAN 3000.

1.4.1.3 Create MLT

ERS5520-1: Step 1 – Create MLT 1

```
5520-1(config)#mlt 1 member 23-24 learning disable
5520-1(config)#mlt 1 enable
```

1.4.1.4 VLACP

ERS5520-1: Step 1 – Enable VLACP

```
5520-1(config)# vlacp macaddress 180.c200.f
5520-1(config)# vlacp enable
5520-1(config)# interface fastEthernet 23-24
5520-1(config-if)# vlacp timeout short
5520-1(config-if)# vlacp timeout-scale 5
5520-1(config-if)# vlacp enable
5520-1(config-if)# exit
```

1.4.1.5 Discard Untagged Frames on port uplink ports

ERS5520-1: Step 1 – Enable Discard Untagged Frames

```
5520-1(config)# vlan ports 23-24 filter-untagged-frame enable
```

1.4.1.6 Enable Spanning Tree Fast Start and BPDU Filtering on access ports

ERS5520-1 Step 1 – Enable STP Fast Start and BPDU filtering on access port 14-20

```
5520-24T-1(config)#interface fastEthernet 14-20
5520-24T-1(config-if)#spanning-tree learning fast
5520-24T-1(config-if)#spanning-tree bpdu-filtering timeout 0
5520-24T-1(config-if)# spanning-tree bpdu-filtering enable
5520-24T-1(config-if)# exit
```

1.4.1.7 Configure Management IP address on switch

ERS5520-1 Step 1 – Set the IP address of the switch

```
5520-24T-1(config)# interface vlan 201
5520-24T-1(config-if)# ip address 47.133.56.66 netmask 255.255.255.0
5520-24T-1(config-if)# exit
```

ERS5520-1 Step 1 – Add the default route

```
5520-24T-1(config)# ip routing
5520-24T-1(config)# ip route 0.0.0.0 0.0.0.0 47.133.56.1 1
```

1.4.1.8 Configure RADIUS server

ERS5520-1 Step 1 – Add RADIUS server using key 'nortel'

```
5520-24T-1(config)# radius-server host 47.133.56.101 key

Enter key: ******
Confirm key: ******
```

Please note that at this time, non-EAP MAC RADIUS accounting is not supported. Hence this example does not include the step to enable RADIUS accounting. If you wish, you can enable RADIUS accounting using the command *radius accounting enable*.

1.4.1.9 Enable EAP globally

ERS5520-1 Step 1 – Enable non-EAP (NEAP)

```
5520-24T-1(config)# eap multihost allow-non-eap-enable
```

ERS5520-1 Step 2 – Enable RADIUS authentication for non-EAP (NEAP)

```
5520-24T-1(config)# eap multihost radius-non-eap-enable
```

ERS5520-1 Step 3 – Enable RADIUS non-EAP (NEAP) RADIUS assigned VLAN

```
5520-24T-1(config)# eapol multihost non-eap-use-radius-assigned-vlan
```

ERS5520-1 Step 2 – Remove the default NEAP password format of IpAddr.MACAddr.PortNumber

```
5520-24T-1(config)# no eapol multihost non-eap-pwd-fmt
```

ERS5520-1 Step 3 – Enable NEAP password format of MAC address only

```
5520-24T-1(config)# eapol multihost non-eap-pwd-fmt mac-addr
```

ERS5520-1 Step 4 – Enable EAP globally

```
5520-24T-1(config)# eapol enable
```

1.4.1.10 Enable EAP at interface level

ERS5520-1 Step 1 – Enable EAP on port 14-20 with NEAP, set the maximum allowable EAP and NEAP clients to 1, enable EAP multihost and enable RADIUS NEAP phone

```
5520-24T-1(config)# interface fastEthernet 14-20
5520-24T-1(config-if)# eapol status auto
5520-24T-1(config-if)# eapol multihost allow-non-eap-enable
5520-24T-1(config-if)# eapol multihost eap-mac-max 1
5520-24T-1(config-if)# eapol multihost non-eap-mac-max 1
5520-24T-1(config-if)# eapol multihost radius-non-eap-enable
5520-24T-1(config-if)# eapol multihost non-eap-use-radius-assigned-vlan
5520-24T-1(config-if)# eapol multihost enable
5520-24T-1(config-if)# exit
```

1.4.2 ERS 5520 Switch: Verify Operations

1.4.2.1 Verify EAP Global and Port Configuration

Step 1 – Verify that EAP has been enabled globally and the correct port members:

```
5520-24T-1# show eapol port 14-20
```

Result:

```
EAPOL Administrative State:  Enabled
Port-mirroring on EAP ports: Disabled
EAPOL User Based Policies:  Disabled
EAPOL User Based Policies Filter On MAC Addresses:  Disabled
Port:  14
    Admin Status:  Auto
    Auth:  No
    Admin Dir:  Both
    Oper Dir:  Both
    ReAuth Enable:  No
    ReAuth Period:  3600
    Quiet Period:  60
    Xmit Period:  30
    Supplic Timeout:  30
    Server Timeout:  30
    Max Req:  2
    RDS DSE:  No
|
|
Port:  20
    Admin Status:  Auto
    Auth:  No
    Admin Dir:  Both
    Oper Dir:  Both
    ReAuth Enable:  No
    ReAuth Period:  3600
    Quiet Period:  60
    Xmit Period:  30
    Supplic Timeout:  30
    Server Timeout:  30
    Max Req:  2
    RDS DSE:  No
```

On the ERS5520 verify the following information:

Option	Verify
EAPOL Administrative State	Verify that the EAPOL is ***Enabled*** globally.
EAPOL User Based Policies	Verify that EAPOL policies are ***Enabled*** globally.
Admin Status	Verify that the EAP is enabled on ports 14 to 20 by verifying that the Admin Status is set to ***Auto***.

Auth	The value will be ***No*** even if the IP Phone has successfully authenticated. Only if there a Supplicant attached to the IP Phone and it has successfully authenticated will this value change to Yes.

1.4.2.2 Verify EAP Multihost Configuration

Step 1 – Verify that EAP multihost has been globally configured correctly:

```
5520-24T-1#show eapol multihost
```

Result:

```
       Allow Non-EAPOL Clients:  Enabled
       Use RADIUS To Authenticate Non-EAPOL Clients:  Enabled
       Allow Non-EAPOL Clients After Single Auth (MHSA):  Disabled
       Allow Non-EAPOL VoIP Phone Clients:  Disabled
       EAPOL Request Packet Generation Mode:  Multicast
       Allow Use of RADIUS Assigned VLANs:  Disabled
       Allow Use of Non-Eapol RADIUS Assigned VLANs:  Enabled
       Non-EAPOL RADIUS Password Attribute Format:  MACAddr
       Non-EAPOL User Based Policies:  Enabled
       Non-EAPOL User Based Policies Filter On MAC Addresses:  Disabled
       Use most recent RADIUS VLAN:  Disabled
```

Step 2 – Verify that EAP multihost has been configured correctly at interface level:

```
5520-24T-1#show eapol multihost interface 14-20
```

Result:

```
       Port:  14
           MultiHost Status:  Enabled
           Max Eap Clients:  1
           Allow Non-EAP Clients:  Enabled
           Max Non-EAP Client MACs:  1
           Use RADIUS To Auth Non-EAP MACs:  Enabled
           Allow Auto Non-EAP MHSA:  Disabled
           Allow Non-EAP Phones:  Disabled
           RADIUS Req Pkt Send Mode:  Multicast
           Allow RADIUS VLANs:  Disabled
           Allow Non-EAP RADIUS VLANs:  Enabled
           Use most recent RADIUS VLAN:  Disabled
       |
       |
       Port:  20
           MultiHost Status:  Enabled
           Max Eap Clients:  1
           Allow Non-EAP Clients:  Enabled
           Max Non-EAP Client MACs:  1
           Use RADIUS To Auth Non-EAP MACs:  Enabled
           Allow Auto Non-EAP MHSA:  Disabled
           Allow Non-EAP Phones:  Disabled
           RADIUS Req Pkt Send Mode:  Multicast
           Allow RADIUS VLANs:  Disabled
           Allow Non-EAP RADIUS VLANs:  Enabled
```

```
          Use most recent RADIUS VLAN:  Disabled
```

On the ERS5520 verify the following information:

Option	Verify
Allow Non-EAPOL Clients:	Verify that non-EAPOL (NEAP) is ***Enabled*** globally and at interface level.
Use RADIUS To Authenticate Non-EAPOL Clients:	Verify the use RADUIS to authenticate non-EAPOL option is ***Enabled*** globally and at interface level.
Non-EAPOL RADIUS Password Attribute Format:	Verify that the non-EAP password format is set for ***MACAddr.*** Please note, some of the older software releases required a leading period "." before and after the MAC address.
Allow Non-EAP RADIUS VLANs:	Verity that non-EAPOL RADIUS VLANs is ***Enabled*** globally and at interface level.

1.4.2.3 Verify EAP Multihost Status

Step 1 – Assuming Siemens devices on ports 14 & 15 and Philips devices on ports19 & 20, verify device MAC addressses:

```
5520-24T-1# show eapol multihost non-eap-mac status
```

Result:

```
      Port Client MAC Address State
      ---- ------------------ ------------------------------
      14   00:18:65:00:02:01 Authenticated By RADIUS
      15   00:18:65:00:02:02 Authenticated By RADIUS
      19   00:09:5C:00:02:03 Authenticated By RADIUS
      20   00:09:5C:00:02:04 Authenticated By RADIUS
```

Step 2 – Assuming Siemens devices on ports 14 & 15 and Philips devices on ports19 & 20, verify VLAN membership:

```
5520-24T-1# show vlan interface info 14-20
```

Result:

```
             Filter     Filter
            Untagged Unregistered
      Port   Frames     Frames     PVID PRI    Tagging     Name
      ---- -------- ------------ ---- --- -------------- ----------------
      14    No        Yes          1600 0   UntagAll       Port 14
      15    No        Yes          1600 0   UntagAll       Port 15
      16    No        Yes          3000 0   UntagAll       Port 16
      17    No        Yes          3000 0   UntagAll       Port 17
      18    No        Yes          3000 0   UntagAll       Port 18
      19    No        Yes          1500 0   UntagAll       Port 19
```

```
        20    No        Yes            1500 0    UntagAll        Port 20
```

```
5520-24T-1# show vlan
```

Result:

```
        Id  Name                 Type     Protocol         User PID Active IVL/SVL Mgmt
        --- -------------------- -------- ---------------- -------- ------ ------- ----
        1   VLAN #1              Port     None             0x0000   Yes    IVL     No
                Port Members: 1-19,21-22
        201 mgmt                 Port     None             0x0000   Yes    IVL     No
                Port Members: 23-24
        1500 philips              Port    None             0x0000   Yes    IVL     No
                Port Members: 19-20,23-24
        1600 siemens              Port    None             0x0000   Yes    IVL     No
                Port Members: 14-15,23-24
        3000 general              Port    None             0x0000   Yes    IVL     No
                Port Members: 14-20,23-24
        Total VLANs: 5
```

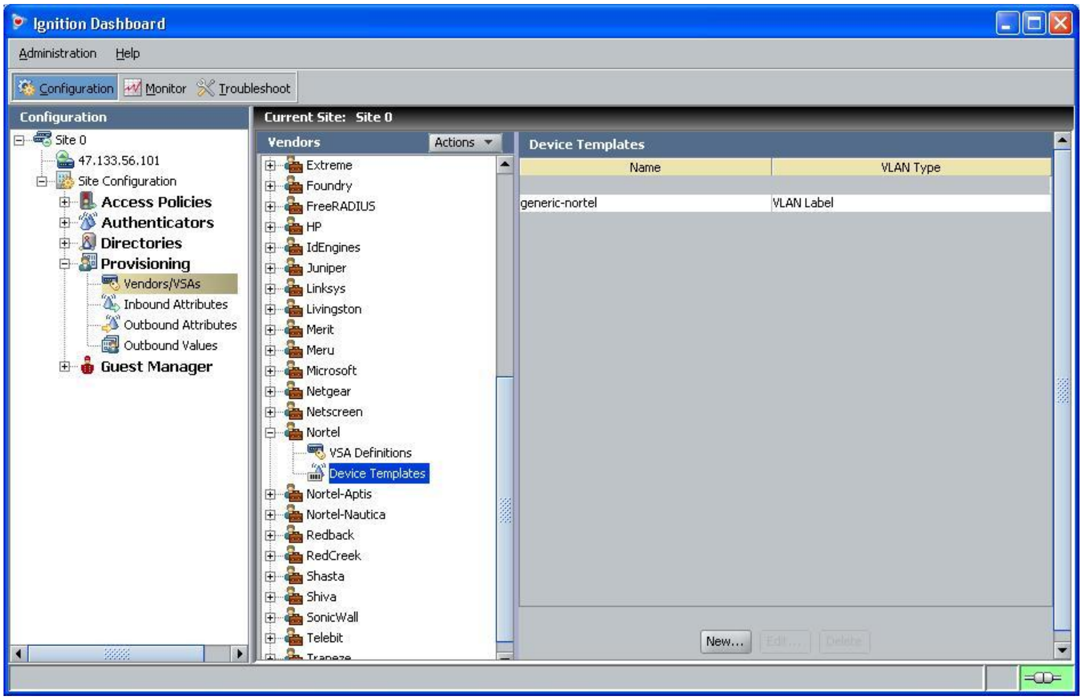
On ERS5520-1, verify the following information:

Option	Verify
Port	Display the ports where the device has successfully been authenticated.
Client MAC Address	If the IP phone has successfully authenticated via NEAP, its MAC address should be shown.
State	Verity that ***Authenticated By RADIUS*** is displayed
PVID Port Members	Assuming that we have two Philips devices on ports 19 & 20 and two Siemens devices on ports 14 & 15. Ports 14 & 15 should be members of VLAN 1600 with PVID of 1600. Ports 19 & 20 should be members of VLAN 1500 with PVID of 1500.

1.4.3 IDE Setup

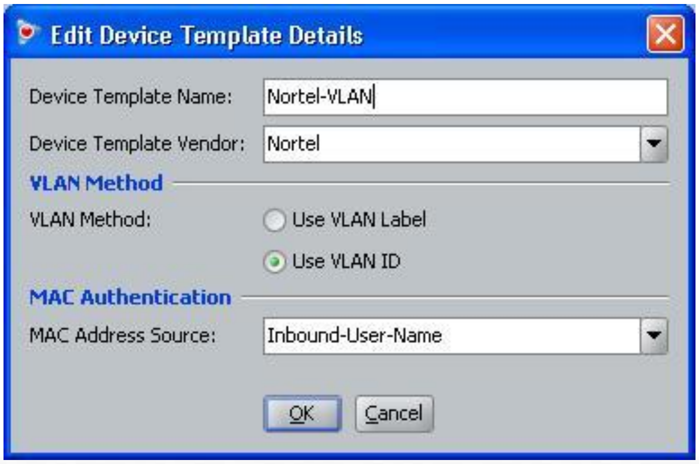
1.4.3.1 Create a new Nortel device template

IDE Step 1 – Go to *Site Configuration ->Provisioning -> Vendor/VSA's -> Nortel -> Device Template -> New*



Name	VLAN Type
generic-nortel	VLAN Label

IDE Step 2 – Name the new Nortel device template (Nortel-VLAN in this example), set the VLAN Method to *Use VLAN ID*, set the *MAC Address Source:* to *Inbound-User-Name*, and click on *OK*


Edit Device Template Details

Device Template Name: Nortel-VLAN

Device Template Vendor: Nortel

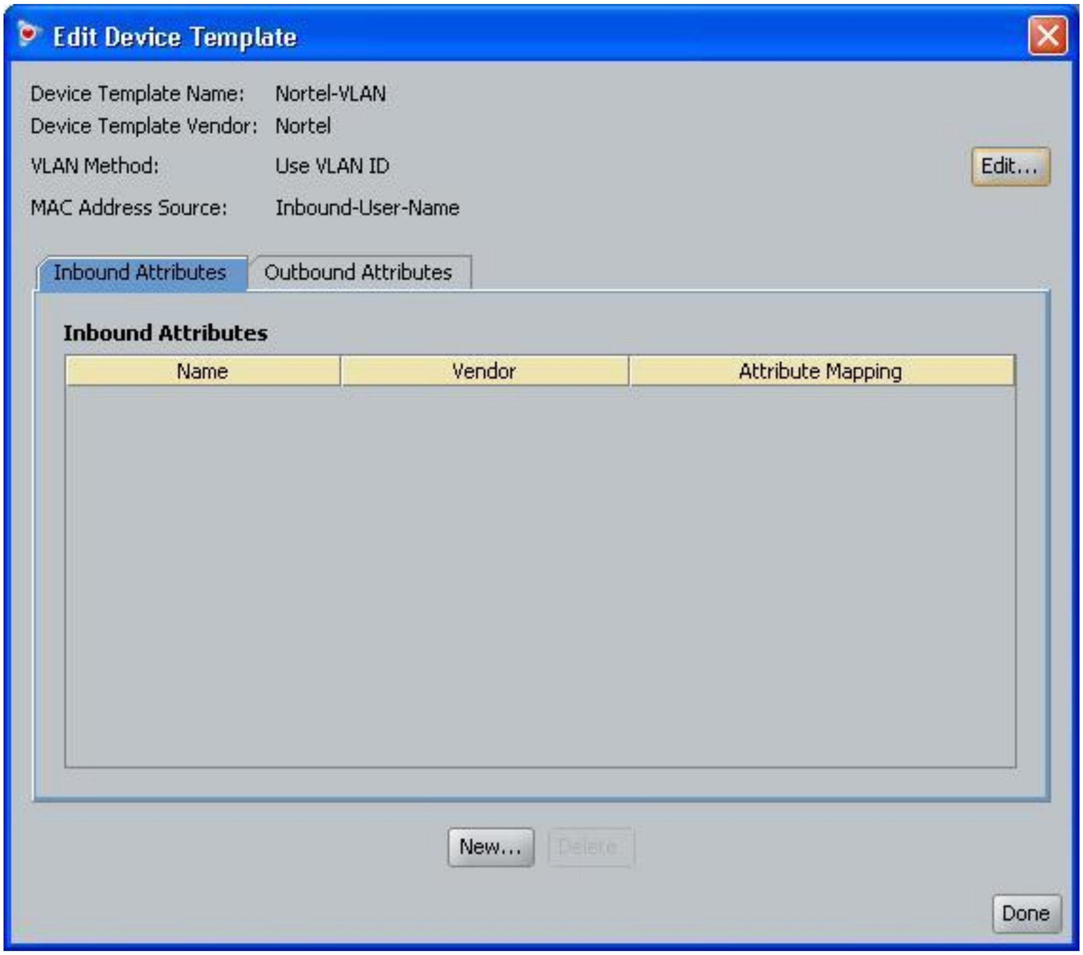
VLAN Method

VLAN Method: ○ Use VLAN Label ● Use VLAN ID

MAC Authentication

MAC Address Source: Inbound-User-Name

IDE Step 3 – Click on *Done* to complete configuration



Edit Device Template

Device Template Name: Nortel-VLAN
Device Template Vendor: Nortel
VLAN Method: Use VLAN ID
MAC Address Source: Inbound-User-Name

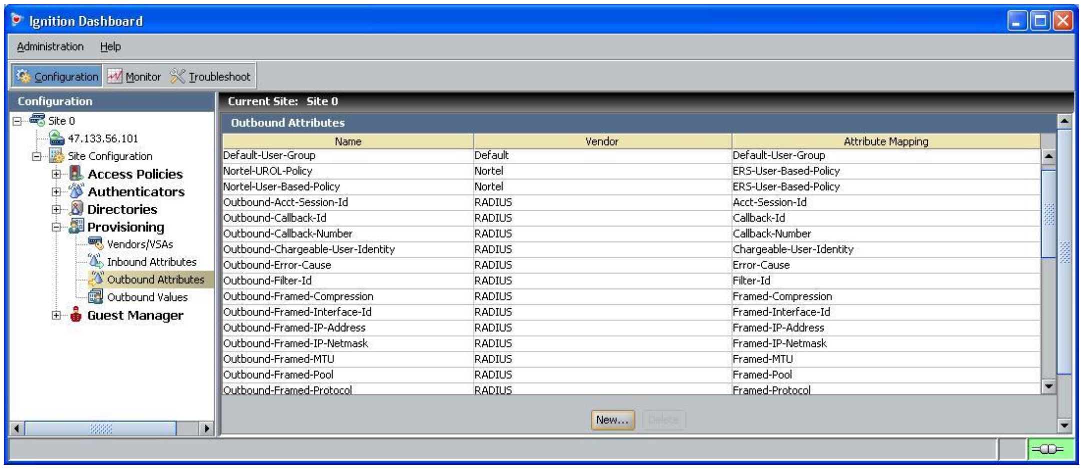
Inbound Attributes

Name	Vendor	Attribute Mapping

☠ Please note that you must change the Avaya switch device template *MAC Address Source* from the default setting of *Inbound-Calling-Station-Id* to *Inbound-User-Name* for device authentication to work when using a Avaya ERS switch as an EAP authenticator. This only applies to device authentication and not user authentication.

1.4.3.2 Configure an Outbound Attribute on Ignition Server for VLAN

IDE Step 1 – Go to *Site Configuration -> Provisioning -> Outbound Attributes -> New*

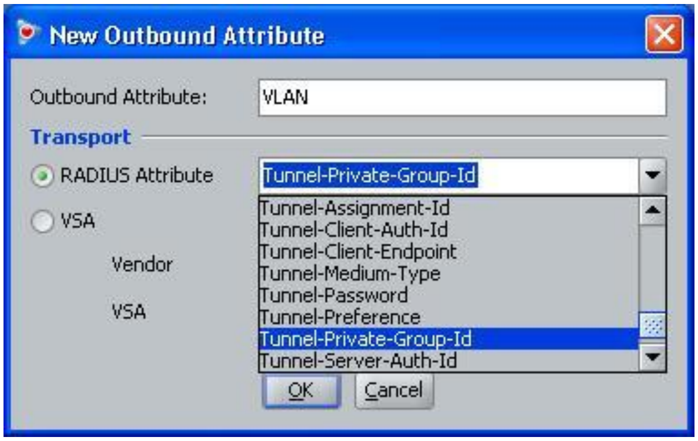


Current Site: Site 0

Outbound Attributes

Name	Vendor	Attribute Mapping
Default-User-Group	Default	Default-User-Group
Nortel-UROL-Policy	Nortel	ERS-User-Based-Policy
Nortel-User-Based-Policy	Nortel	ERS-User-Based-Policy
Outbound-Acct-Session-Id	RADIUS	Acct-Session-Id
Outbound-Callback-Id	RADIUS	Callback-Id
Outbound-Callback-Number	RADIUS	Callback-Number
Outbound-Chargeable-User-Identity	RADIUS	Chargeable-User-Identity
Outbound-Error-Cause	RADIUS	Error-Cause
Outbound-Filter-Id	RADIUS	Filter-Id
Outbound-Framed-Compression	RADIUS	Framed-Compression
Outbound-Framed-Interface-Id	RADIUS	Framed-Interface-Id
Outbound-Framed-IP-Address	RADIUS	Framed-IP-Address
Outbound-Framed-IP-Netmask	RADIUS	Framed-IP-Netmask
Outbound-Framed-MTU	RADIUS	Framed-MTU
Outbound-Framed-Pool	RADIUS	Framed-Pool
Outbound-Framed-Protocol	RADIUS	Framed-Protocol

IDE Step 2 – Via the *Outbound Attribute* window, enter a name for the attribute (i.e. VLAN as used in this example), and select *Tunnel-Private-Group-Id* via the *RADIUS Attribute* radio button. Click on *OK* when done

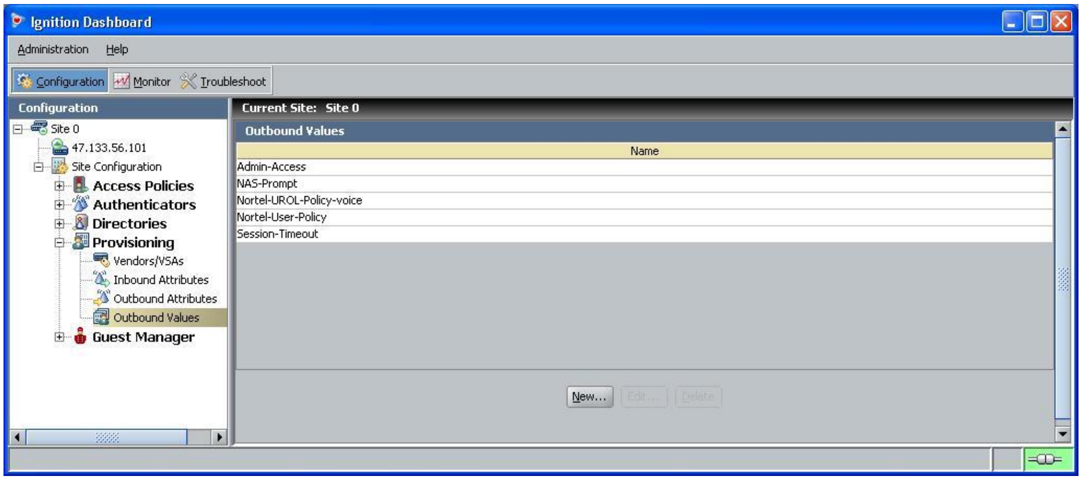


Outbound Attribute: VLAN

● RADIUS Attribute: Tunnel-Private-Group-Id

○ VSA

IDE Step 3 – Go to *Site Configuration -> Provisioning -> Outbound Values -> New*

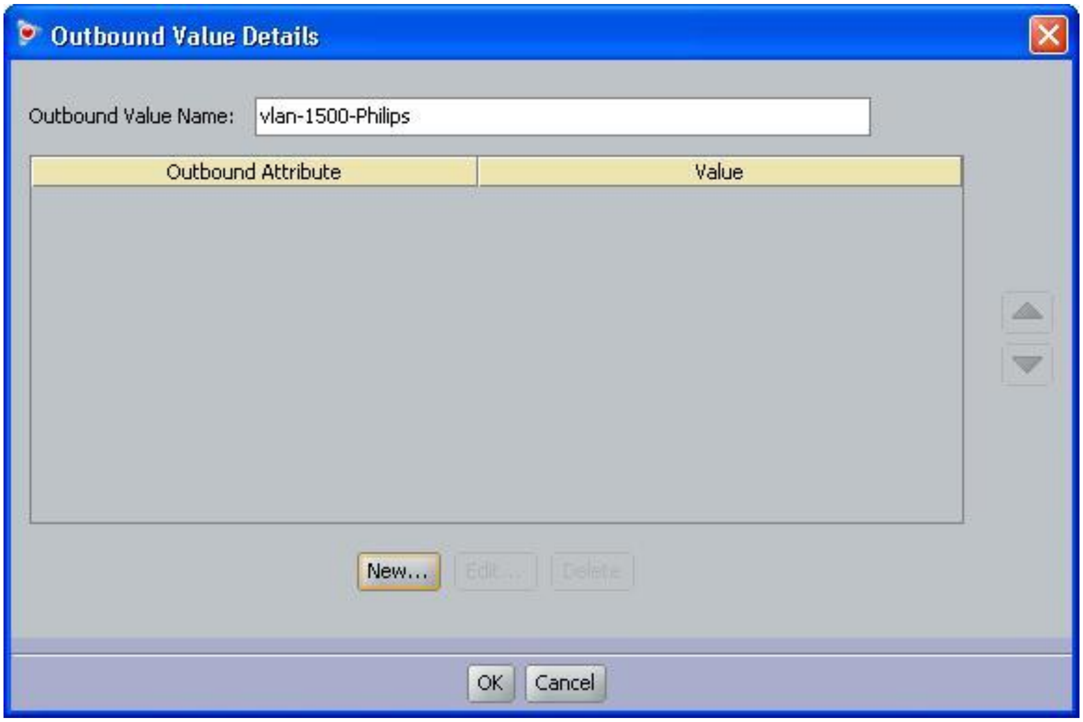


Current Site: Site 0

Outbound Values

Name
Admin-Access
NAS-Prompt
Nortel-UROL-Policy-voice
Nortel-User-Policy
Session-Timeout

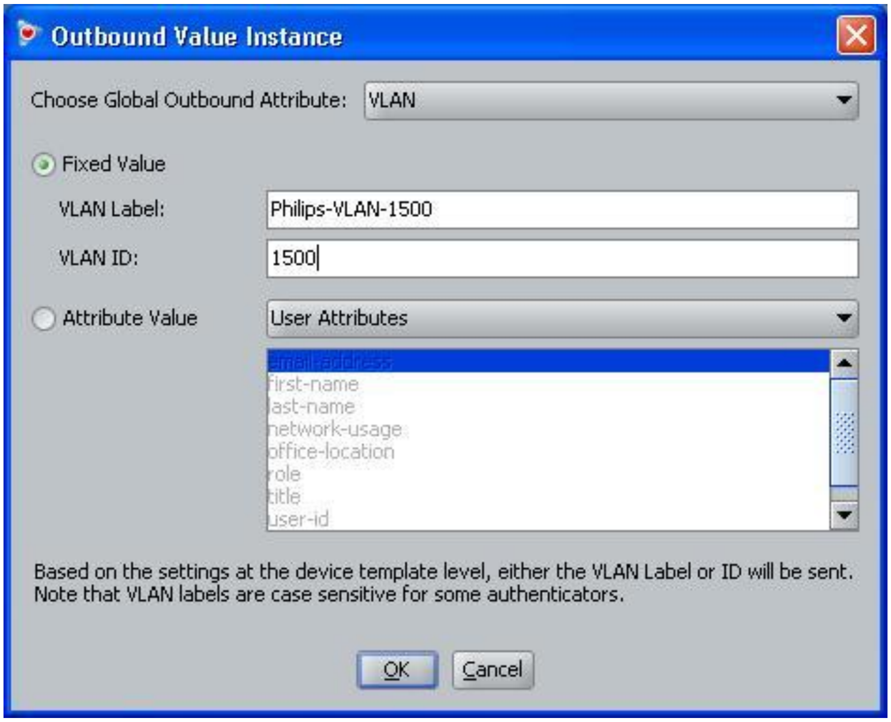
IDE Step 4 – Using the Outbound Attribute created in Step 2, we will add the VLAN ID value for the Philips VLAN. Start by entering a name via the *Outbound Value Name:* window (i.e. vlan-1500-Philips as used in this example) and click on *New*



Outbound Value Name: vlan-1500-Philips

Outbound Attribute	Value

IDE Step 5 – Select the Outbound Attributes name created in Step 2 (i.e. VLAN as used in this example) via the *Choose Global Outbound Attribute:* pull down menu. Make sure the *Fixed Value* radio button is selected. Enter an name (i.e. Philips-VLAN-1500 as used in this example) in the *VLAN Label:* window and enter the correct VLAN number (i.e. 1500 as used in this example) in the *VLAN ID:* window. Click on *OK* twice when done.



Outbound Value Instance

Choose Global Outbound Attribute: VLAN

● Fixed Value

VLAN Label: Philips-VLAN-1500

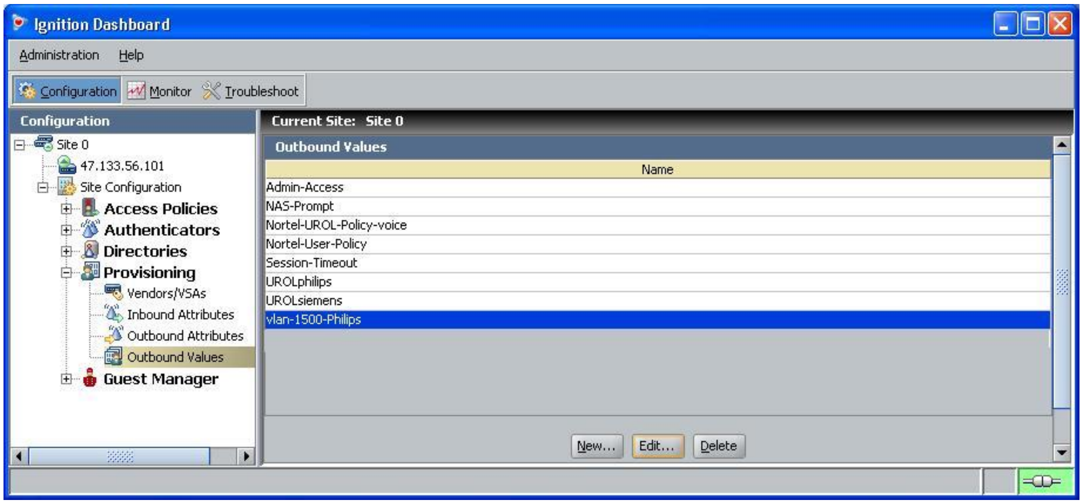
VLAN ID: 1500

○ Attribute Value: User Attributes

email-address
first-name
last-name
network-usage
office-location
role
title
user-id

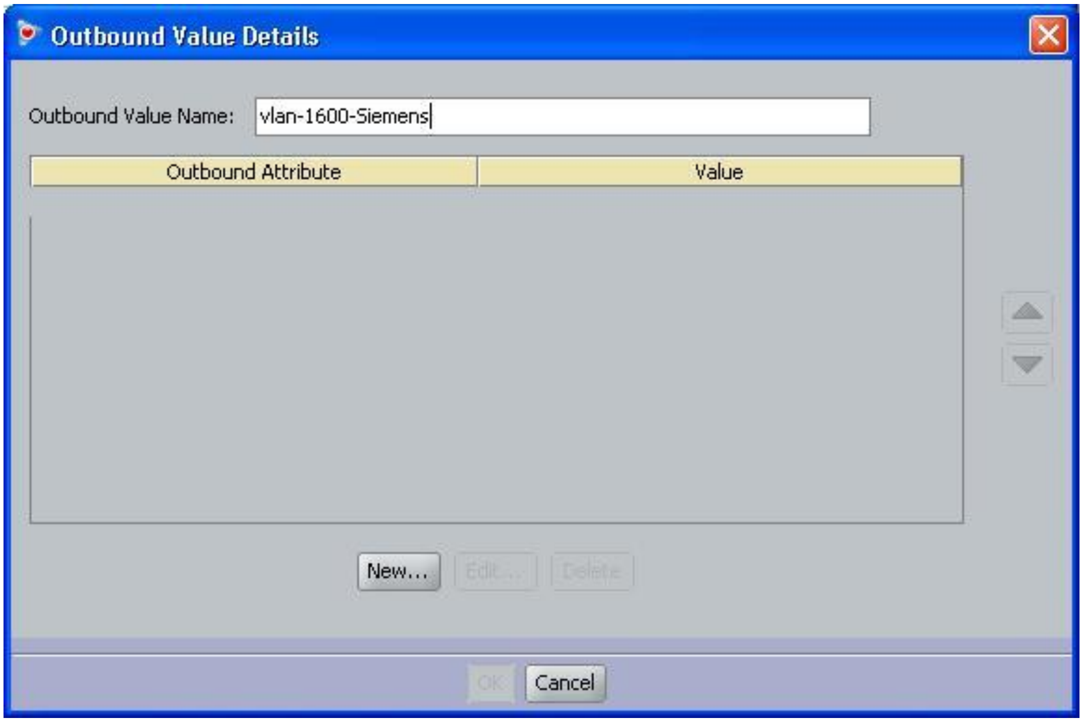
Based on the settings at the device template level, either the VLAN Label or ID will be sent.
Note that VLAN labels are case sensitive for some authenticators.

IDE Step 6 – We will now repeat step 3 to 5 to add the RADIUS attribute for the Siemens VLAN. Go to *Site Configuration -> Provisioning -> Outbound Values -> New*



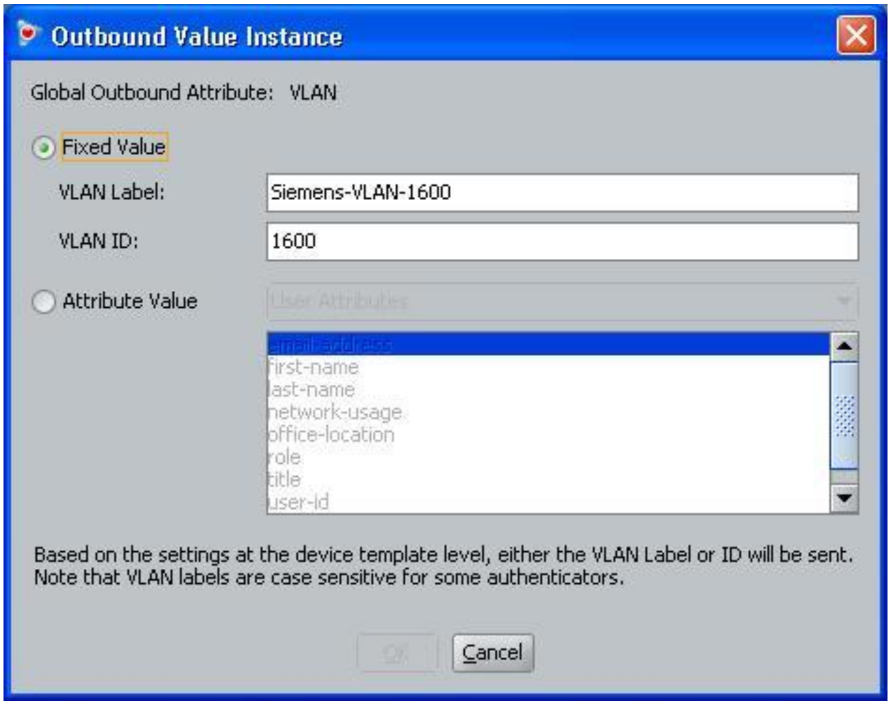
Name
Admin-Access
NAS-Prompt
Nortel-UROL-Policy-voice
Nortel-User-Policy
Session-Timeout
UROLphilips
UROLsiemens
vlan-1500-Philips

IDE Step 7 – Using the Outbound Attribute created in Step 2, we will add the VLAN ID value for the Siemens VLAN. Start by entering a name via the *Outbound Value Name:* window (i.e. vlan-1600-Siemens as used in this example) and click on *New*



Outbound Value Name: vlan-1600-Siemens

IDE Step 8 – Select the Outbound Attributes name created in Step 2 (i.e. VLAN as used in this example) via the *Choose Global Outbound Attribute:* pull down menu. Make sure the *Fixed Value* radio button is selected. Enter a name (i.e. Siemens-VLAN-1600 as used in this example) in the *VLAN Label:* window and enter the correct VLAN number (i.e. 1600 as used in this example) in the *VLAN ID:* window. Click on *OK* twice when done.



Global Outbound Attribute: VLAN

● Fixed Value

VLAN Label: Siemens-VLAN-1600

VLAN ID: 1600

○ Attribute Value

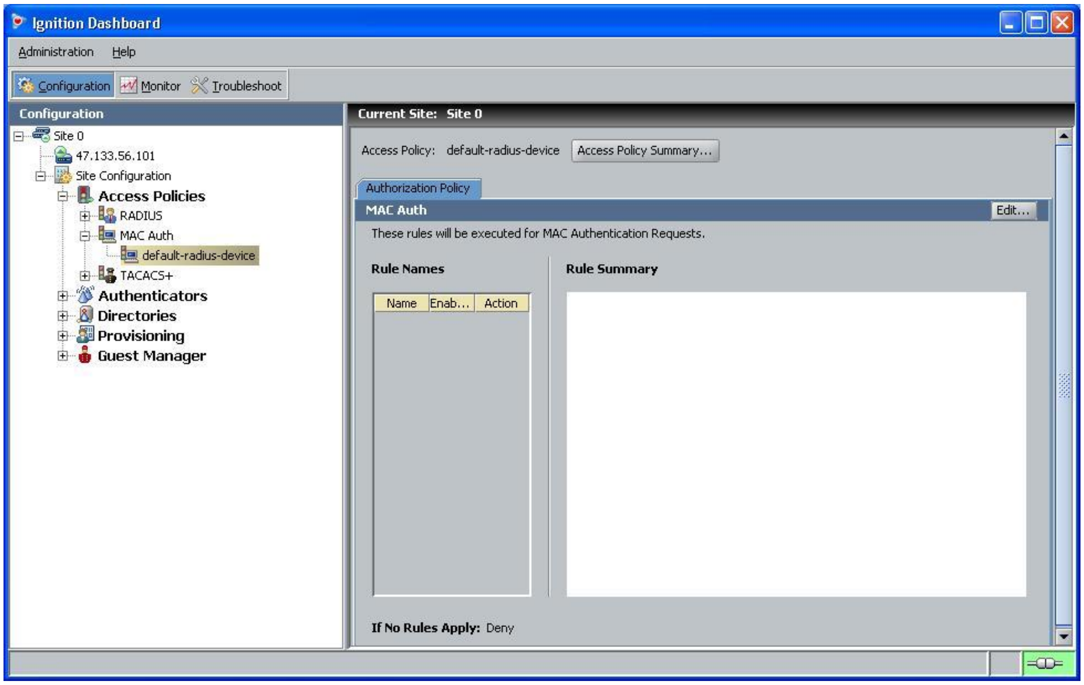
Based on the settings at the device template level, either the VLAN Label or ID will be sent. Note that VLAN labels are case sensitive for some authenticators.

1.4.3.3 Add Access Policy

The following is a list of top biomedical manufacturers vendor MAC's. The Philips and Siemens MAC prefix as shown in this table will be used for this policy.

Prefix	Vendor
00095C	Philips Medical System – Cardiac and Monitoring System
00251B	Philips CareServant
001865	Siemens Medical Solutions Diagnostics Manufacturing (formerly Bayer Diagnostics Sudbury Ltd)
0030E6	Draeger Medical Systems, Inc. (was: SIEMENS MEDICAL SYSTEMS)
0003B1	Hospira Inc. (was: Abbott Laboratories)
001AFA	Welch Allyn, Inc.

IDE Step 1 – Go to *Site Configuration -> Access Policies -> MAC Auth -> default-radius-device* and click on *Edit*

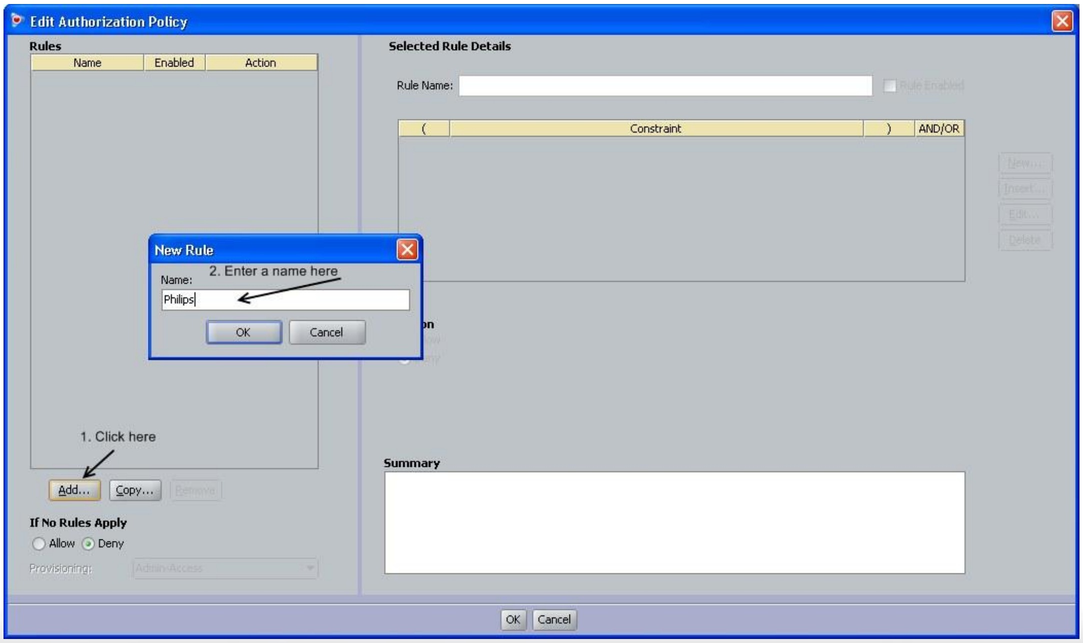


Access Policy: default-radius-device

These rules will be executed for MAC Authentication Requests.

If No Rules Apply: Deny

IDE Step 2 – First we will create a rule for the Philips medical devices. Start by clicking on *Add* and then enter a name for the rule when the *New Rule* window pops up.



2. Enter a name here

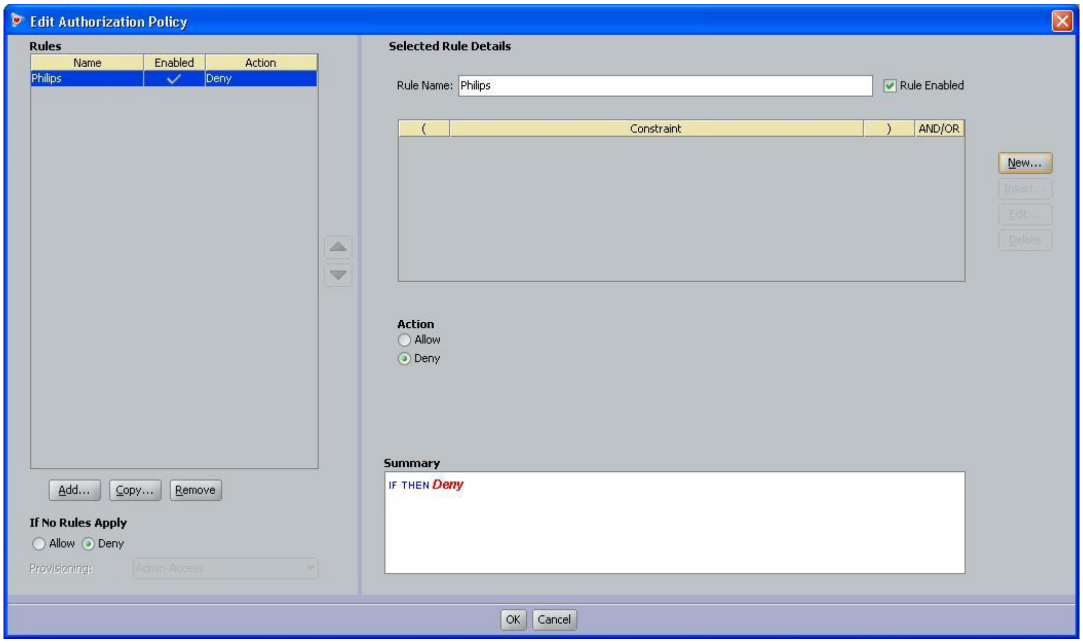
Name: Philips

1. Click here

If No Rules Apply

○ Allow ● Deny

IDE Step 3 – Via the *Edit Authentication Policy* window, click on *New*



Edit Authorization Policy

Rules

Name	Enabled	Action
Philips	✓	Deny

Selected Rule Details

Rule Name: Philips ☑ Rule Enabled

(	Constraint	)	AND/OR

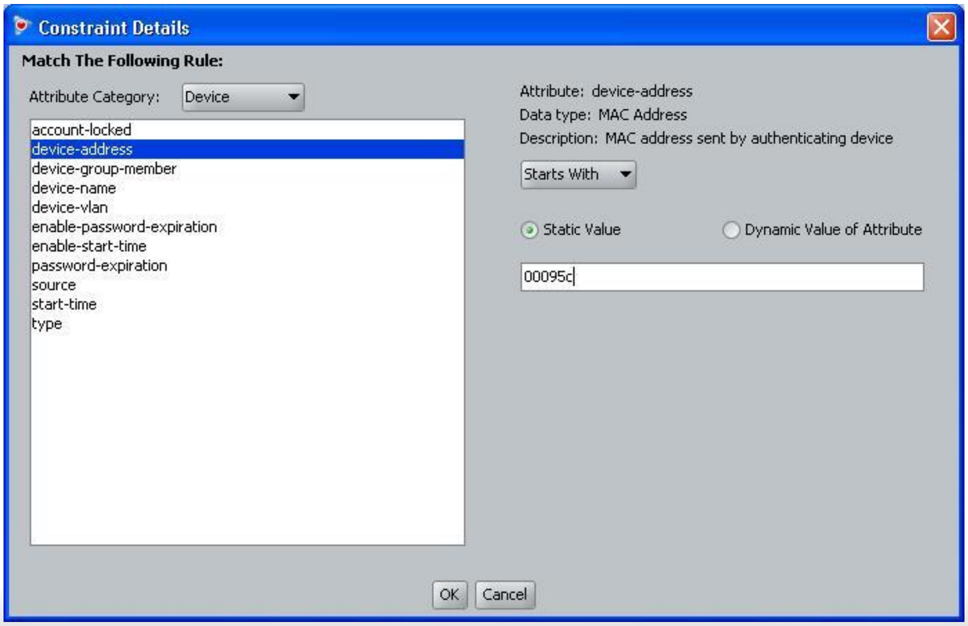
Action
○ Allow
● Deny

Summary
IF THEN *Deny*

If No Rules Apply
○ Allow ● Deny

Provisioning: Admin-Access

IDE Step 4 – In the *Constraint Details* window, under *Attribute Category*, select *Device* and then scroll down and select *device-address*. Next, via the right hand side plane, select *Starts With*, make sure *Static Value* is selected and enter the first three digits of the MAC address. In our example, we are authenticating Philips MAC addresses which start with "00:09:5C" so we will enter *00095c*. Click on *OK* when completed.



Constraint Details

Match The Following Rule:

Attribute Category: Device

- account-locked
- device-address
- device-group-member
- device-name
- device-vlan
- enable-password-expiration
- enable-start-time
- password-expiration
- source
- start-time
- type

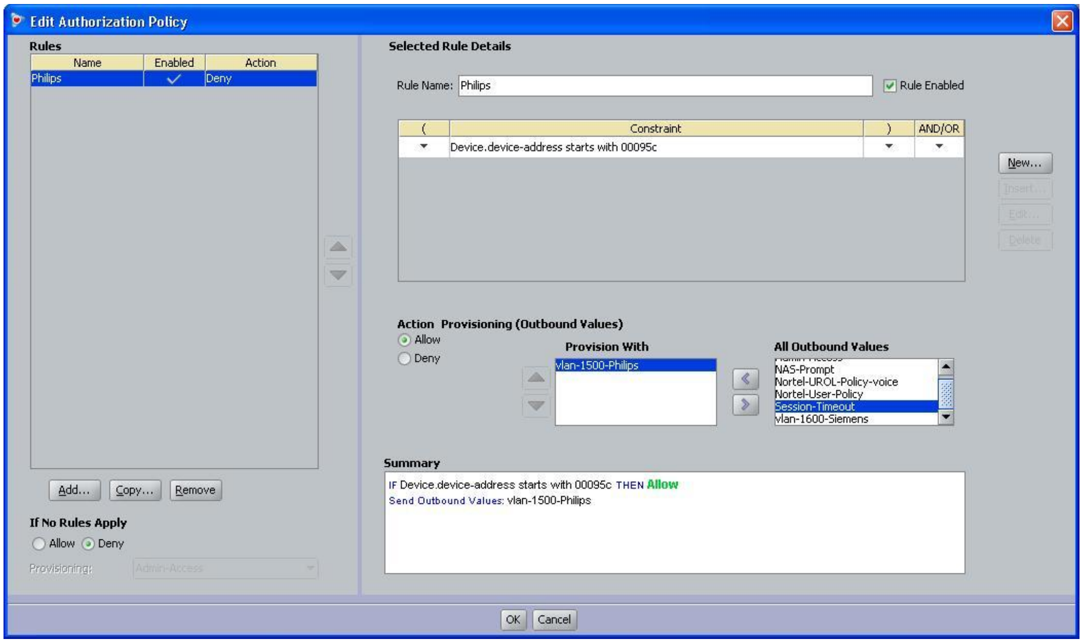
Attribute: device-address
Data type: MAC Address
Description: MAC address sent by authenticating device

Starts With

● Static Value ○ Dynamic Value of Attribute

00095c

IDE Step 5 – Once back at the *Edit Authentication Policy* window, click the *Allow* radio button via *Action Provisioning* and move the attribute we configured above named *vlan-1500-philips* from *All Outbound Value* box to the *Provision With* box.



Rules

Name	Enabled	Action
Philips	✓	Deny

Selected Rule Details

Rule Name: Philips ☑ Rule Enabled

(	Constraint	)	AND/OR
	Device.device-address starts with 00095c		

Action Provisioning (Outbound Values)

● Allow
○ Deny

Provision With: vlan-1500-Philips

All Outbound Values: NAS-Prompt, Nortel-UROL-Policy-voice, Nortel-User-Policy, Session-Timeout, vlan-1600-Siemens

Summary

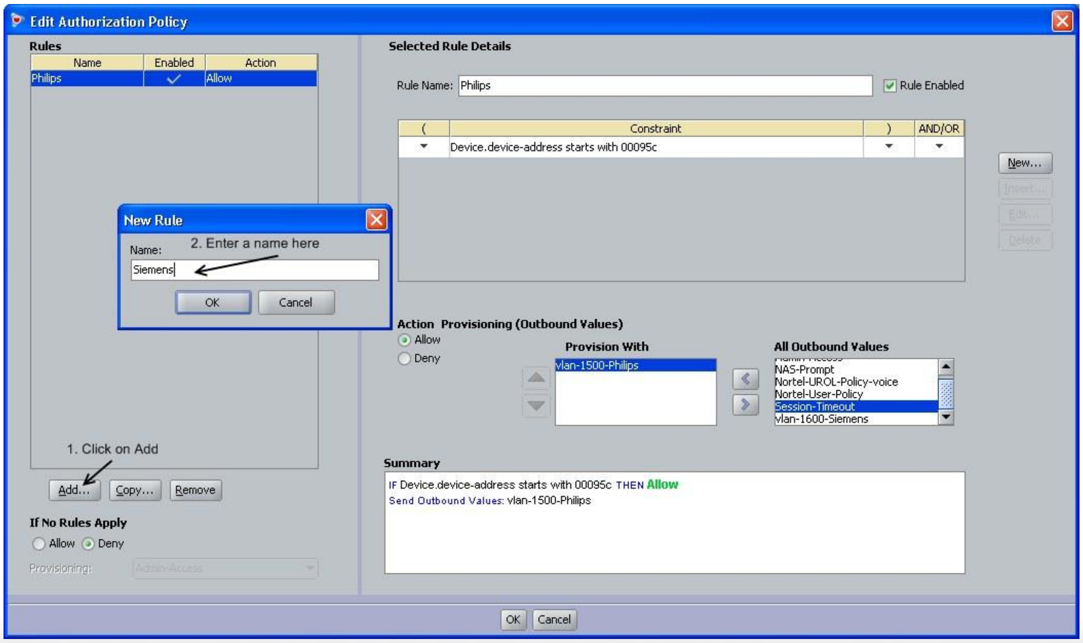
IF Device.device-address starts with 00095c THEN Allow
Send Outbound Values: vlan-1500-Philips

If No Rules Apply

○ Allow ● Deny

Provisioning: Admin-Access

IDE Step 6 – Next, we will create a rule for the Siemens medical devices. Click on *Add* and then enter a name for the rule when the *New Rule* window pops up.



Rules

Name	Enabled	Action
Philips	✓	Allow

Selected Rule Details

Rule Name: Philips ☑ Rule Enabled

(	Constraint	)	AND/OR
	Device.device-address starts with 00095c		

New Rule

2. Enter a name here

Name: Siemens

Action Provisioning (Outbound Values)

● Allow
○ Deny

Provision With: vlan-1500-Philips

All Outbound Values: NAS-Prompt, Nortel-UROL-Policy-voice, Nortel-User-Policy, Session-Timeout, vlan-1600-Siemens

1. Click on Add

Summary

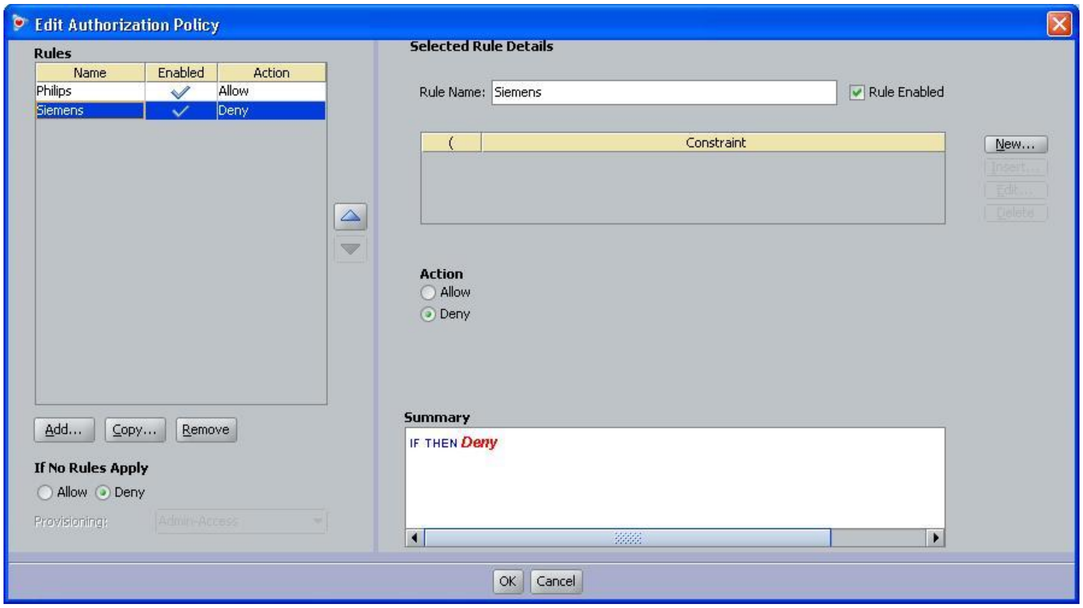
IF Device.device-address starts with 00095c THEN Allow
Send Outbound Values: vlan-1500-Philips

If No Rules Apply

○ Allow ● Deny

Provisioning: Admin-Access

IDE Step 7 – Via the *Edit Authentication Policy* window, click on *New.*



Edit Authorization Policy

Rules

Name	Enabled	Action
Philips	✓	Allow
Siemens	✓	Deny

If No Rules Apply: ○ Allow ● Deny

Provisioning: Admin-Access

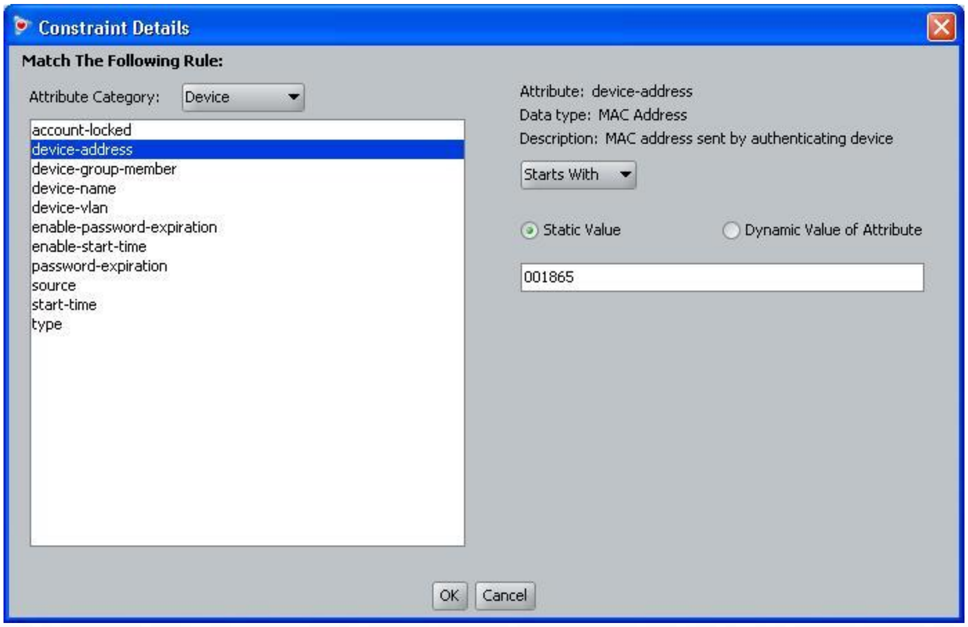
Selected Rule Details

Rule Name: Siemens ☑ Rule Enabled

Action: ○ Allow ● Deny

Summary: IF THEN *Deny*

IDE Step 8 – In the *Constraint Details* window, under *Attribute Category*, select *Device* and then scroll down and select *device-address*. Next, via the right hand side plane, select *Starts With*, make sure *Static Value* is selected and enter the first three digits of the MAC address. In our example, we are authenticating Siemens MAC addresses which start with "00:18:65" so we will enter *001865*. Click on *OK* when completed.



Constraint Details

Match The Following Rule:

Attribute Category: Device

- account-locked
- device-address
- device-group-member
- device-name
- device-vlan
- enable-password-expiration
- enable-start-time
- password-expiration
- source
- start-time
- type

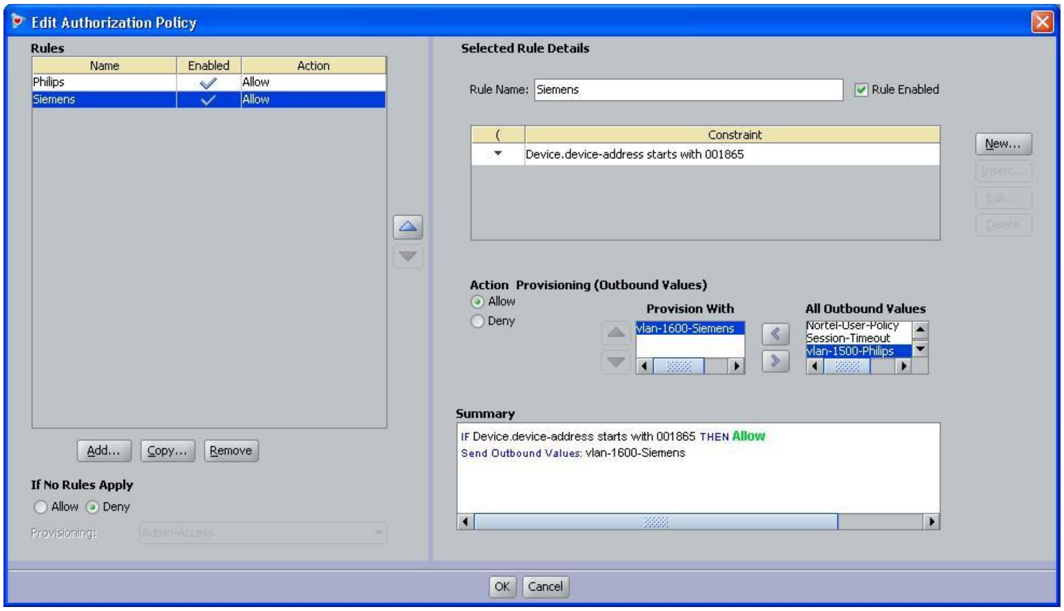
Attribute: device-address
Data type: MAC Address
Description: MAC address sent by authenticating device

Starts With

● Static Value ○ Dynamic Value of Attribute

001865

IDE Step 9 – Once back at the *Edit Authentication Policy* window, click the *Allow* radio button via *Action Provisioning* and move the attribute we configured above named *vlan-1600-Siemens* from *All Outbound Value* box to the *Provision With* box.



Edit Authorization Policy

Rules

Name	Enabled	Action
Philips	✓	Allow
Siemens	✓	Allow

Add... Copy... Remove

If No Rules Apply

○ Allow ● Deny

Provisioning: Admin-Access

Selected Rule Details

Rule Name: Siemens ☑ Rule Enabled

(	Constraint
	Device.device-address starts with 001865

New... Insert... Edit... Delete

Action Provisioning (Outbound Values)

● Allow

○ Deny

Provision With: vlan-1600-Siemens

All Outbound Values: Nortel-User-Policy, Session-Timeout, vlan-1500-Philips

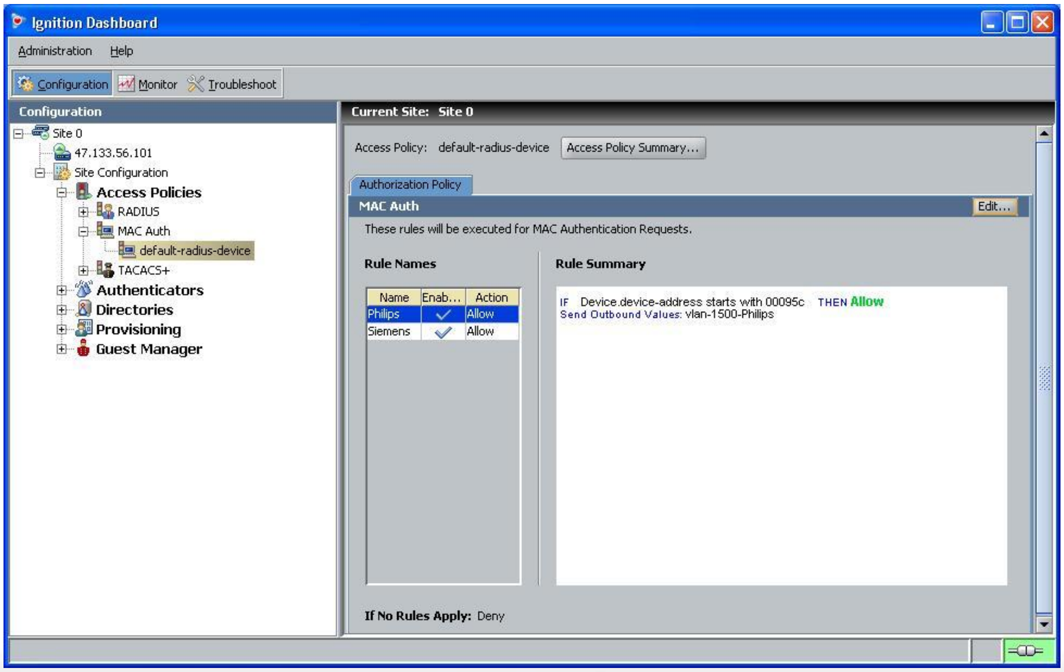
Summary

IF Device.device-address starts with 001865 THEN Allow

Send Outbound Values: vlan-1600-Siemens

OK Cancel

IDE Step 10 – Once completed, the policy should look something like the following. Click on the *Access Policy Summary* button next to verify the policy as shown below



Ignition Dashboard

Administration Help

Configuration Monitor Troubleshoot

Configuration

- Site 0
  - 47.133.56.101
  - Site Configuration
    - Access Policies
      - RADIUS
      - MAC Auth
        - default-radius-device
      - TACACS+
    - Authenticators
    - Directories
    - Provisioning
    - Guest Manager

Current Site: Site 0

Access Policy: default-radius-device Access Policy Summary...

Authorization Policy

MAC Auth Edit...

These rules will be executed for MAC Authentication Requests.

Rule Names

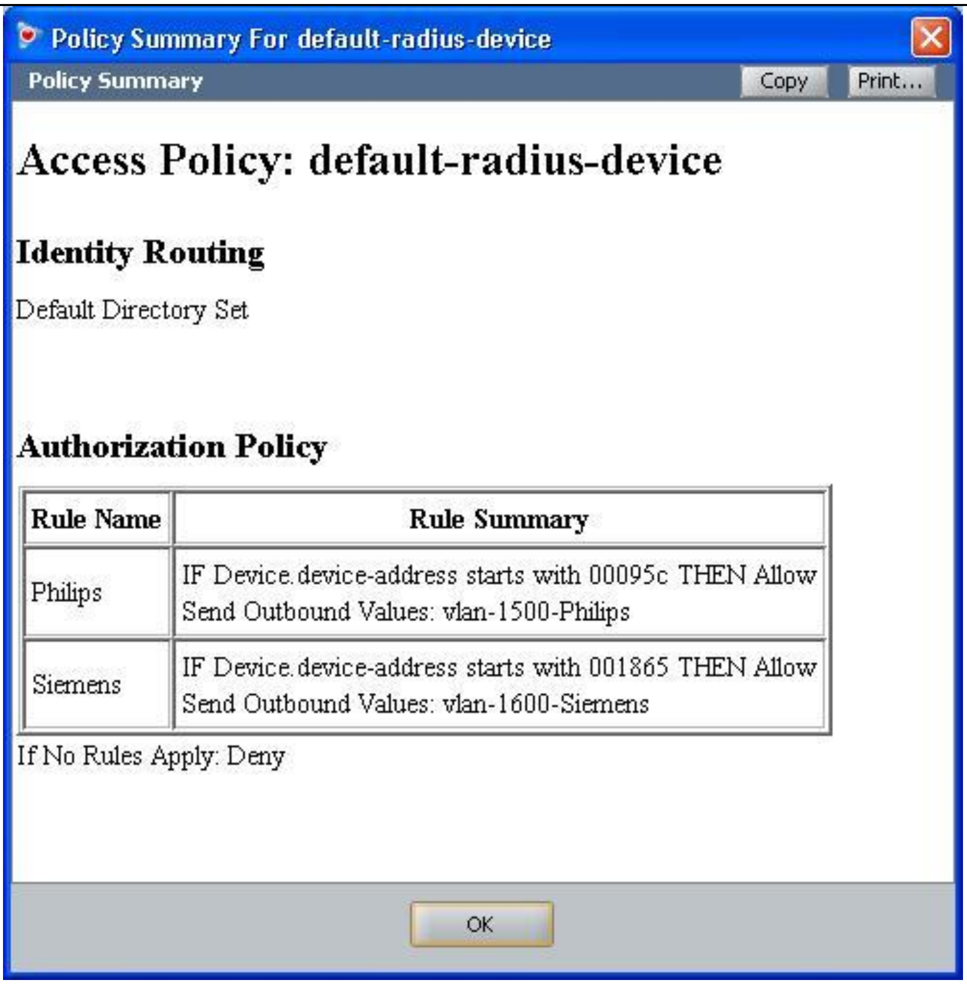
Name	Enab...	Action
Philips	✓	Allow
Siemens	✓	Allow

Rule Summary

IF Device.device-address starts with 00095c THEN Allow

Send Outbound Values: vlan-1500-Philips

If No Rules Apply: Deny



Access Policy: default-radius-device

Identity Routing

Default Directory Set

Authorization Policy

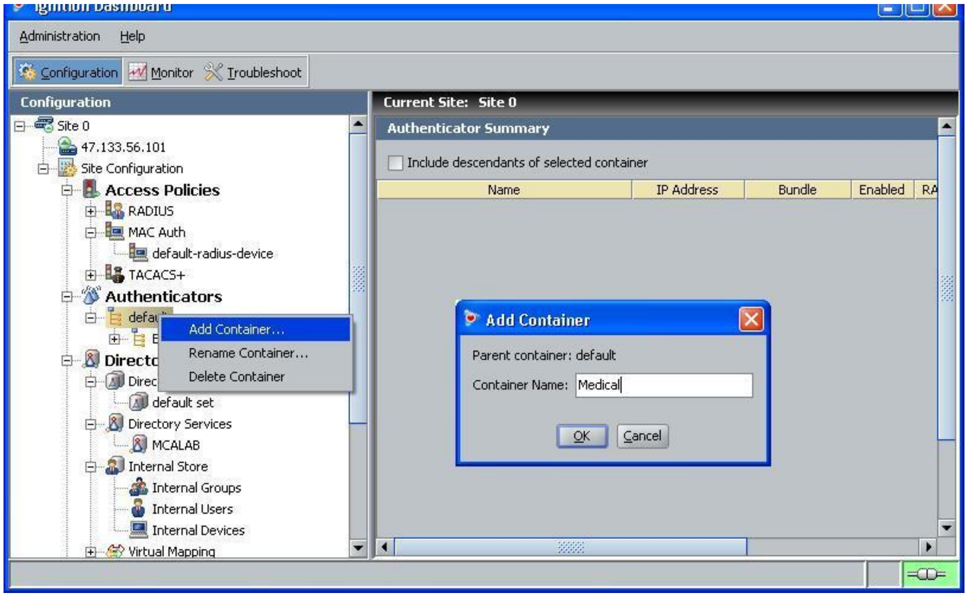
Rule Name	Rule Summary
Philips	IF Device.device-address starts with 00095c THEN Allow Send Outbound Values: vlan-1500-Philips
Siemens	IF Device.device-address starts with 001865 THEN Allow Send Outbound Values: vlan-1600-Siemens

If No Rules Apply: Deny

1.4.3.4 Add the Nortel switches as authenticators

For Ignition Server to process the Avaya switch RADIUS requests, each switch must be added as an Authenticator.

IDE Step 1 – Go to *Site Configuration -> Authenticators -> default.* For example, we will create new container named *Medical* by right clicking *default* and selecting *Add Container*.

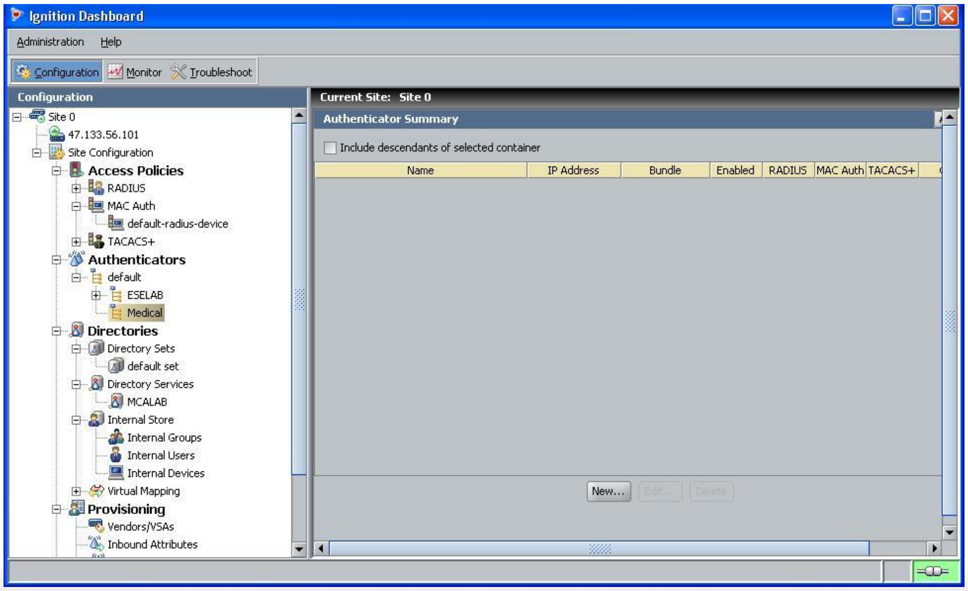


Add Container

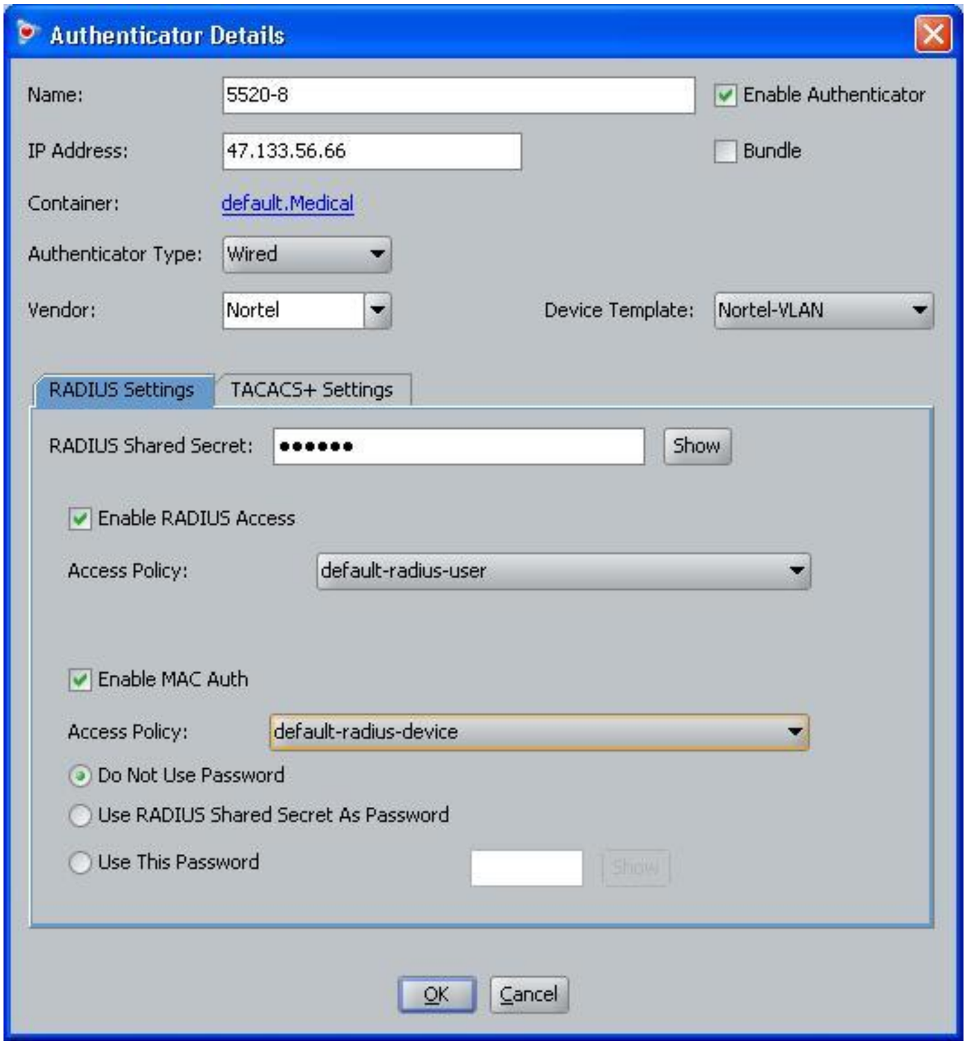
Parent container: default

Container Name: Medical

IDE Step 2 – Go to *Site Configuration -> Authenticators -> default -> Medical* and click on *New.*



IDE Step 3 – Enter the settings as shown below. For the *Device Template*, select the template we created in the section above titled “Create a new Nortel device template”, *Nortel-VLAN* as used in our example. Make sure *Enable MAC Auth* is checked off and *Do Not Use Password* is selected to allow device authentication. You can leave *Enable RADIUS Access* checked off if you like for user authentication, but, it is not required for this example. Click on *OK* when done.



Authenticator Details

Name: 5520-8

☑ Enable Authenticator

IP Address: 47.133.56.66

□ Bundle

Container: default.Medical

Authenticator Type: Wired

Vendor: Nortel

Device Template: Nortel-VLAN

RADIUS Shared Secret: ●●●●●●

☑ Enable RADIUS Access

Access Policy: default-radius-user

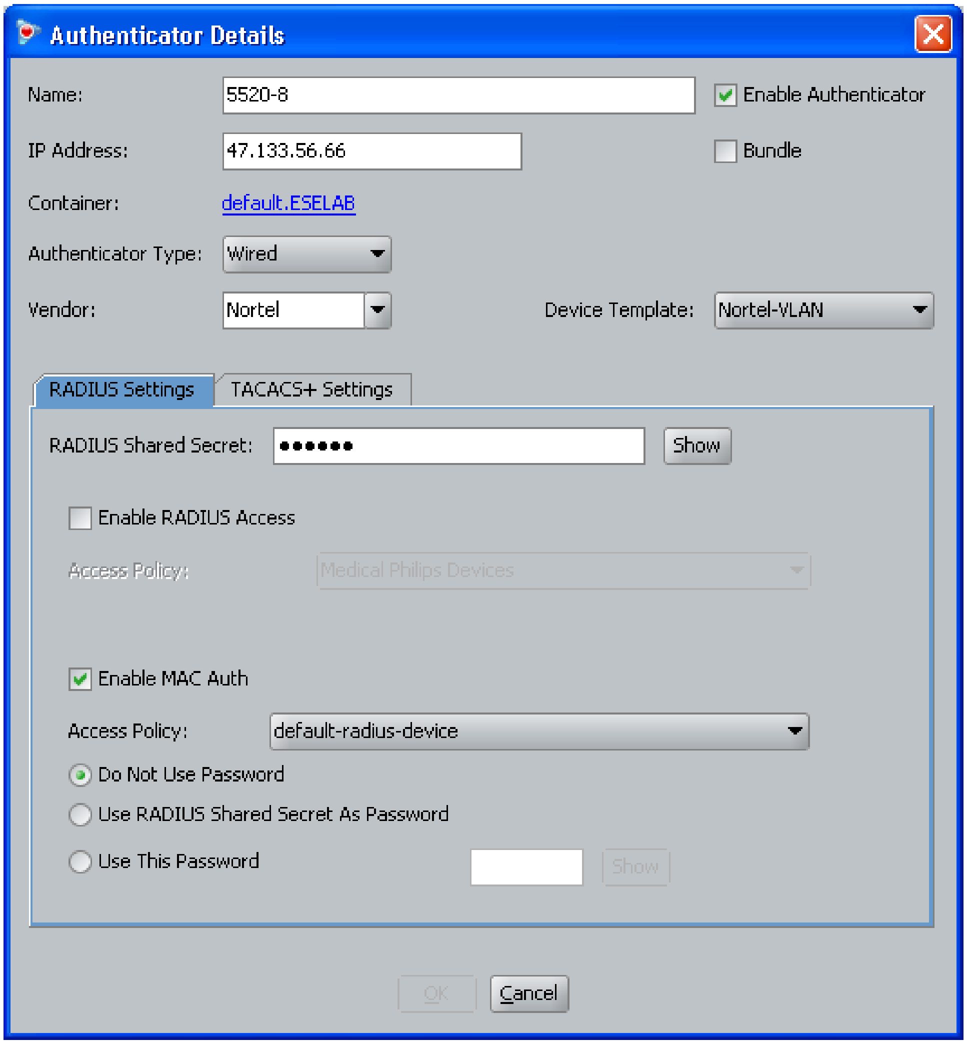
☑ Enable MAC Auth

Access Policy: default-radius-device

● Do Not Use Password

○ Use RADIUS Shared Secret As Password

○ Use This Password



Authenticator Details

Name: 5520-8 ☑ Enable Authenticator

IP Address: 47.133.56.66 □ Bundle

Container: default.ESELAB

Authenticator Type: Wired

Vendor: Nortel Device Template: Nortel-VLAN

RADIUS Settings | TACACS+ Settings

RADIUS Shared Secret: •••••• Show

□ Enable RADIUS Access

Access Policy: Medical Philips Devices

☑ Enable MAC Auth

Access Policy: default-radius-device

● Do Not Use Password

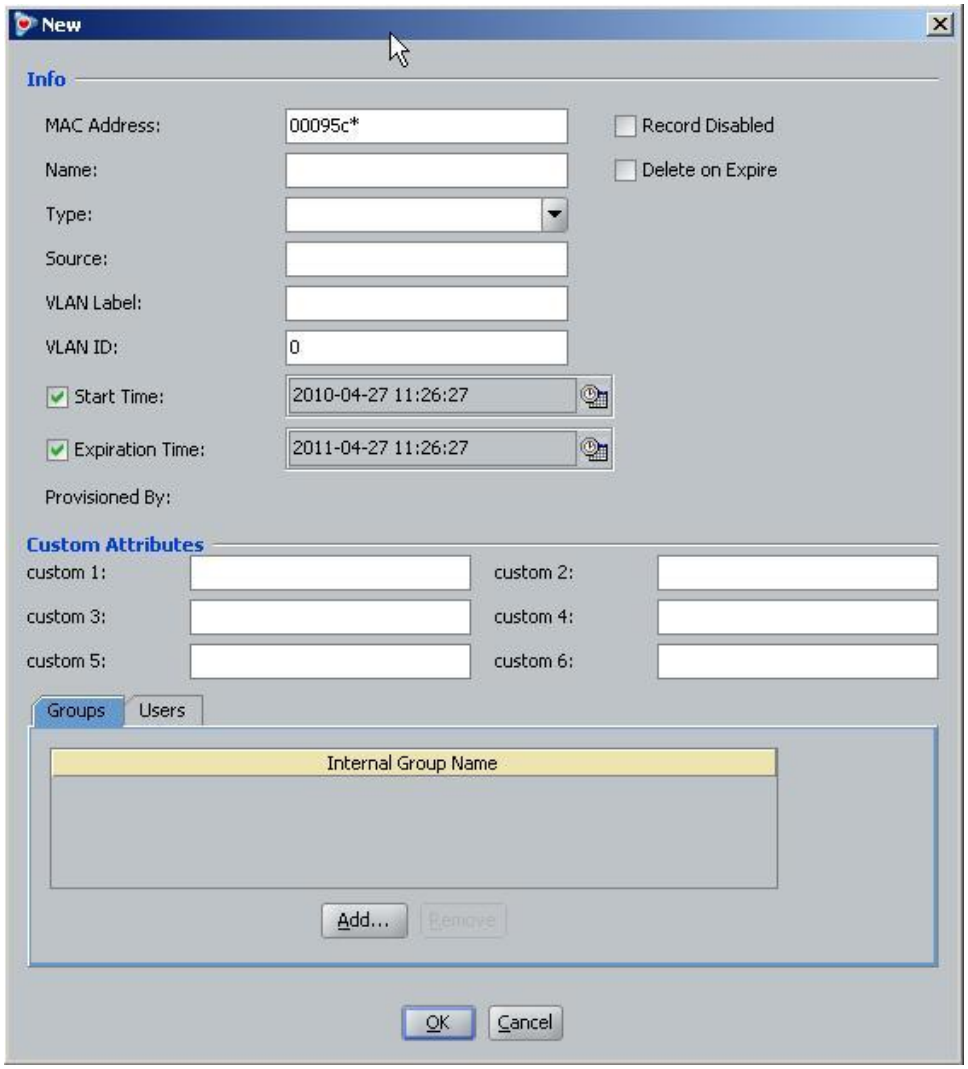
○ Use RADIUS Shared Secret As Password

○ Use This Password Show

1.4.3.5 Add Internal Devices

Next, we will add the vendor MAC prefix via the Internal Store on Ignition Server.

IDE Step 1 – Go to *Site Configuration -> Directories -> Internal Store -> Internal Devices.* First, we will add the MAC prefix for Philips. Via the Internal Devices window. Click on *New* and enter the MAC prefix *00095c as shown below and click *OK* when done.**



New

Info

MAC Address: 00095c*

☐ Record Disabled

Name:

☐ Delete on Expire

Type:

Source:

VLAN Label:

VLAN ID: 0

☑ Start Time: 2010-04-27 11:26:27

☑ Expiration Time: 2011-04-27 11:26:27

Provisioned By:

Custom Attributes

custom 1:

custom 2:

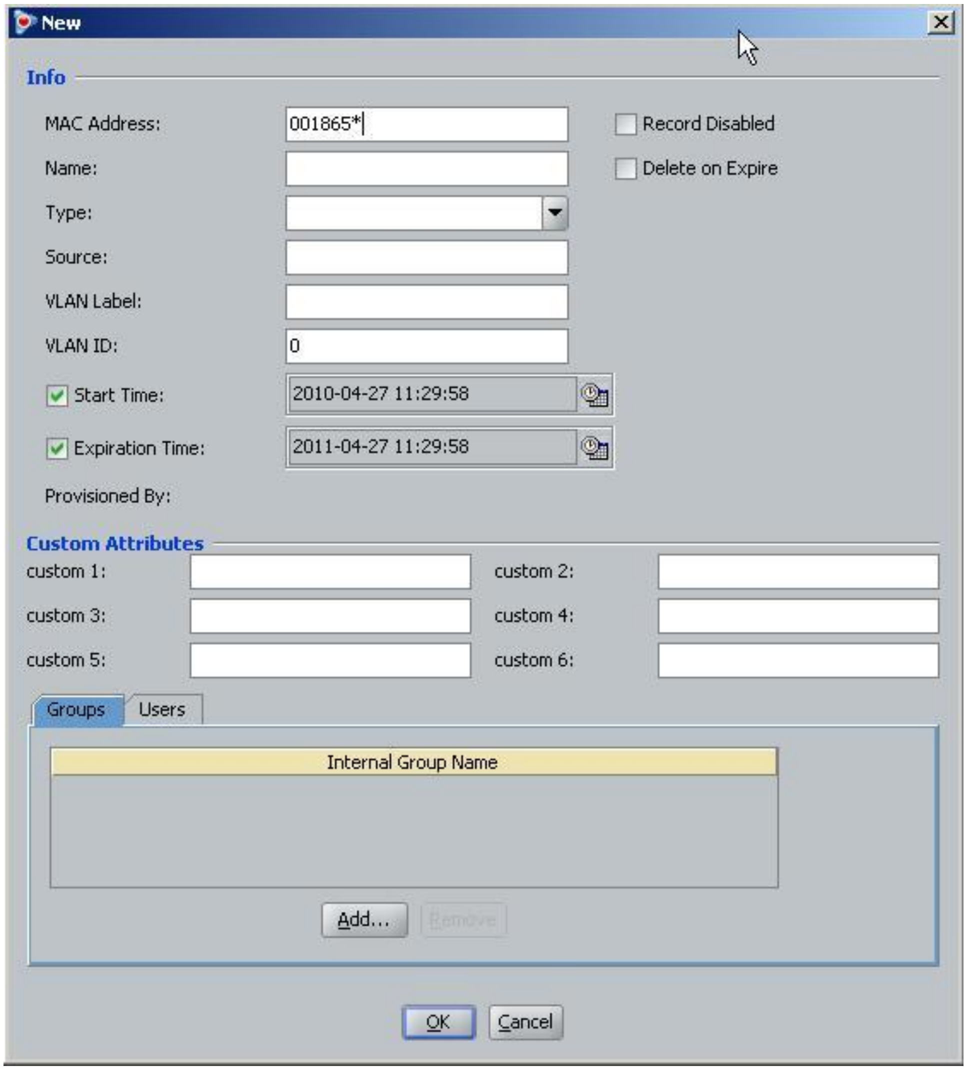
custom 3:

custom 4:

custom 5:

custom 6:

IDE Step 2 – Go to *Site Configuration -> Directories -> Internal Store -> Internal Devices.* Next, we will add the MAC prefix for Siemens Via the Internal Devices window. Click on *New* and enter the MAC prefix *001865* as shown below and click *OK* when done.**



MAC Address: 001865*

□ Record Disabled

Name:

□ Delete on Expire

Type:

Source:

VLAN Label:

VLAN ID: 0

☑ Start Time: 2010-04-27 11:29:58

☑ Expiration Time: 2011-04-27 11:29:58

Provisioned By:

custom 1:

custom 2:

custom 3:

custom 4:

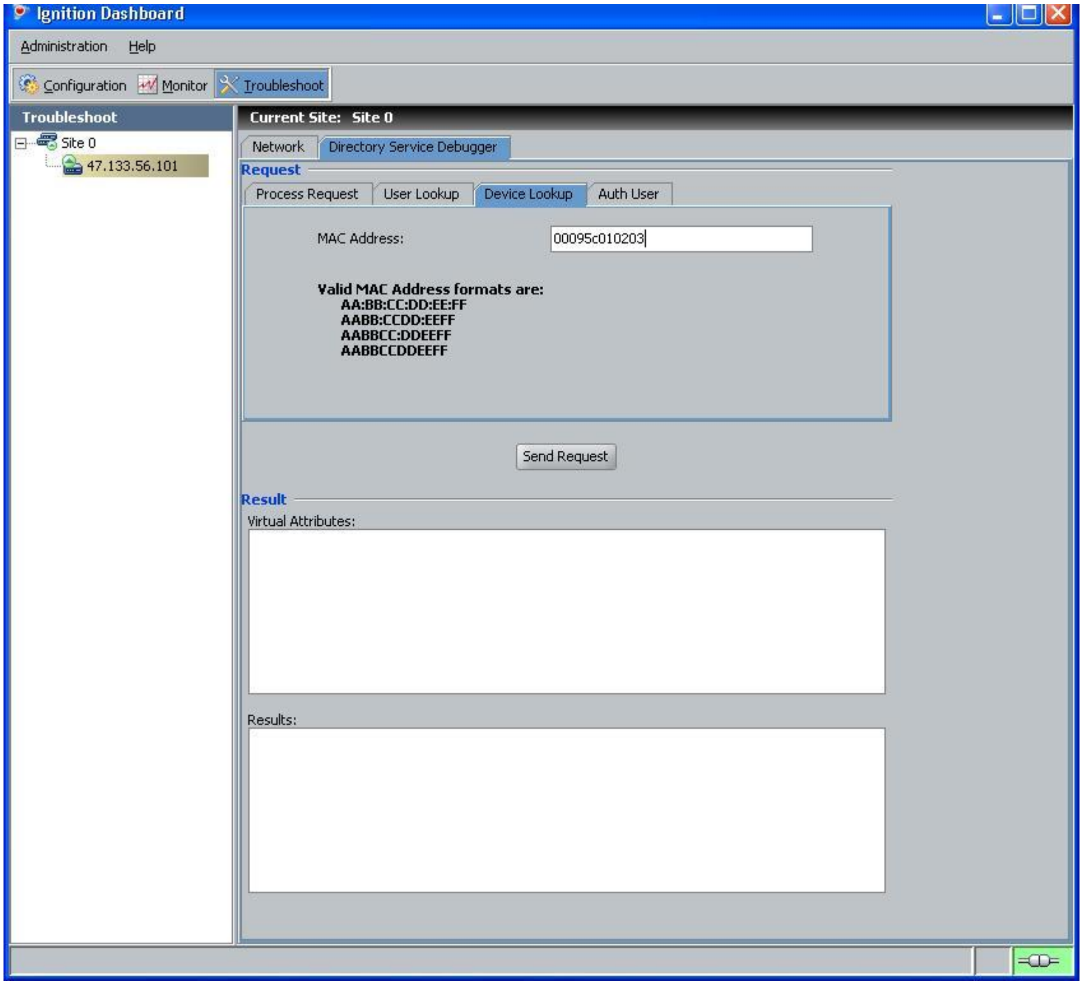
custom 5:

custom 6:

1.4.4 Verify IDE Device Authentication

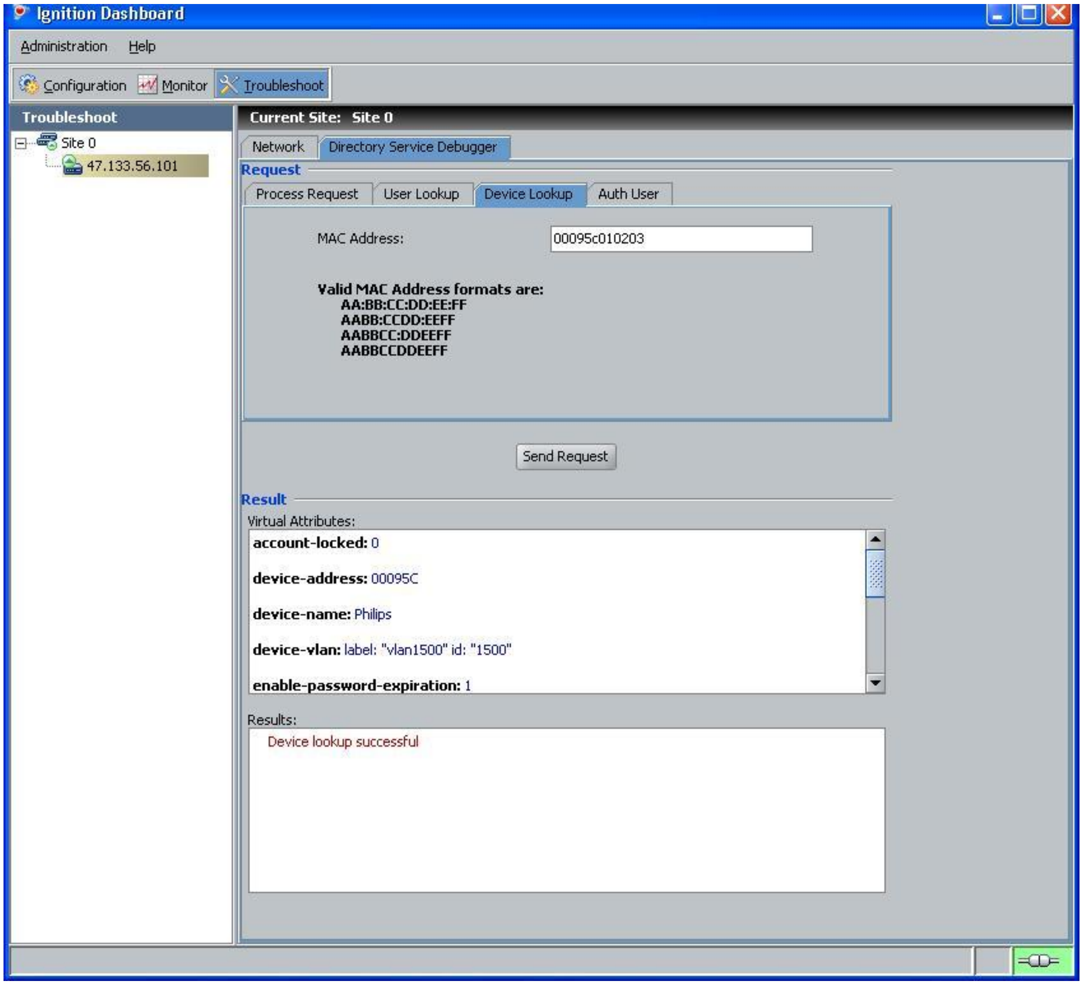
You can test a device lookup and authentication by using the Ignition Server Advanced Troubleshooting feature. For example, let’s assume we wish to test a Philips device which starts with a vendor MAC of “00:09:5c”.

Step 1 – Via Ignition Dashboard, select the IP address of the Ignition Server, click on the *Troubleshoot* tab, go to *Directory Service Debugger* and select the *Device Lookup* tab. Enter a valid MAC address to test such as *00095c010203* and click on the *Send Request* button.



MAC Address: 00095c010203

Valid MAC Address formats are:
AA:BB:CC:DD:EE:FF
AABB:CCDD:EEFF
AABBCC:DDEEFF
AABBCCDDEEFF

Result:


MAC Address: 00095c010203

Valid MAC Address formats are:
AA:BB:CC:DD:EE:FF
AABB:CCDD:EEFF
AABBCC:DDEEFF
AABBCCDDEEFF

Virtual Attributes:

account-locked: 0

device-address: 00095C

device-name: Philips

device-vlan: label: "vlan1500" id: "1500"

enable-password-expiration: 1

Results:

Device lookup successful

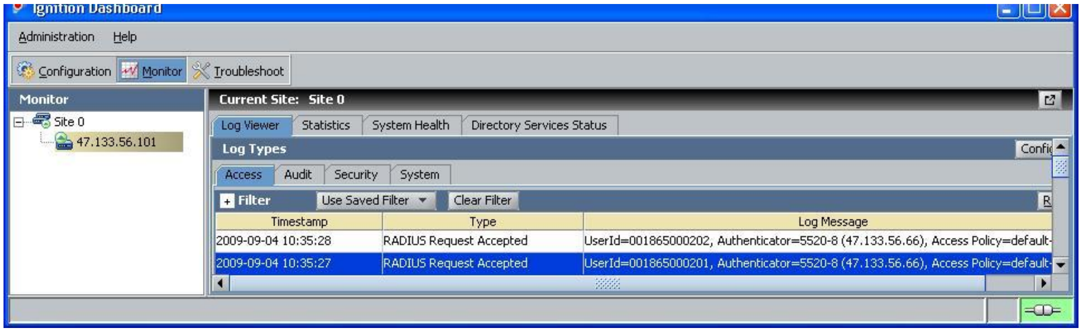
Via Dashboard, verify the following information:

Option	Verify
Results	First of all, if successful, ***Device lookup successful*** should be displayed
Virtual Attributes	Verify the following pertaining to the configuration used in this example: • Account-locked: ***0*** (0 indicates account is not locked) • Device-address: ***00095c*** • Device-name: ***Philips*** • Device-vlan: label: ***“vlan1500” id: “1500”***

1.4.5 Verify device authentication from ERS switch

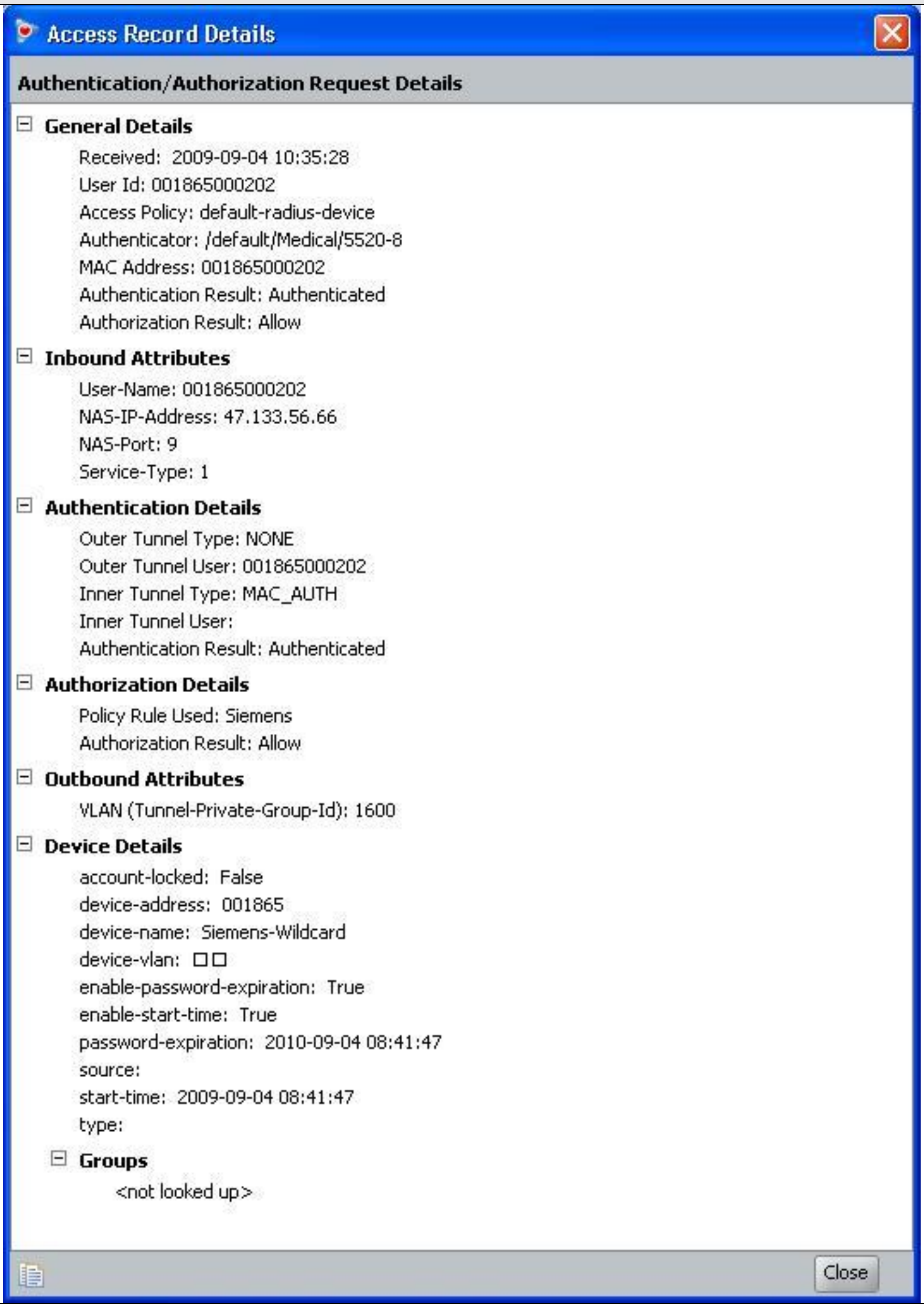
You can view the authentication details for each device and user via Ignition Dashboard which provides extensive details about the device or user. From here you can get the full MAC address for the device, what port was used on the authenticator switch, and various details pertaining to the device such as RADIUS attributes and device details. Knowing this information, you could keep a database of all medical device identifiers and the switch and port number this device is attached to. If you like, you could then setup RADIUS user authentication for an individual MAC address instead of device authentication using a MAC wildcard.

Step 1 – In Dashboard, select the IP address of the Ignition Server and click on the *Monitor* tab, go to *Log Viewer,* and select the *Access* tab. Via the message of a valid device, right-click the message and select *Access Record Details*.



Timestamp	Type	Log Message
2009-09-04 10:35:28	RADIUS Request Accepted	UserId=001865000202, Authenticator=5520-8 (47.133.56.66), Access Policy=default-
2009-09-04 10:35:27	RADIUS Request Accepted	UserId=001865000201, Authenticator=5520-8 (47.133.56.66), Access Policy=default-

Result:



Authentication/Authorization Request Details

⊟ General Details

Received: 2009-09-04 10:35:28
User Id: 001865000202
Access Policy: default-radius-device
Authenticator: /default/Medical/5520-8
MAC Address: 001865000202
Authentication Result: Authenticated
Authorization Result: Allow

⊟ Inbound Attributes

User-Name: 001865000202
NAS-IP-Address: 47.133.56.66
NAS-Port: 9
Service-Type: 1

⊟ Authentication Details

Outer Tunnel Type: NONE
Outer Tunnel User: 001865000202
Inner Tunnel Type: MAC_AUTH
Inner Tunnel User:
Authentication Result: Authenticated

⊟ Authorization Details

Policy Rule Used: Siemens
Authorization Result: Allow

⊟ Outbound Attributes

VLAN (Tunnel-Private-Group-Id): 1600

⊟ Device Details

account-locked: False
device-address: 001865
device-name: Siemens-Wildcard
device-vlan: □□
enable-password-expiration: True
enable-start-time: True
password-expiration: 2010-09-04 08:41:47
source:
start-time: 2009-09-04 08:41:47
type:

⊟ Groups

<not looked up>

At minimum, verify the following items:

Option	Verify
Authentication Result	If successful, ***Authenticated*** should be displayed. If not, verify the device using the previous step and if this also fails, verify the Ignition Server configuration.
Authorization Result	If successful, ***Allow*** should be displayed. If not, verify the device using the previous step and if this also fails, verify the Ignition Server configuration.
User Id	This field displays the full MAC address of the device.
Access Policy	This field displays the Ignition Server policy used for this device. It should match the configuration you used for this device.
NAS-Port	This is useful information in that it displays the port number on the Avaya ERS switch where device is on. You can use this information to keep track if each device MAC address and what port on the switch the device is connected to.

1.4.6 Adding User Based Policies (UBP) Option

The ERS 5500 and ERS 5600 both support User Based Policies (UBP) that can be used with EAP or non-EAP MAC authentication. UBP filter sets can be configured locally on the switch and applied upon an EAP Supplicant or non-EAP device successfully authenticating against a RADIUS server. Once the EAP Supplicate or non-EAP device is authenticated by RADIUS, the RADIUS server can be setup to send a RADIUS attribute for UBP. The RADIUS return attribute for UBP is simply the UBP filter set name. This allows you to configure different UBP filter sets and have RADIUS tell the switch what policy to apply based on the user or device credentials.

The following command is used to configure UBP:

- ERS5520(config)#***qos ubp classifier name <Word 1..16 character string> ?***

```
addr-type      Specify the address type (IPv4, IPv6) classifier criteria
block          Specify the label to identify access-list elements that are of
               the same block
drop-action    Specify the drop action
ds-field       Specify the DSCP classifier criteria
dst-ip         Specify the destination IP classifier criteria
dst-mac        Specify the destination MAC classifier criteria
dst-port-min   Specify the L4 destination port minimum value classifier
               criteria
ethertype      Specify the ethertype classifier criteria
eval-order     Specify the evaluation order
flow-id        Specify the IPv6 flow identifier classifier criteria
next-header    Specify the IPv6 next header classifier criteria
priority       Specify the user priority classifier criteria
protocol       Specify the IPv4 protocol classifier criteria
set-drop-prec  Specify the set drop precedence
src-ip         Specify the source IP classifier criteria
src-mac        Specify the source MAC classifier criteria
src-port-min   Specify the L4 source port minimum value classifier criteria
update-1p      Specify the update user priority
update-dscp    Specify the update DSCP
vlan-min       Specify the Vlan ID minimum value classifier criteria
vlan-tag       Specify the vlan tag classifier criteria
<cr>
```

Assuming we wish to add UBP configuration to this example, please following the configuration steps shown below.

1.4.6.1 ERS5520 Policy Configuration

Although any number of items can be configured for the policy, we will create two simply policies to remark all traffic from the Philips VLAN with a DSCP value of 26 (Gold) and remark all traffic from the Siemens VLAN with a DSCP value of 16 (Silver).

ERS5520-1 Step 1 – Configure a policy using the name 'philips' and remark DSCP with a DSCP value of 26. We will set the eval-order to 5 (value from 1-255) in case you wish to add additional filters in the future with a higher preference.

```
5520-24T-1(config)# qos ubp classifier name philips ethertype 0x0800 update-dscp
26 eval-order 5
```

ERS5520-1 Step 2 – Enable the UBP set

```
5520-24T-1(config)# qos ubp set name philips
```

ERS5520-1 Step 3 – Configure a policy using the name ‘philips’ and remark DSCP with a DSCP value of 26. We will set the eval-order to 5 (value from 1-255) in case you wish to add additional filters in the future with a higher preference.

```
5520-24T-1(config)# qos ubp classifier name siemens ethertype 0x0800 update-dscp
16 eval-order 5
```

ERS5520-1 Step 4 – Enable the UBP set

```
5520-24T-1(config)# qos ubp set name siemens
```

ERS5520-1 Step 3 – Enable ubp

```
5520-24T-1(config)# qos agent ubp high-security-local
```

The default ubp classifier action non-match action is for forward traffic. In older software releases for the ERS5500, this was not the case and you had to enter the command *qos ubp set name <policy_name> drop-nm-action disable*. You can quickly check to see if the software versions you are using require the drop non-match action by simple typing in *qos ubp set name philips ?* and checking if the command *drop-nm-action* is displayed or not.

1.4.6.2 Enable EAP User Based Policies at Global Level

ERS5520-1 Step 1 – Enable EAP user-based Policies

```
5520-24T-1(config)# eapol user-based-policies enable
```

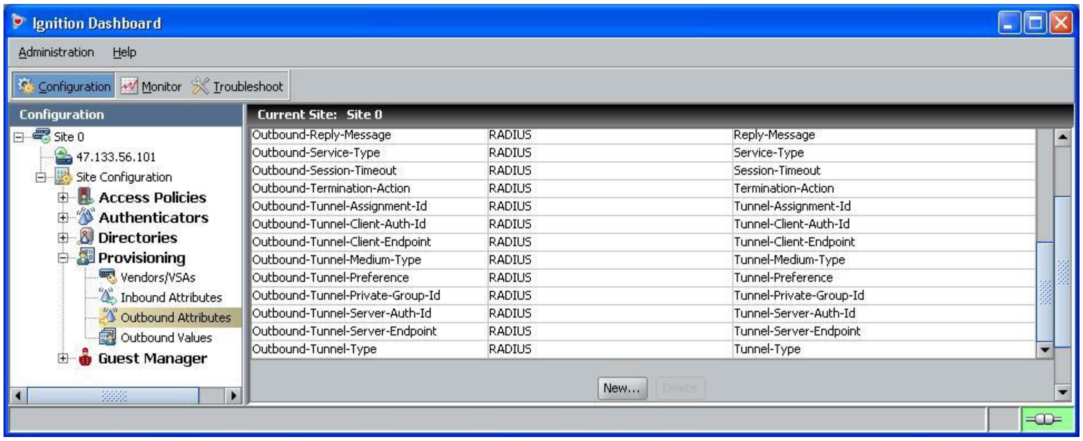
ERS5520-1 Step 2 – Enable EAP multihost NEAP policies

```
5520-24T-1(config)# eapol multihost non-eap-user-based-policies enable
```

1.4.6.3 IDE Policy Setup

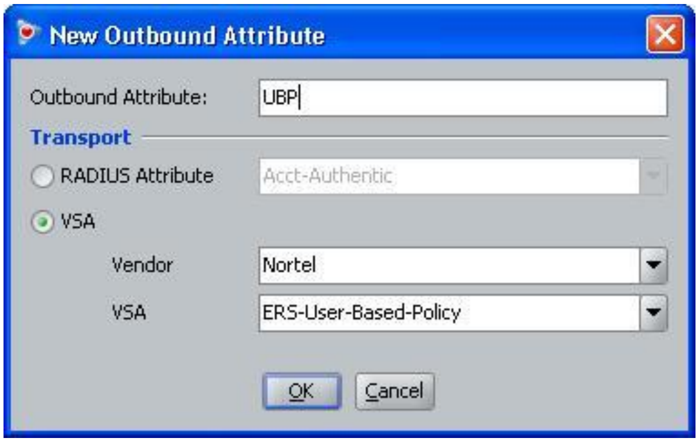
On the RADIUS server, Nortel Specific Option 562 using Vendor-assigned attribute number 110 is used by setting the string value to the policy configured on the ERS5520 switch with the string always starting with "UROL" and then the policy name – i.e *UROLphilips* and *UROLsiemens* as per the policies configured on ERS5520-1. On Ignition Server, the Nortel vendor VSA definitions are already defined and can be viewed by using Ignition Dashboard and going to *Site Configuration -> Provisioning -> Vendors/VSAs -> Nortel -> VSA Definitions* where the attribute used for UBP is named *ERS-User-Based-Policy*.

IDE Step 1 – Go to *Site Configuration ->Provisioning -> Outbound Attributes* and click on *New*.



Outbound-Reply-Message	RADIUS	Reply-Message
Outbound-Service-Type	RADIUS	Service-Type
Outbound-Session-Timeout	RADIUS	Session-Timeout
Outbound-Termination-Action	RADIUS	Termination-Action
Outbound-Tunnel-Assignment-Id	RADIUS	Tunnel-Assignment-Id
Outbound-Tunnel-Client-Auth-Id	RADIUS	Tunnel-Client-Auth-Id
Outbound-Tunnel-Client-Endpoint	RADIUS	Tunnel-Client-Endpoint
Outbound-Tunnel-Medium-Type	RADIUS	Tunnel-Medium-Type
Outbound-Tunnel-Preference	RADIUS	Tunnel-Preference
Outbound-Tunnel-Private-Group-Id	RADIUS	Tunnel-Private-Group-Id
Outbound-Tunnel-Server-Auth-Id	RADIUS	Tunnel-Server-Auth-Id
Outbound-Tunnel-Server-Endpoint	RADIUS	Tunnel-Server-Endpoint
Outbound-Tunnel-Type	RADIUS	Tunnel-Type

IDE Step 2 – Enter an appropriate name in the *Outbound Attribute* window (i.e. UBP as used in this example), select VSA Vendor *Nortel* and VSA value *ERS-User-Based-Policy* as shown below.



Outbound Attribute: UBP

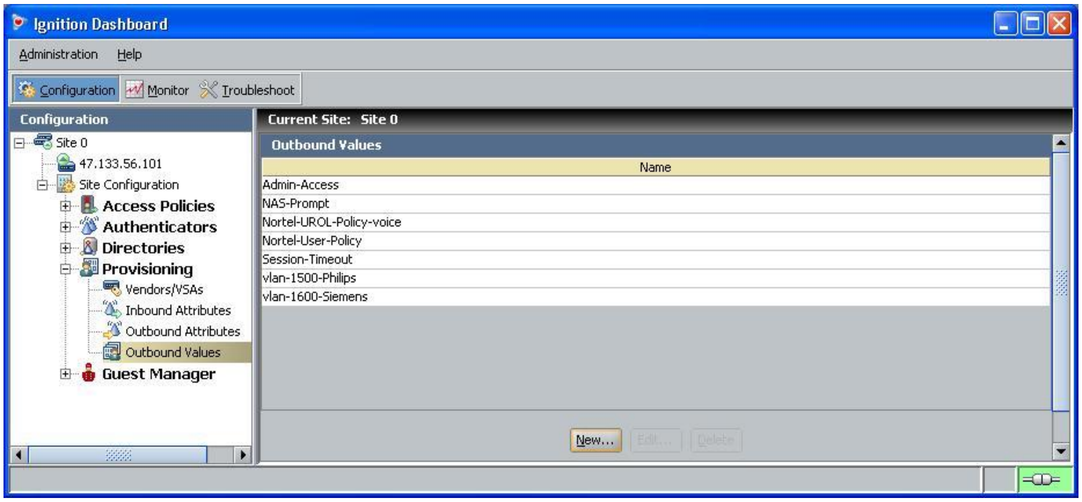
○ RADIUS Attribute: Acct-Authentic

● VSA

Vendor: Nortel

VSA: ERS-User-Based-Policy

IDE Step 3 – Go to *Site Configuration ->Provisioning -> Outbound Values* and click on *New*.

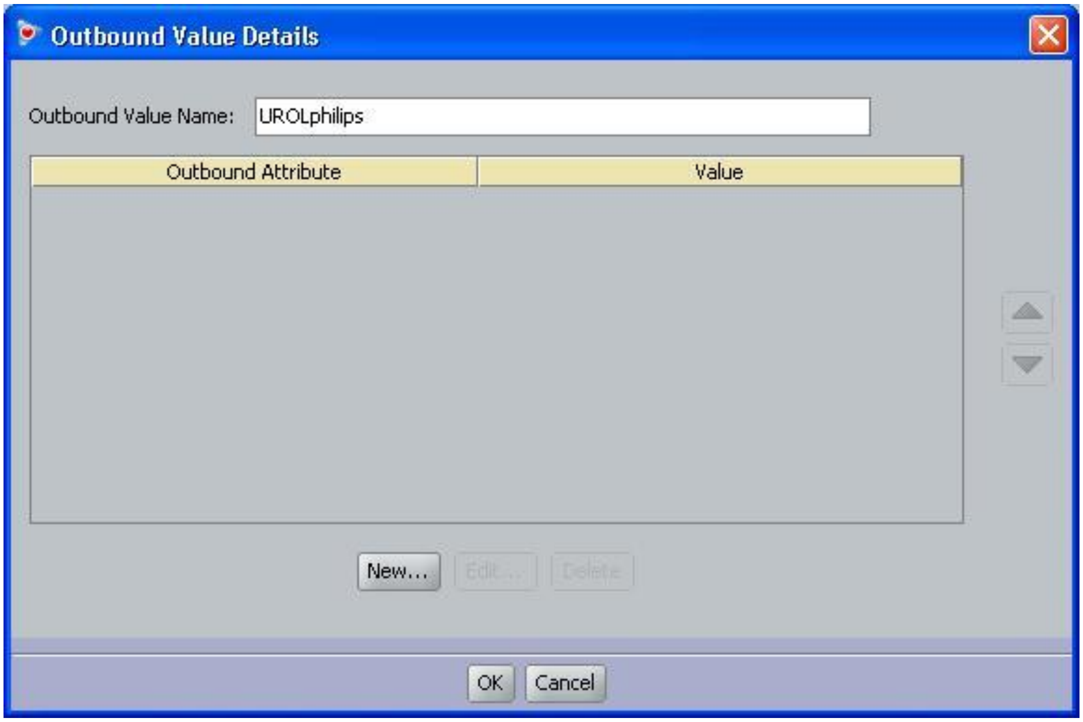


Current Site: Site 0

Outbound Values

Name
Admin-Access
NAS-Prompt
Nortel-UROL-Policy-voice
Nortel-User-Policy
Session-Timeout
vlan-1500-Philips
vlan-1600-Siemens

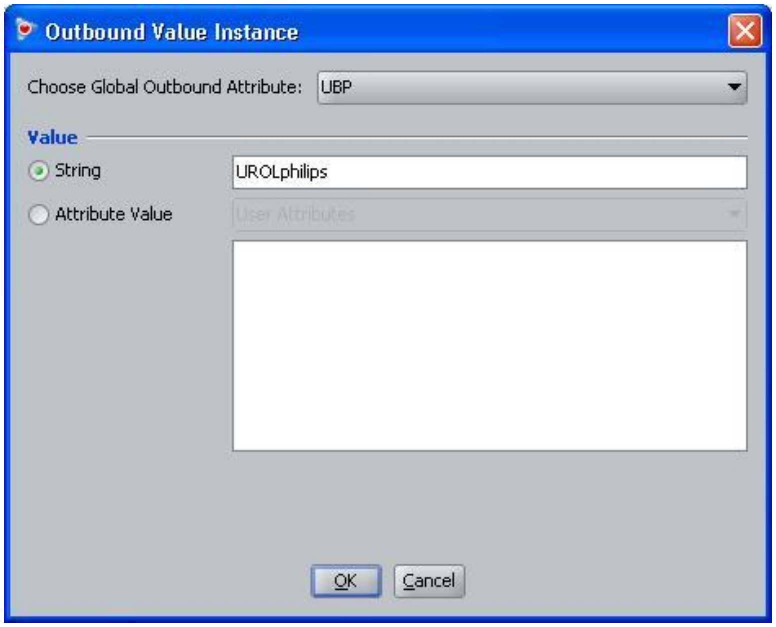
IDE Step 4 – When the *Outbound Value Details* window pops up, enter a name (i.e. UROLphilips as used in this example) via the *Outbound Value Name* window and click on *New*.



Outbound Value Name: UROLphilips

Outbound Attribute	Value

IDE Step 5 – When the *Outbound Value instance* window pops up, under *Choose Global Outbound Attribute:* and select the outbound attribute name from step 2 above. Select *Value* of *String* and enter string name of *UROLphilips* for the UBP name of "*philips"* configured for the Philips devices on the ERS5520 switch. Click on OK twice.

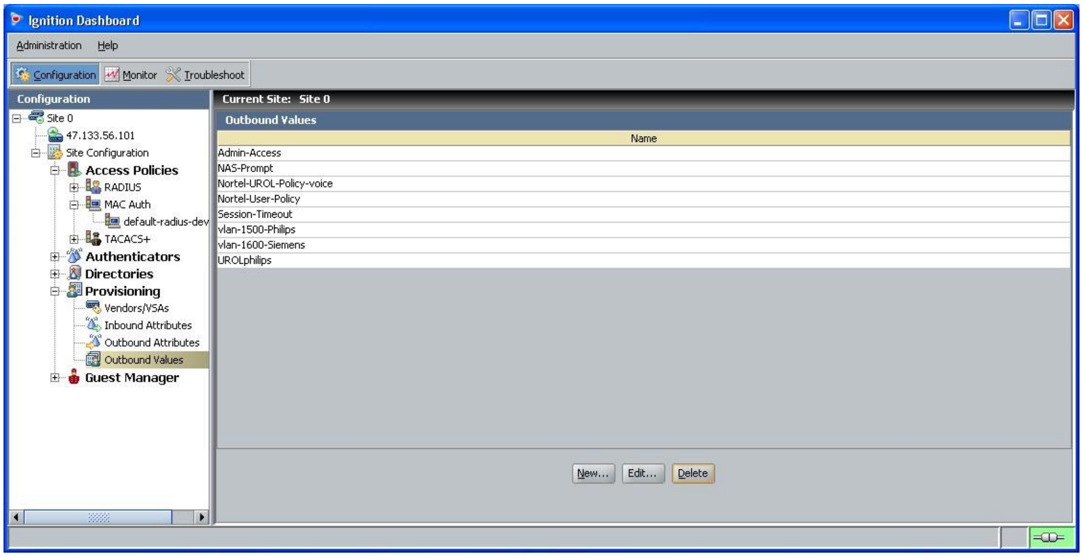


Choose Global Outbound Attribute: UBP

● String: UROLphilips

○ Attribute Value

IDE Step 6 – Via *Site Configuration ->Provisioning -> Outbound Values* and click on *New* one more time to add the outbound attribute for the Siemens devices

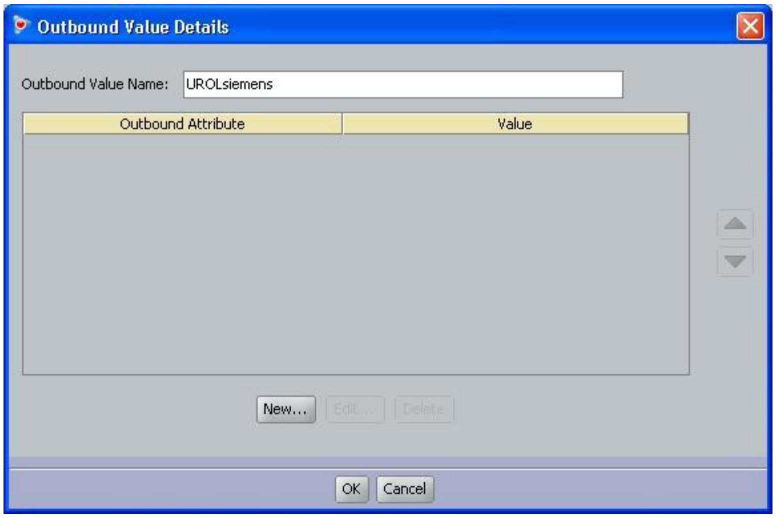


Current Site: Site 0

Outbound Values

Name
Admin-Access
NAS-Prompt
Nortel-UROL-Policy-voice
Nortel-User-Policy
Session-Timeout
vlan-1500-Philips
vlan-1600-Siemens
UROLphilips

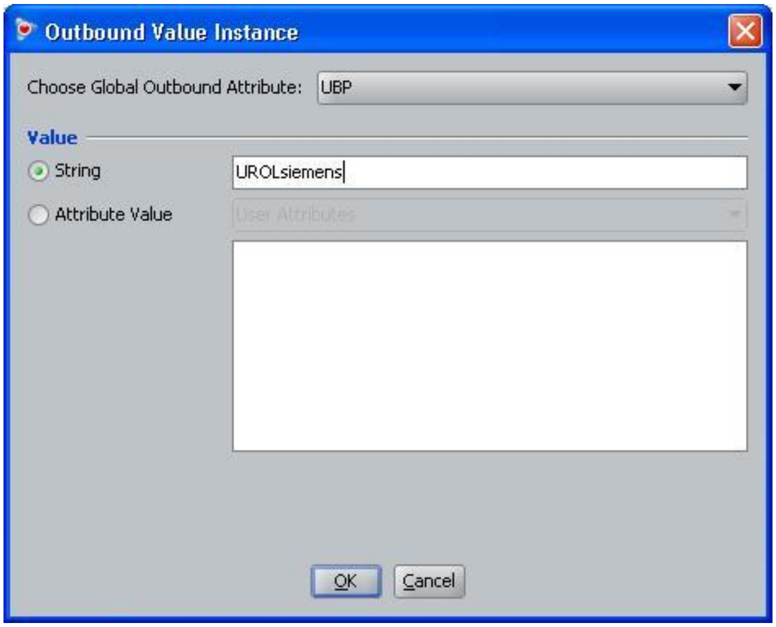
IDE Step 7 – When the *Outbound Value Details* window pops up, enter a name (i.e. UROLsiemens as used in this example) via the *Outbound Value Name* window and click on *New*.


Outbound Value Details

Outbound Value Name: UROLsiemens

Outbound Attribute	Value

IDE Step 8 – When the *Outbound Value instance* window pops up, under *Choose Global Outbound Attribute:* and select the outbound attribute name from step 2 above. Select *Value* of *String* and enter string name of *UROLsiemenss* for the UBP name of "*siemens"* configured for the Philips devices on the ERS5520 switch. Click on OK twice.


Outbound Value Instance

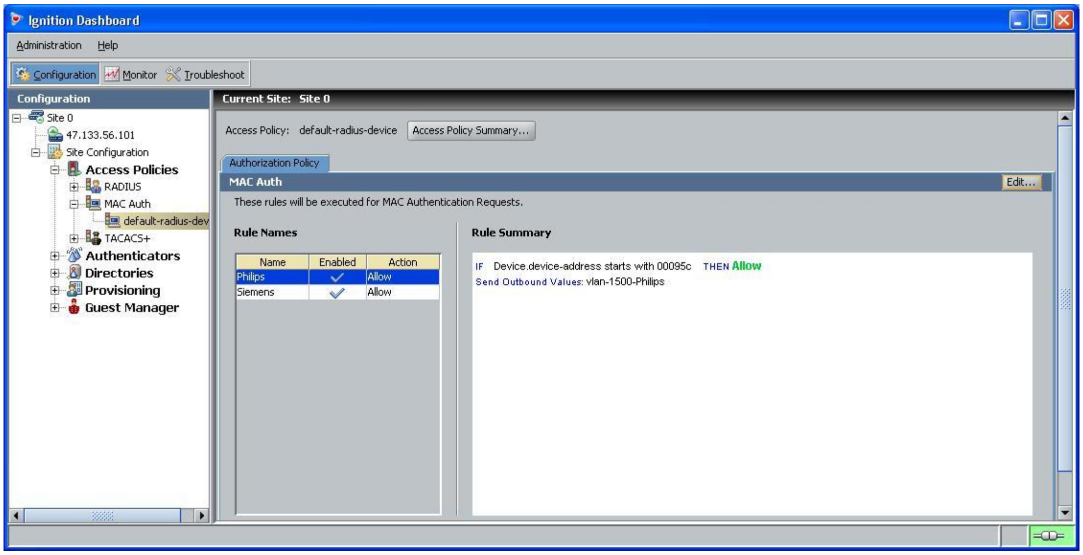
Choose Global Outbound Attribute: UBP

Value

● String: UROLsiemens

○ Attribute Value: User Attributes

IDE Step 9 – Go to *Site Configuration -> Access Policies -> MAC Auth -> default-radius-device* and via the *Authorization Policy* tab, select *Philips* and click on *Edit*



Current Site: Site 0

Access Policy: default-radius-device

MAC Auth

These rules will be executed for MAC Authentication Requests.

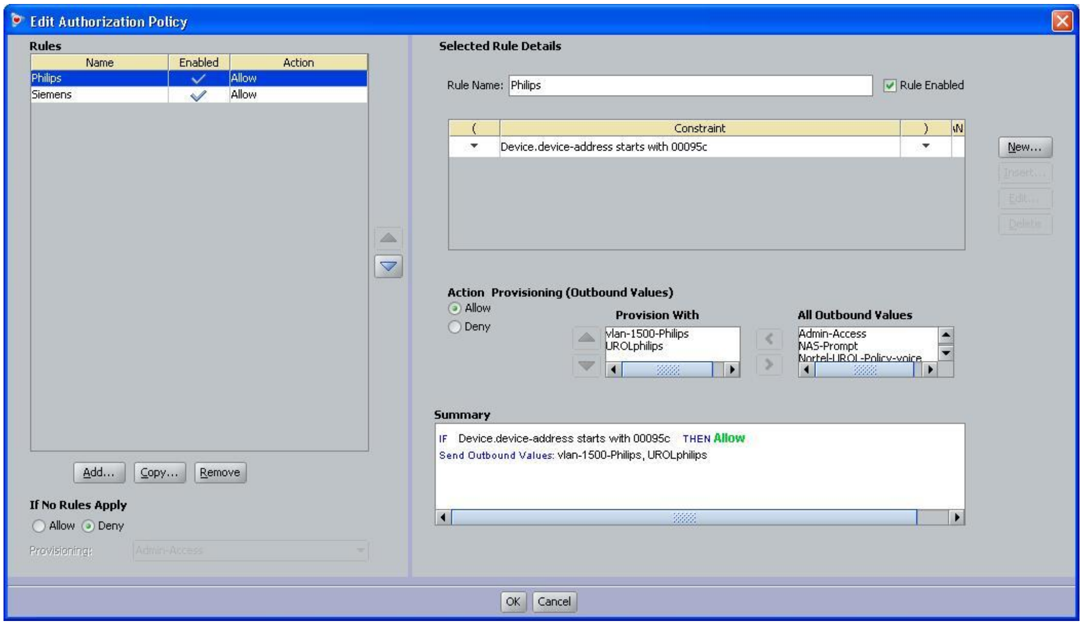
Rule Names

Name	Enabled	Action
Philips	✓	Allow
Siemens	✓	Allow

Rule Summary

IF Device.device-address starts with 00095c THEN Allow
Send Outbound Values: vlan-1500-Philips

IDE Step 10 – Move the attribute we configured above named *UROLphilips* from *All Outbound Value* box to the *Provision With* box and click *OK*.



Rules

Name	Enabled	Action
Philips	✓	Allow
Siemens	✓	Allow

If No Rules Apply
○ Allow ● Deny
Provisioning: Admin-Access

Selected Rule Details

Rule Name: Philips ☑ Rule Enabled

(	Constraint	)	N
	Device.device-address starts with 00095c		

Action Provisioning (Outbound Values)
● Allow
○ Deny

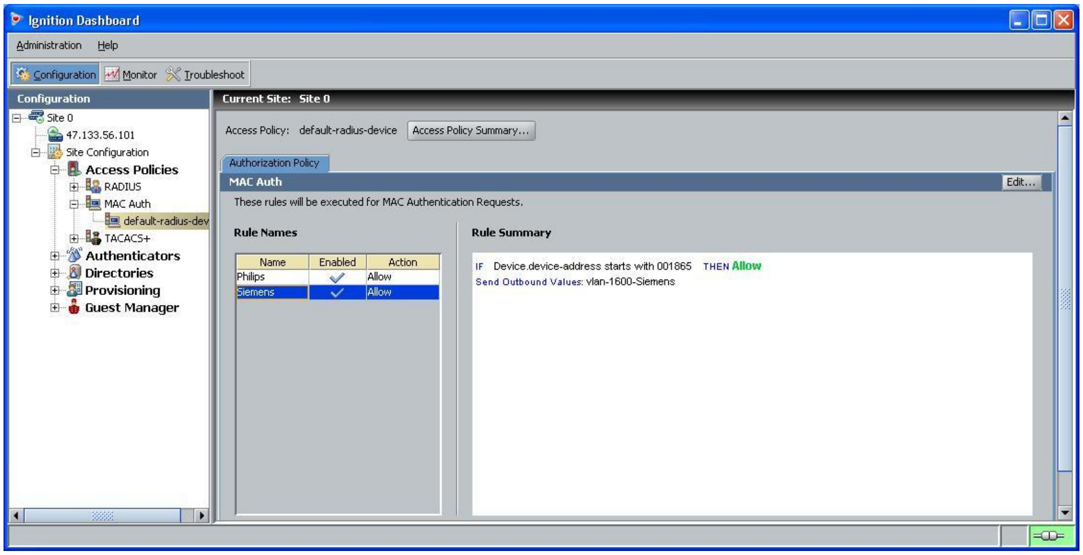
Provision With: vlan-1500-Philips, UROLphilips

All Outbound Values: Admin-Access, NAS-Prompt, Nortel-UROL-Policy-voice

Summary

IF Device.device-address starts with 00095c THEN Allow
Send Outbound Values: vlan-1500-Philips, UROLphilips

IDE Step 11 – Go to *Site Configuration -> Access Policies -> MAC Auth -> default-radius-device* and via the *Authorization Policy* tab, select *Siemens* and click on *Edit*



Current Site: Site 0

Access Policy: default-radius-device

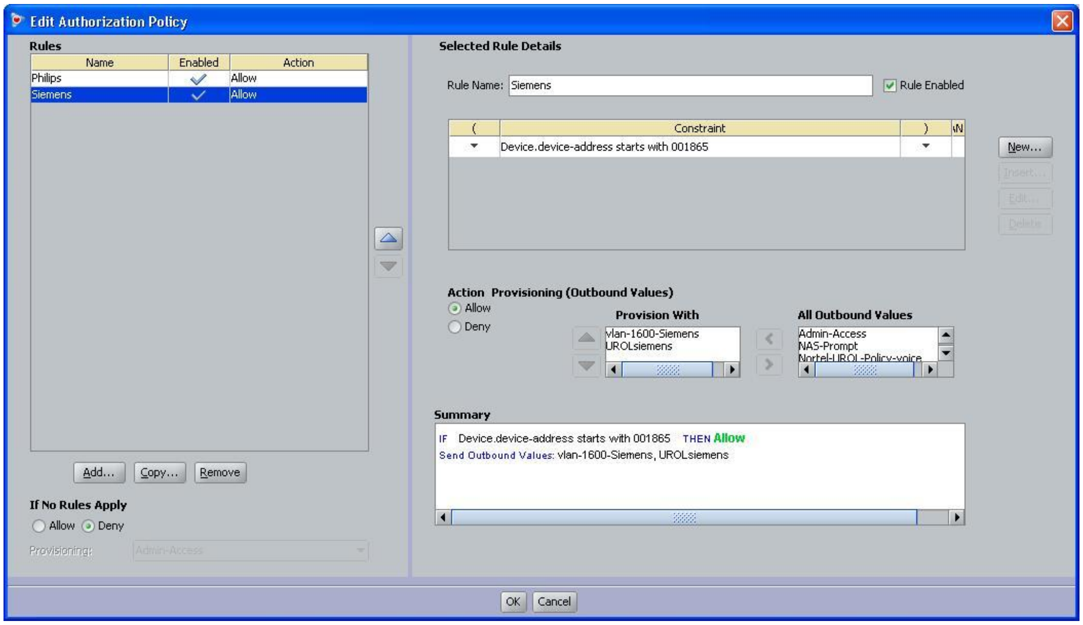
MAC Auth

These rules will be executed for MAC Authentication Requests.

Name	Enabled	Action
Philips	✓	Allow
Siemens	✓	Allow

IF Device.device-address starts with 001865 THEN Allow
Send Outbound Values: vlan-1600-Siemens

IDE Step 12 – Move the attribute we configured above named *UROLsiemens* from *All Outbound Value* box to the *Provision With* box and click *OK*.



Name	Enabled	Action
Philips	✓	Allow
Siemens	✓	Allow

If No Rules Apply
○ Allow ● Deny
Provisioning: Admin-Access

Rule Name: Siemens ☑ Rule Enabled

(	Constraint	)	AN
	Device.device-address starts with 001865		

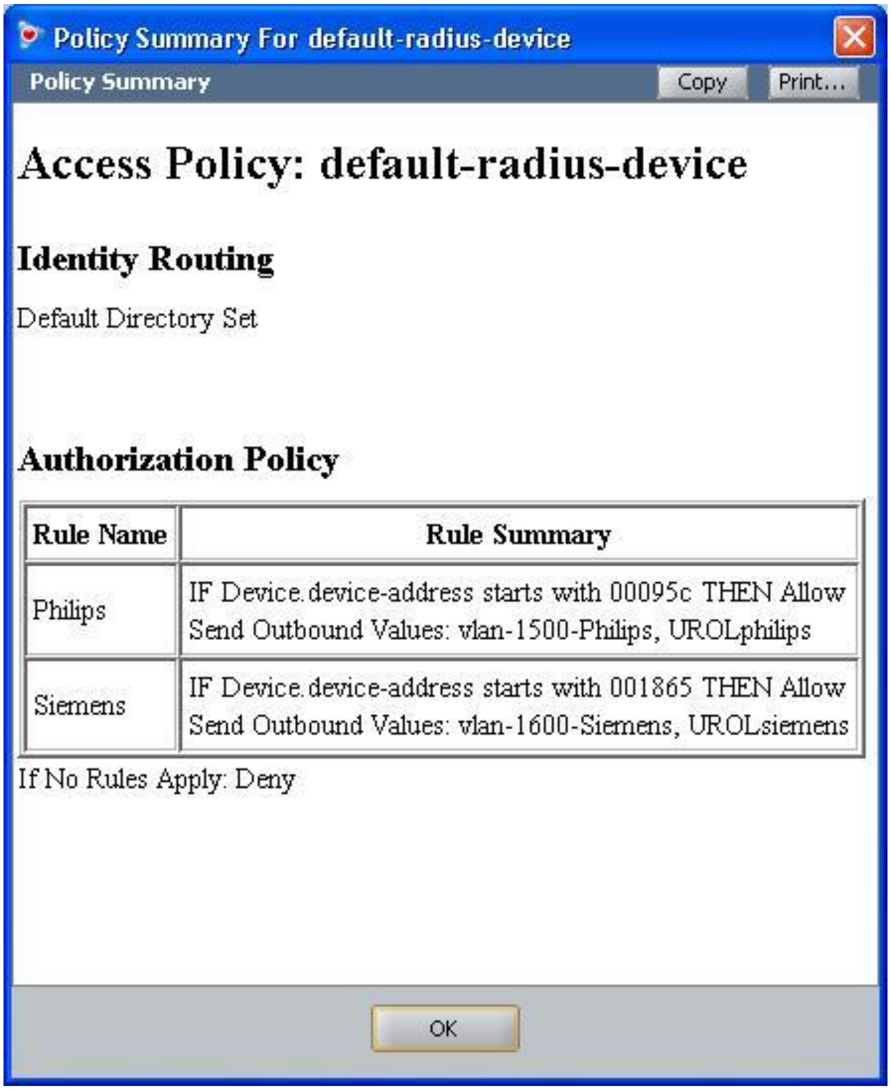
Action Provisioning (Outbound Values)
● Allow
○ Deny

Provision With:
vlan-1600-Siemens
UROLsiemens

All Outbound Values:
Admin-Access
NAS-Prompt
Nortel-UROL-Policy-voice

Summary
IF Device.device-address starts with 001865 THEN Allow
Send Outbound Values: vlan-1600-Siemens, UROLsiemens

IDE Step 13 – Once complete, we can go to *Site Configuration -> Access Policy -> MAC Auth -> default-radius-device* and clicking on *Access Policy Summary* to view the policy configuration which should look something like the following.



Access Policy: default-radius-device

Identity Routing

Default Directory Set

Authorization Policy

Rule Name	Rule Summary
Philips	IF Device.device-address starts with 00095c THEN Allow Send Outbound Values: vlan-1500-Philips, UROLphilips
Siemens	IF Device.device-address starts with 001865 THEN Allow Send Outbound Values: vlan-1600-Siemens, UROLsiemens

If No Rules Apply: Deny

1.4.7 Verify UBP configuration and operation via ERS5520-1

1.4.7.1 Verify EAP Policy

Step 1 – Assuming the IP Phone via port 3 has successfully authenticated via EAP, use the following command to view the UBP Policy:

```
5520-24T-1# show qos ubp classifier
```

Result:

```
       Id: 3
       Name: philips
       Block:
       Eval Order: 5
       Address Type: IPv4
       Destination Addr/Mask: Ignore
       Source Addr/Mask: Ignore
       DSCP: Ignore
       IPv4 Protocol / IPv6 Next Header: Ignore
       Destination L4 Port Min: Ignore
       Destination L4 Port Max: Ignore
       Source L4 Port Min: Ignore
       Source L4 Port Max: Ignore
       IPv6 Flow Id: Ignore
       IP Flags: Ignore
       TCP Control Flags: Ignore
       IPv4 Options: Ignore
       Destination MAC Addr: Ignore
       Destination MAC Mask: Ignore
       Source MAC Addr: Ignore
       Source MAC Mask: Ignore
       VLAN: Ignore
       VLAN Tag: Ignore
       EtherType: 0x0800
       802.1p Priority: All
       Packet Type: Ignore
       Inner VLAN: Ignore
       Action Drop: No
       Action Update DSCP: 0x1A
       Action Update 802.1p Priority: Ignore
       Action Set Drop Precedence: Low Drop
       Storage Type: NonVolatile

       Id: 4
       Name: siemens
       Block:
       Eval Order: 5
       Address Type: IPv4
       Destination Addr/Mask: Ignore
       Source Addr/Mask: Ignore
       DSCP: Ignore
       IPv4 Protocol / IPv6 Next Header: Ignore
       Destination L4 Port Min: Ignore
       Destination L4 Port Max: Ignore
       Source L4 Port Min: Ignore
```

```
        Source L4 Port Max: Ignore
        IPv6 Flow Id: Ignore
        IP Flags: Ignore
        TCP Control Flags: Ignore
        IPv4 Options: Ignore
        Destination MAC Addr: Ignore
        Destination MAC Mask: Ignore
        Source MAC Addr: Ignore
        Source MAC Mask: Ignore
        VLAN: Ignore
        VLAN Tag: Ignore
        EtherType: 0x0800
        802.1p Priority: All
        Packet Type: Ignore
        Inner VLAN: Ignore
        Action Drop: No
        Action Update DSCP: 0x10
        Action Update 802.1p Priority: Ignore
        Action Set Drop Precedence: Low Drop
        Storage Type: NonVolatile
```

On the ERS5520 verify the following information:

Option	Verify
Name:	Verify the policy name, should be ***philips*** and ***siemens*** for this example.
Eval Order:	Verify the port number is correct, should be ***5*** for this example.
Address Type:	Verify the Address Type is correct, should be ***IPv4*** for this example – default setting.
EtherType:	Verify the EtherType is correct, should be ***0x0800***.
Action Update DSCP:	Verify the DSCP value is correct, should be ***0x1A*** (decimal 26) for the Philips policy and ***0x10*** (decimal 16) for the Siemens policy.

1.4.7.2 Verify EAP Policy upon the NEAP client successfully authenticating

Step 1 – Assuming the IP Phone via port 3 has successfully authenticated via EAP, use the following command to view the UBP Policy:

```
5520-24T-1# show qos ubp interface
```

Result:

```
         Id  Unit Port Filter Set Name
       _____ ____ ____ _______________
       55001 1    14   siemens
       55004 1    19   philips
```

On the ERS5520 verify the following information:

Option	**Verify**
Port	Verify the port number is correct according the device authenticated
Filter Set Name	If the device has successfully authenticated, and if the RADIUS server has been configured correctly, the policy named ***philips*** or ***simens*** will be displayed.

1.4.7.3 Verify the Medical Device traffic via the ERS8600 core switches using IPFIX

IPFIX can be enabled on the core switches to view and monitor the traffic coming in from the edge ERS5520 switch. By using IPFIX, you can display various information such as source and destination IP addresses, source and destination UDP/TCP port numbers, source and destination MAC addresses, ingress and egress port numbers used on the ERS8600 switch, DSCP values, and TCP flags. By using this information, we can simply verify that the UBP policy is working on the ERS5520 switch by looking at the DSCP values. In addition, you can use IPFIX to look for more specific traffic pattern to further enhance the UBP policy.

Use the following commands to configure and view the traffic flow assuming the port used on the ERS8600 to connect to ERS5520-1 is port 3/29:

```
ERS8600-5:5# config ip ipfix state enable
ERS8600-5:5# config ip ipfix port 3/29 all-traffic enable
ERS8600-6:5# show ip ipfix flows 3

================================================================================
                                  IPFIX Flows
================================================================================
Slot Number : 3                             Total Number Of Flows : 2

Port/  SrcIP/DstIP     Src/   Protcol/  DSCP/    Egrss  Start/Last
Vlan   Addr            Dst    Obsv      TcpFlag  Port/  Time
                       Port   Point              Mgid
--------------------------------------------------------------------------------
3/29   192.168.20.30   63     udp       104      3/30   SEP 09 14:14:28
1500   192.168.20.40   63     Port      none            SEP 09 14:15:58

3/29   192.168.40.10   63     udp       64       3/30   SEP 09 14:14:28
1600   192.168.40.20   63     Port      none            SEP 09 14:15:58

Total number of Displayed Flows on Slot 3 : 2

--------------------------------------------------------------------------------
Port/  SrcMac/DstMac      Byte/Pkt
Vlan                      Count
--------------------------------------------------------------------------------
3/29   00:09:5c:00:02:03  41880241880

1500   00:09:5c:00:02:04   615885910

3/29   00:18:65:00:02:01  4280620468
1600   00:18:65:00:02:02    62950301

Total number of Displayed Flows on Slot 3 : 2
```

Please note the DSCP values shown are the full ToS values. To calculate the actual DSCP value, drop the two least significant binary bits. For this example, 104 in binary is “1101000” and 64 in binary is “1000000” where if you drop the two least significant bits become binary “11010” or decimal 26 and binary “10000” or decimal 16 respectively.

2. Software Baseline

Product	Minimum Software Level
Identity Engines	6.0.1
ERS2500	4.2
ERS4500	5.3
ERS5500	5.1
ERS5600	6.0

3. Reference Documentation

Document Title	Publication Number	Description
Identity Engines Ignition Server, Release 6.0 – Document Collection	NIEIS_6.0_Doc_Collection_20090706, Rev 02	Ignition Server Software Release 6.0
Avaya Ethernet Routing Switch 2500 Series Release 4.1 Document Collection	ERS2500_4.2_Doc_Collection_20090302	Ethernet Routing Switch 2500 Software Release 4.2
Avaya Ethernet Routing Switch 4500 Series Release 5.1 Document Collection	ERS4500_5.3_Doc_Collection_20090731	Ethernet Routing Switch 4500 Software Release 5.3
Avaya Ethernet Routing Switch 5500 Series Release 5.1 Document Collection	ERS5500_6.1_Doc_Collection_20090525	Ethernet Routing Switch 5000 Software Release 6.1