Ignition Server

Engineering

> Ignition Server Microsoft NAP with Active Directory Authentication Technical Configuration Guide

Avaya Data Solutions

Document Date: June 2011

Document Number: NN48500-625

Document Version: 1.1

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http:// www.avaya.com/support.

Abstract

This Technical Configuration Guide outlines the configuration steps required to authenticate computers and users via Microsoft Active Directory through an Identity Engines Ignition Server and determine network access based on the end-points compliance state. The main components include the Avaya Wireless LAN 8100 Controller and Access Points, Avaya Ethernet Routing Switches, Avaya Ignition Server and an Active Directory user store running on a Microsoft Windows Server 2003 server.

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	June 2011	1.0	KLM	Initial Draft
2	June 2011	1.1	KLM	Minor Corrections

Table of Contents

Figures 5

Tables........ 6

Conventions 7

1. Overview 8

 1.1 Network Access Protection 9

2. Configuration Example........ 11

 2.1 Components........ 11

 2.2 Hardware & Software 12

 2.3 Ignition Server 14

 2.4 Avaya Wireless LAN 8100 68

 2.5 Avaya Ethernet Routing Switch........ 76

 2.6 Microsoft Windows 7 81

3. Verification 94

 3.1 Avaya Ethernet Routing Switch........ 94

 3.2 Wireless LAN 8100 100

4. Troubleshooting 106

 4.1 Authentication........ 106

 4.2 CA Root Certificates........ 110

 4.3 Active Directory Cache........ 112

5. Reference Documentation 114

Figures

Figure 1.0 – Avaya Wireless Guest Management Solution 8
Figure 1.1 – Example Ignition Server Posture Profile 9
Figure 2.2 – Topology 12
Figure 2.3.2 – Active Directory 26
Figure 2.3.3.1 – Directory Sets 33
Figure 2.3.4.1 – Virtual Groups 36

Tables

Table 2.2 – Hardware and Software 13
Table 2.3.5.1 – Dynamic VLANs 40
Table 2.3.8.1 – Authorization Policies 52

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 Lucida Console font:

```
ERS5520-48T# show sys-info

Operation Mode:          Switch
MAC Address:             00-12-83-93-B0-00
PoE Module FW:           6370.4
Reset Count:             83
Last Reset Type:         Management Factory Reset
Power Status:            Primary Power
Autotopology:            Enabled
Pluggable Port 45:       None
Pluggable Port 46:       None
Pluggable Port 47:       None
Pluggable Port 48:       None
Base Unit Selection:     Non-base unit using rear-panel switch
sysDescr:                Ethernet Routing Switch 5520-48T-PWR
                         HW:02       FW:6.0.0.10  SW:v6.2.0.009
                         Mfg Date:12042004    HW Dev:H/W rev.02
```

1. Overview

Microsoft Network Access Protection (NAP) is a set of operating system components that provide a platform for protected access to private networks. The NAP platform provides a way of detecting the health state of a Windows device that is attempting to connect to a network and will restrict access until the defined policy requirements for connecting to the network have been met.

The Avaya Ignition Server release 7.0 introduces support for Microsoft NAP which allows customers to perform end-point inspection on Microsoft Windows XP, Windows Vista and Windows 7 workstations with or without a Windows Server 2008 Microsoft Network Policy server:

1) Allows customers with Windows Server 2003 deployments to deploy NAP by leveraging the Ignition Server as the Health Authority (HA).

2) Allows customers with Windows Server 2008 environments to deploy NAP by leveraging the Ignition Server or Network Policy Server (NPS) as the Health Authority (HA).

3) Allows customers with Windows Server 2003 or Windows Server 2008 environments to deploy NAP in addition to Avaya's Authenticated Network Architecture (ANA).

The solution outlined in this guide allows customers with Windows Server 2003 or Windows Server 2008 environments to deploy NAP on wired and wireless networks using the Ignition Server as the RADIUS server and Health Authority. The Ignition Server provides PEAP authentication for users against Active Directory and will assign compliant users to a Corporate VLAN based on Active Directory group membership and non-compliant users to a Remediated VLAN.

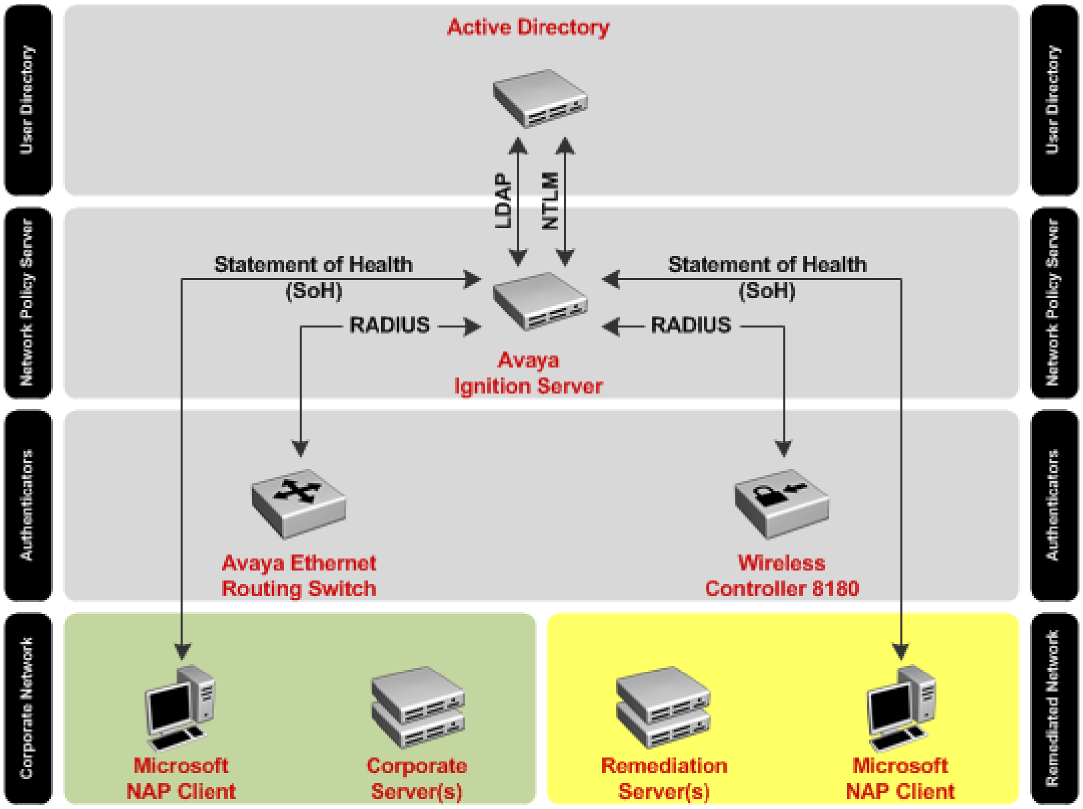
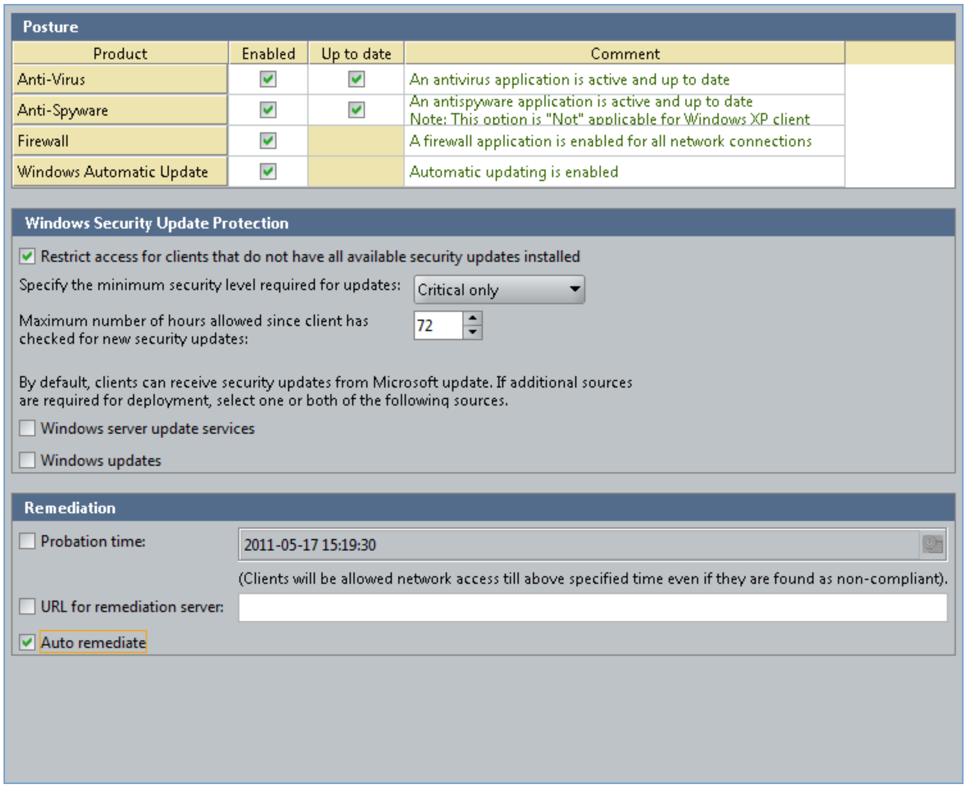


Figure 1.0 – Avaya Wireless Guest Management Solution

1.1 Network Access Protection

Network Access Protection (NAP) is a Microsoft technology for controlling network access for users based on the system health of a Windows workstation. With NAP system administrators define policies for system health requirements which the Windows host computers must comply before being permitted unrestricted access to the network. NAP policies can verify that security software such as Anti-Virus, Anti-Spyware and Firewall are operating and up to date and can also verify that the latest system updates are installed.

Tip – On the Avaya Ignition Server the Windows system components to validate are defined in a Posture Profiles while the actions to take are defined using Authorization Policies.



Posture

Product	Enabled	Up to date	Comment
Anti-Virus	☑	☑	An antivirus application is active and up to date
Anti-Spyware	☑	☑	An antispyware application is active and up to date Note: This option is "Not" applicable for Windows XP client
Firewall	☑		A firewall application is enabled for all network connections
Windows Automatic Update	☑		Automatic updating is enabled

Windows Security Update Protection

☑ Restrict access for clients that do not have all available security updates installed

Specify the minimum security level required for updates: Critical only

Maximum number of hours allowed since client has checked for new security updates: 72

By default, clients can receive security updates from Microsoft update. If additional sources are required for deployment, select one or both of the following sources.

□ Windows server update services

□ Windows updates

Remediation

□ Probation time: 2011-05-17 15:19:30

(Clients will be allowed network access till above specified time even if they are found as non-compliant).

□ URL for remediation server:

☑ Auto remediate

Figure 1.1 – Example Ignition Server Posture Profile

NAP allows network administrators to define levels of network access based on a client's identity, the Active Directory groups to which the client belongs, and the degree to which the client complies with corporate governance policy. Windows hosts that comply can be granted full un-restricted access to the network while hosts which fail compliance are provided with restricted network access with the necessary permissions required to become complaint. NAP also provides a mechanism for automatically bringing the client into compliance (a process known as remediation) and then dynamically increasing its level of network access.

The Avaya Ignition Server NAP solution consists of the following components:

- ***NAP Clients*** – Are Windows hosts that report system health to a NAP enforcement point. NAP clients are provided Windows 7, Windows Vista, Windows XP with Service Pack 3 (SP3), Windows Server 2008, and Windows Server 2008 R2. NAP clients currently support PEAP for authentication and system health reporting.
- ***NAP Enforcement Point*** – IEEE 802.1X capable devices such as an Avaya Ethernet Routing Switch or Avaya Wireless LAN 8180 controller.
- ***NAP Health Policy Server*** – An Avaya Ignition Server that stores health requirement policies and provides health evaluation for NAP clients. Health requirement policies are configured by the Ignition Server administrator and can include settings that require that NAP client computers have the latest antivirus definitions and security updates installed, a personal firewall enabled, and other settings.
- ***Authentication, Authorization and Accounting Server (AAA)*** – An Avaya Ignition Server that receives PEAP authentication requests from the NAP Enforcement Points and validates the users credentials and determines group membership against an Active Directory user directory.

A NAP deployment using an Avaya Ignition Server operates in a identical manner to a Microsoft Windows Server 2008 deployment with the exception that the Ignition Server is used as the AAA server and Health Policy Server:

1) When a NAP-capable client computer contacts a NAP enforcement point, it submits its current health state. The NAP enforcement point sends the NAP client's health state to the NAP health policy server on the Ignition Server for evaluation using the RADIUS protocol. The Ignition Server also provides PEAP authentication for the NAP client. Users can be authenticated locally or against an external directory such as Active Directory.

2) The Ignition Server evaluates the health state of the NAP client:

    a. If the NAP client is determined to be compliant, the Ignition Server forwards a RADIUS Access-Accept with the users assigned un-restricted VLAN.

    b. If the NAP client is determined to be non-compliant, the Ignition Server forwards a RADIUS Access-Accept with the users assigned restricted VLAN. A non-compliant NAP client on the restricted network may access remediation servers to install the necessary components and updates. After remediation is complete, the NAP client can perform a new health evaluation in conjunction with a new authentication request and be assigned to their un-restricted VLAN.

2. Configuration Example

2.1 Components

The Avaya Ignition Server Network Access Protection (NAP) solution outlined in this guide consists of the following software and hardware components:

1. Configuration and Management:
   - *Ignition Dashboard Application* – A Windows based application used to configure and manage the Ignition Server that provides authentication, authorization and accounting as well as an interface into Active Directory.
2. Access Control:
   - *Ignition Server* – Authenticates and authorizes NAP users who wish to connect to the network, captures accounting information and evaluates the health of the devices.
   - *Active Directory User Directory* – The centralized user directory which is queried by the Ignition Server to authenticate and authorize end-users who wish to gain access to the wireless network.
3. Authenticators:
   - *Avaya Ethernet Routing Switch 4500* – Provides wired connectivity to corporate users which are authenticated using RADIUS against the Ignition Server.
   - *Avaya Wireless LAN 8100* – Provides wireless connectivity and mobility to corporate users which are authenticated using RADIUS against the Ignition Server.
4. Client:
   - *Apple MacBook Pro (Bootcamp with Windows 7 Enterprise)* – End user device that connects and authenticates to the Avaya Ethernet Routing Switch 4500 or Wireless LAN.

2.2 Hardware & Software

The following diagram depicts the hardware and software components and the topology used to create this guide:

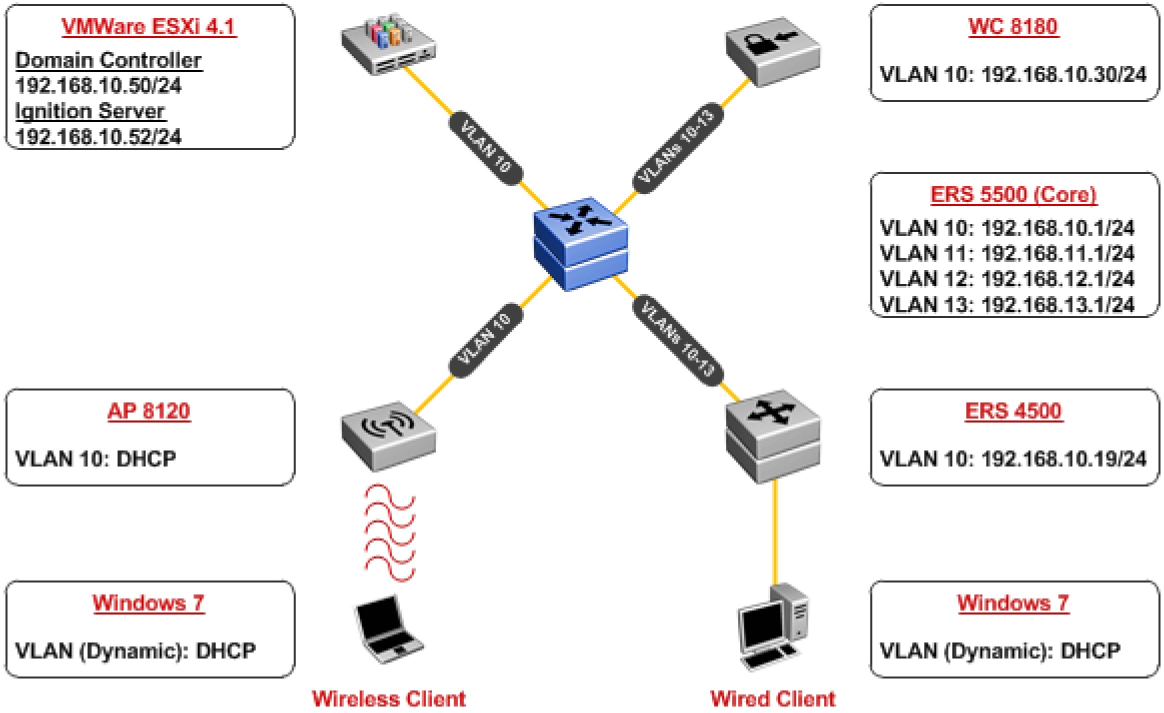


Figure 2.2 – Topology

The following table highlights the hardware and software outlined above used to create this guide:

Hardware and Software Components
Dell PowerEdge D610 Server – VMWare ESXi Version 4.1.0: 1. Avaya Ignition Server – Version 07.00.00.020468 2. Microsoft Windows Server 2003 Enterprise Edition with Service Pack 2: ○ Active Directory Services ○ Certificate Services ○ DNS Services
Avaya Ethernet Routing Switch 5520-48T-PWR – Version 6.2.0.009
Avaya Ethernet Routing Switch 4550T – Version 5.4.1 Avaya Ethernet Routing Switch 4524GT – Version 5.4.1
Avaya WLAN 8100 Series – Version 1.0.1.007 • 1 x WLAN Controller 8180 • 3 x WLAN Access Point 8120
IBM Thinkpad T500 – Windows 7 Enterprise: • Intel® WiFi Link 5100 AGN 802.11a/b/g PCI Express Wireless Adaptor • Microsoft Windows Client with Intel Extensions

Table 2.2 – Hardware and Software

2.3 Ignition Server

The following section outlines the configuration steps required to configure the Avaya Ignition Server to authenticate NAP users against Active Directory then assign a VLAN based on compliance state and Active Directory group membership:

Note – This guide assumes all certificates are issued from a common public or Enterprise certification authority. For this guide Microsoft Certificate Services configured as an Enterprise Root CA will be utilized.

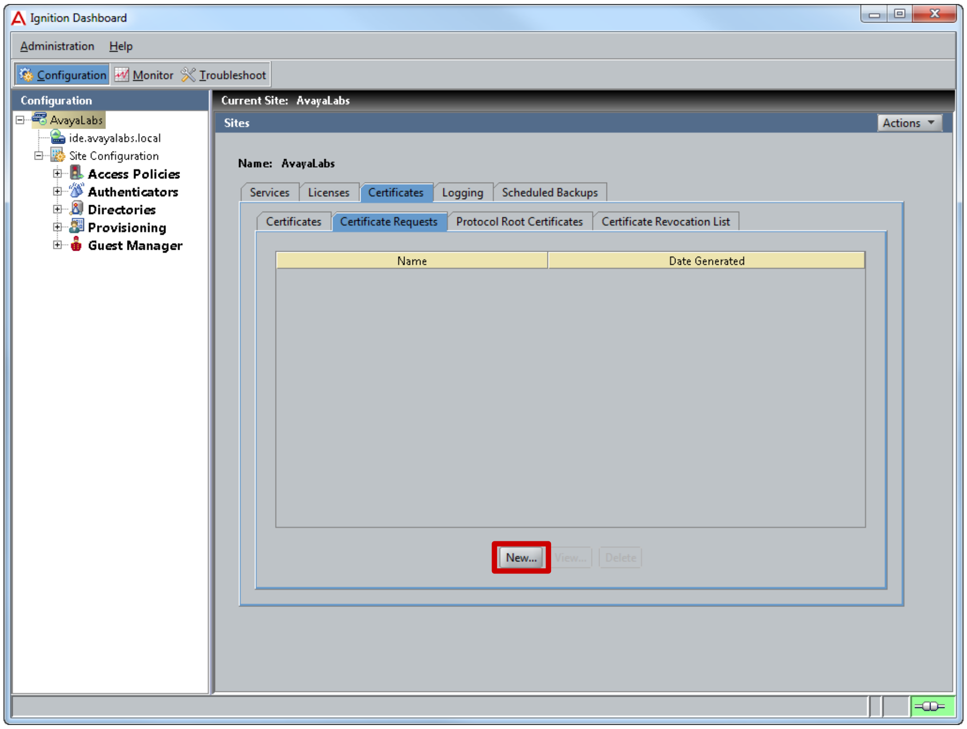
2.3.1 Digital Certificates

As PEAP authentication is used by the NAP clients for authentication, a signed server certificate must be installed on the Ignition Server. The following section highlights the necessary steps required to request a certificate, sign the certificate then install the signed certificate on the Ignition Server.

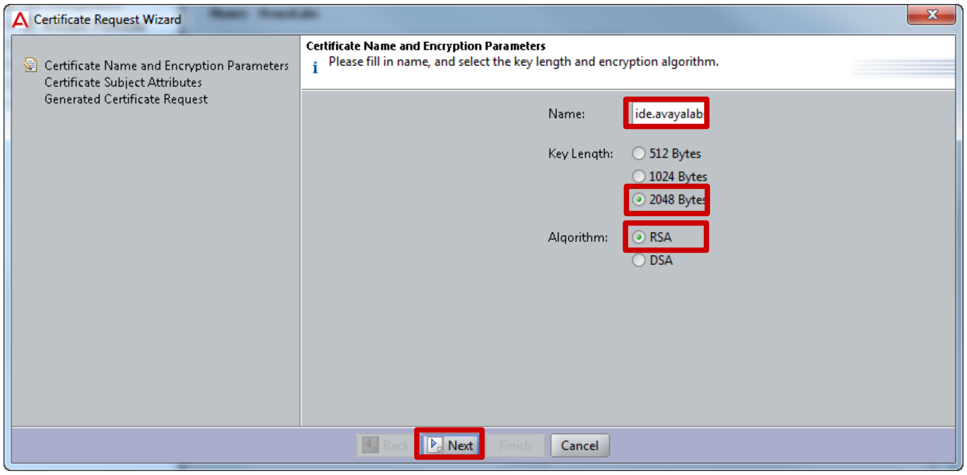
2.3.1.1 Certificate Signing Request (CSR)

Before a signed certificate can be issued and installed on the Ignition Server a public key and certificate signing request (CSR) must be generated. The CSR provides the certificate authority with the necessary information required to generate a signed certificate which will downloaded and installed on the Ignition Server. The signed certificate will be used for PEAP authentication but may also be used for Ignition Server Administration:

1 Within *Ignition Dashboard* select *Site-Name* > *Certificates* > *Certificate Requests*. Click *New*:



2 In the *Name* field enter the hostname and domain name of the Ignition Server. Select the *Key Length* value *2048* then set the *Algorithm* to *RSA*. Click *Next*:



Certificate Request Wizard

- Certificate Name and Encryption Parameters
- Certificate Subject Attributes
- Generated Certificate Request

Certificate Name and Encryption Parameters

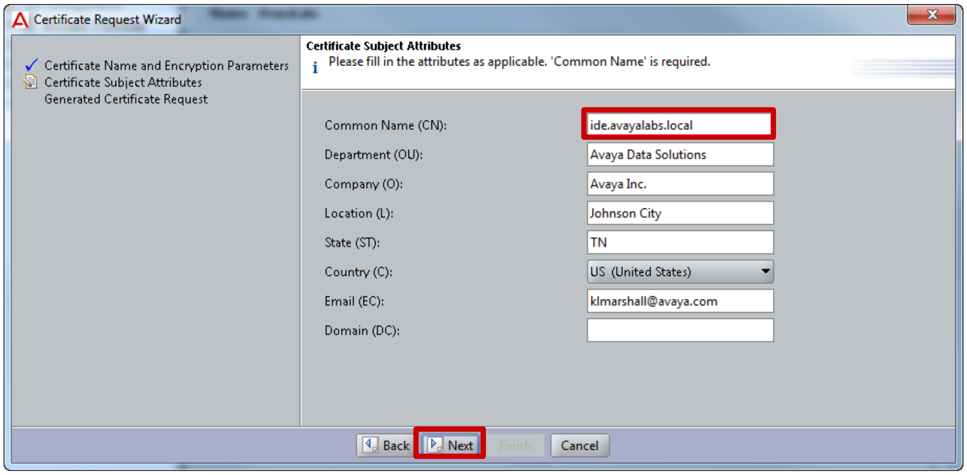
Please fill in name, and select the key length and encryption algorithm.

Name: ide.avayalab

Key Length: ○ 512 Bytes ○ 1024 Bytes ● 2048 Bytes

Algorithm: ● RSA ○ DSA

3 In the *Common Name (CN)* field enter the *hostname* and *domain name* of the Ignition Server. Enter appropriate *Company*, *Regional* and *Contact* information then select *Next*:



Certificate Request Wizard

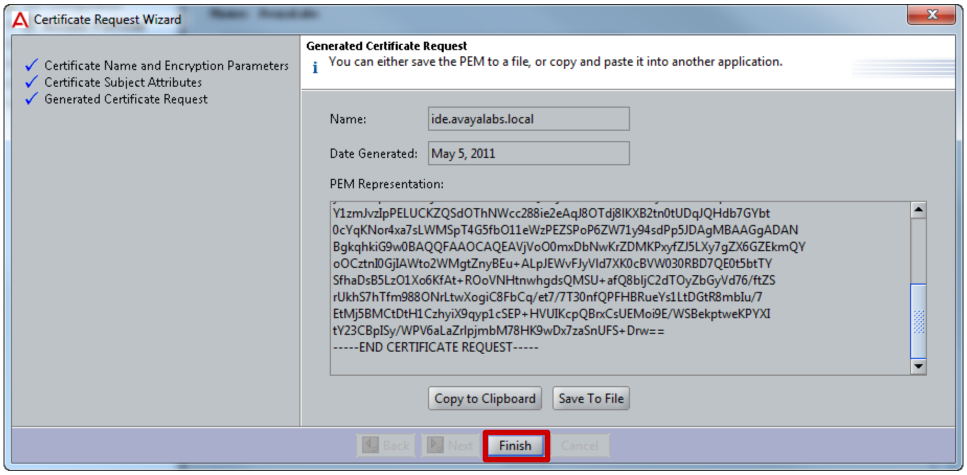
- ✓ Certificate Name and Encryption Parameters
- Certificate Subject Attributes
- Generated Certificate Request

Certificate Subject Attributes

Please fill in the attributes as applicable. 'Common Name' is required.

Common Name (CN):	ide.avayalabs.local
Department (OU):	Avaya Data Solutions
Company (O):	Avaya Inc.
Location (L):	Johnson City
State (ST):	TN
Country (C):	US (United States)
Email (EC):	klmarshall@avaya.com
Domain (DC):	

4 A certificate signing request will be generated. Click *Save To File* (recommended) or *Copy to Clipboard* then click *Finish*:



Certificate Request Wizard
✓ Certificate Name and Encryption Parameters
✓ Certificate Subject Attributes
✓ Generated Certificate Request

Generated Certificate Request

You can either save the PEM to a file, or copy and paste it into another application.

Name: ide.avayalabs.local

Date Generated: May 5, 2011

PEM Representation:

```
Y1zmJvzIpPELUCKZQSdOThNWcc288ie2eAqJ8OTdj8IKXB2tn0tUDqJQHdb7GYbt
0cYqKNor4xa7sLWMSpT4G5fbO11eWzPEZSPoP6ZW71y94sdPp5JDAgMBAAGgADAN
BgkqhkiG9w0BAQQFAAOCAQEAVjVoO0mxDbNwKrZDMKPxyfZJ5LXy7gZX6GZEkmQY
oOCztnI0GjIAWto2WMgtZnyBEu+ALpJEWvFJyVId7XK0cBVW030RBD7QE0t5btTY
SfhaDsB5LzO1Xo6KfAt+ROoVNHtnwhgdsQMSU+afQ8bljC2dTOyZbGyVd76/ftZS
rUkhS7hTfm988ONrLtwXogiC8FbCq/et7/7T30nfQPFHBRueYs1LtDGtR8mbIu/7
EtMj5BMCtDtH1CzhyiX9qyp1cSEP+HVUIKcpQBrxCsUEMoi9E/WSBekptweKPYXI
tY23CBpISy/WPV6aLaZrIpjmbM78HK9wDx7zaSnUFS+Drw==
-----END CERTIFICATE REQUEST-----
```

Note – Check with you network administrator to determine the appropriate key length before generating the CSR. Most CAs require a 2048 bit key.

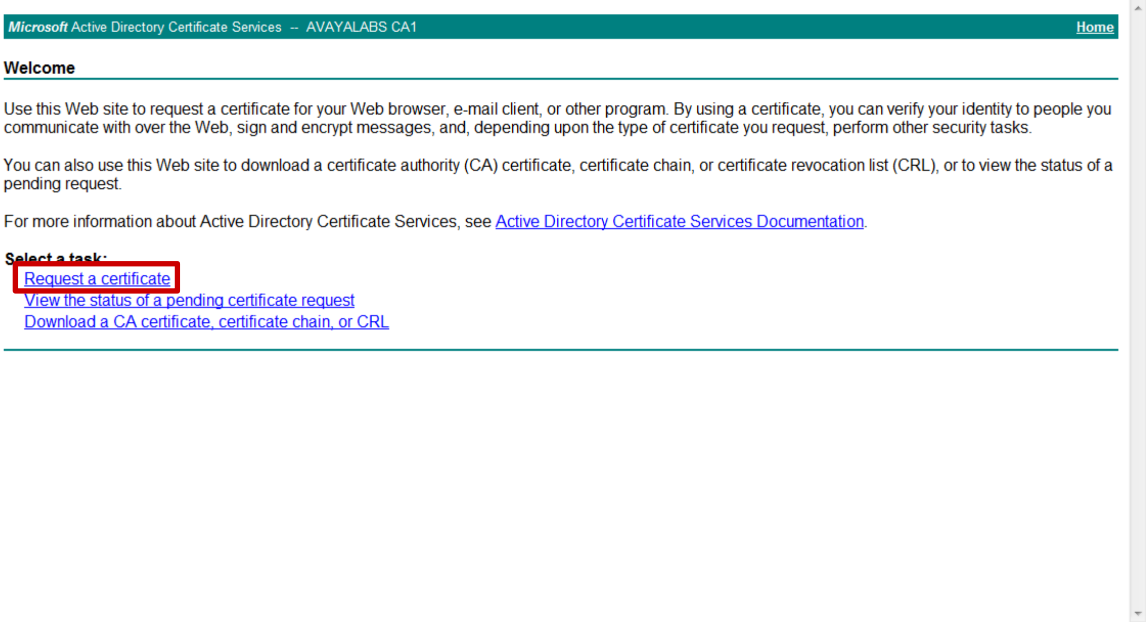
Note – The value provided in the CN field will be presented to the 802.1X client during authentication and may be used by the 802.1X client to validate the identity of the RADIUS authentication server.

2.3.1.2 Certificate Signing

A certificate signing request (CSR) can be signed by a private certificate authority (CA) that is operated and maintained by the enterprise organization or an external public CA which charges a fee for each server certificate issued. In most enterprise organizations a private CA will be deployed which allows certificates to be generated and maintained for internal devices and users. Examples of private CAs include Microsoft Certificate Services, Novell Certificate Authority and OpenSSL

The following provides an example of how to sign a CSR using Microsoft Certificate Services deployed as an Enterprise Root CA using Web Enrollment:

1 Using a web browser connect to Windows Server Web Enrollment web site, enter your credentials then select the task *Request a Certificate*:



Microsoft Active Directory Certificate Services -- AVAYALABS CA1 Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

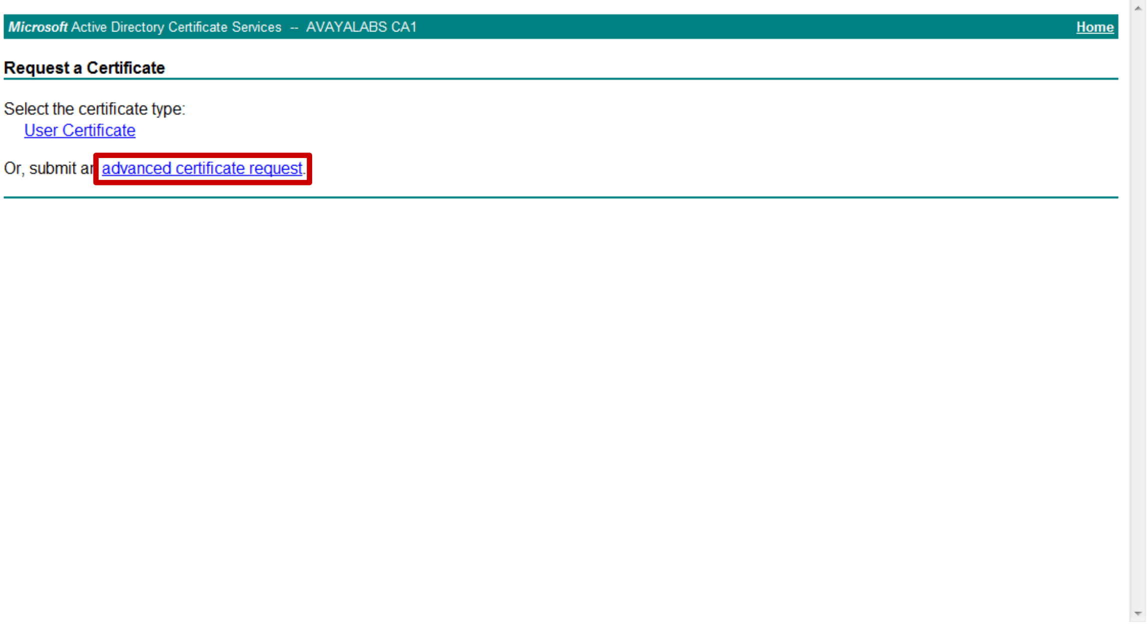
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

2 Select the option *advanced certificate request*:



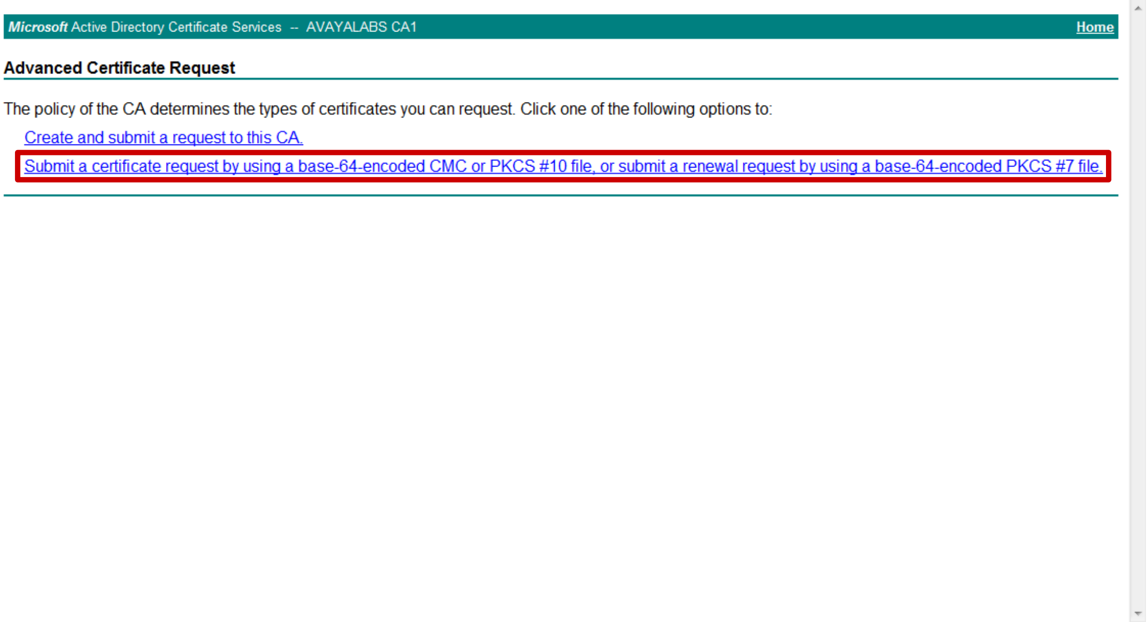
Microsoft Active Directory Certificate Services -- AVAYALABS CA1 Home

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

3 Select the option ***Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file, or submit a renewal request by using a base-64-encoded PKCS#7 file***:



Microsoft Active Directory Certificate Services -- AVAYALABS CA1

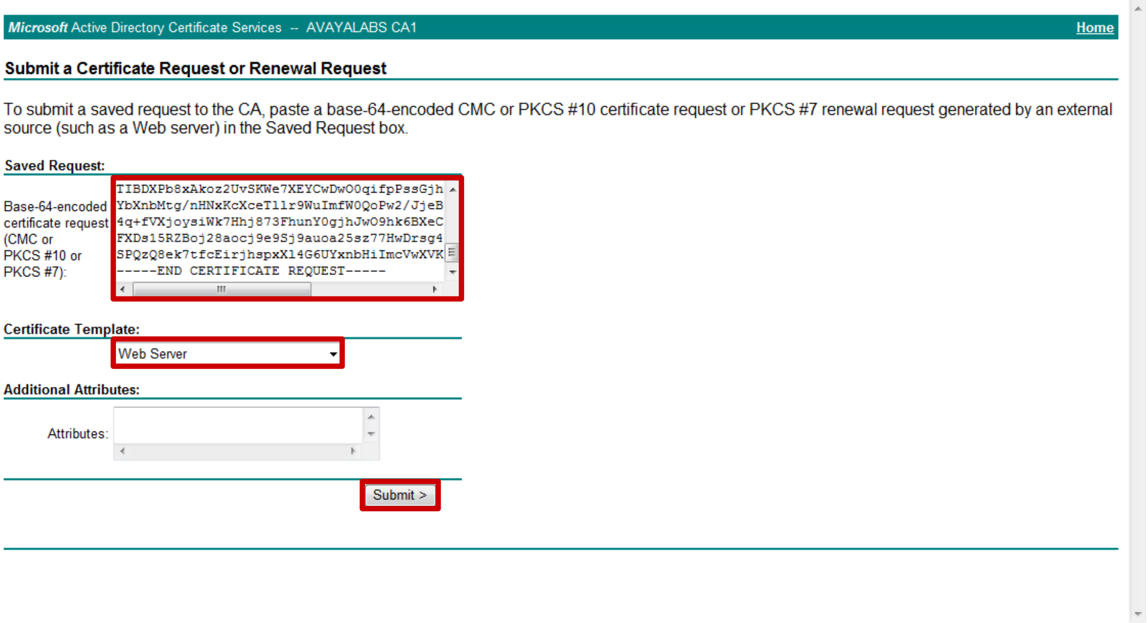
Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

4 In the ***Saved Request*** form field, paste the base-64 encoded text generated by the certificate signing request (CSR) on the Ignition Server. In the ***Certificate Template*** field select the Web Server template (or an alternative pre-defined user defined template) then click ***Submit***:



Microsoft Active Directory Certificate Services -- AVAYALABS CA1

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
TIBDXPb8xAkoz2UvSKWe7XEYCwDwO0qifpPssGjh
YbXnbMtg/nHNxKcXceTllr9WuImfW0QoPw2/JjeB
4q+fVXjoysiWk7Hhj873FhunY0gjhJwO9hk6BXeC
FXDs15RZBoj28aocj9e9Sj9auoa25sz77HwDrsg4
SPQzQ8ek7tfcEirjhspxXl4G6UYxnbHiImcVwXVK
-----END CERTIFICATE REQUEST-----
```

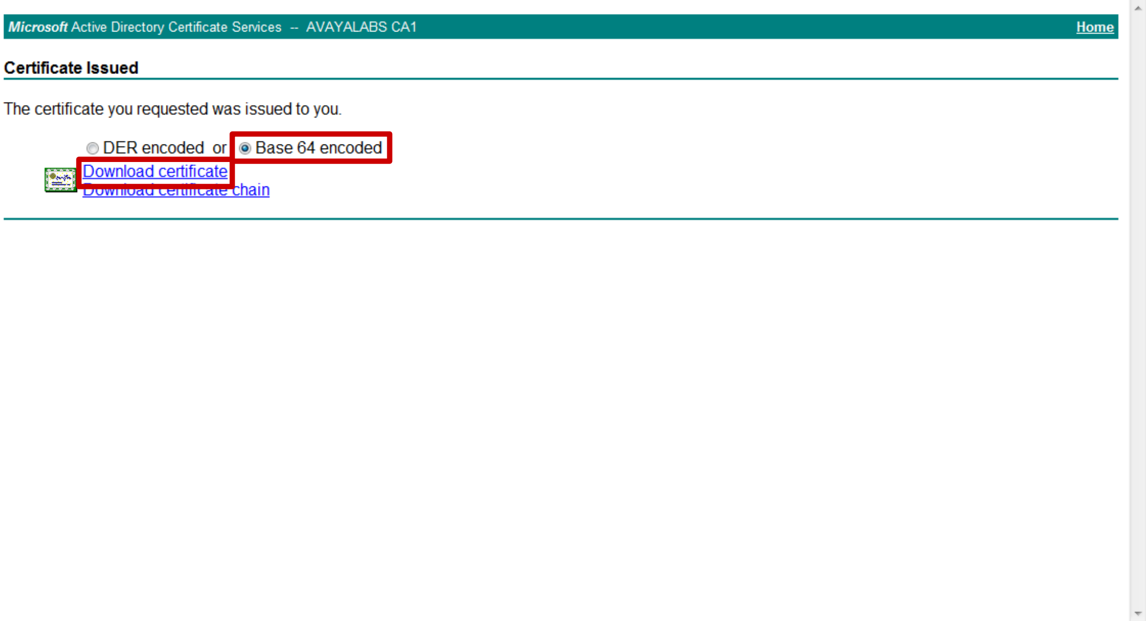
Certificate Template:

Web Server

Additional Attributes:

Attributes:

5 Select the encoding option *Base 64 encoded* then click *Download certificate*. Click *Save* then specify a filename and path for the certificate followed by a second *Save*:



Microsoft Active Directory Certificate Services -- AVAYALABS CA1 Home

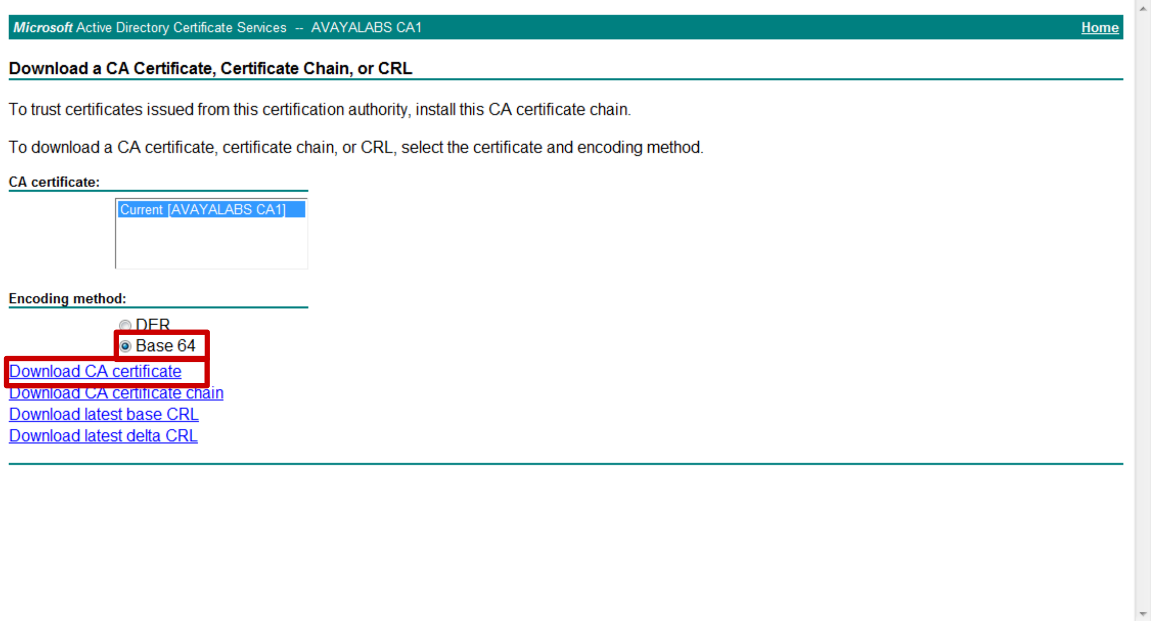
Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

6 In the top right of the window select *Home* to take you to the main page. Select the encoding option *Base 64 encoded* then click *Download CA certificate*. Click *Save* then specify a filename and path for the certificate followed by a second *Save*:



Microsoft Active Directory Certificate Services -- AVAYALABS CA1 Home

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [AVAYALABS CA1]

Encoding method:

○ DER
● Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

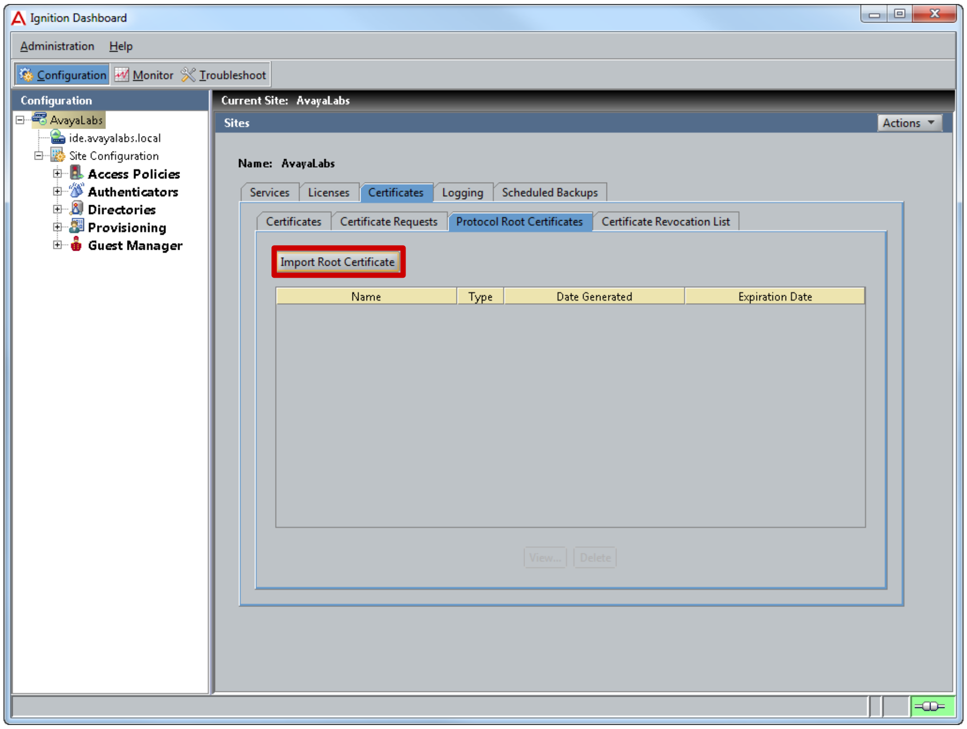
Note – To be installed on the Ignition Server, the signed certificate and corresponding CA root certificate must be issued in a base-64 encoded format.

2.3.1.3 Install CA Root Certificate

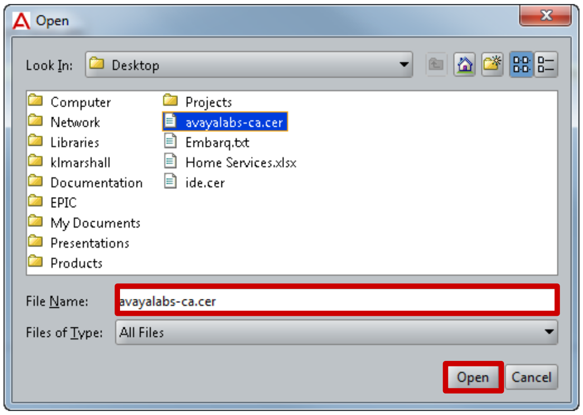
A CA root certificate allows a device to validate certificates issued from the certificate authority. While a CA certificate is not required on the Ignition Server to support PEAP, it is required if you plan on deploying EAP-TLS which uses certificates issued to computers and users. As a best practice it is recommended to install the CA certificate on a device when the server certificate is installed.

To install a CA root certificate on the Ignition Server:

1 Within *Ignition Dashboard* select *Site-Name* > *Certificates* > *Protocol Root Certificates*. Click *Import Root Certificate*:



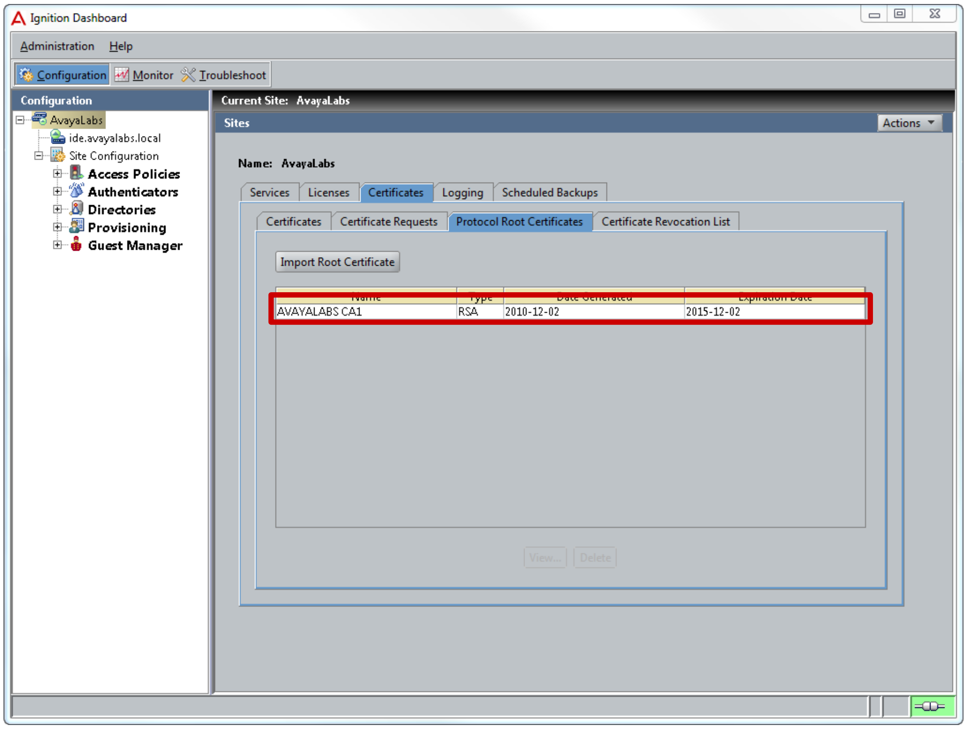
2 Select the *path* and *filename* for the base-64 encoded CA root certificate issued by your certificate authority then click *Open*:



File Name: avayalabs-ca.cer

Files of Type: All Files

3 The *CA root certificate* for the CA that issued the server certificate will now be installed:



Name: AvayaLabs

Name	Type	Date Generated	Expiration Date
AVAYALABS CA1	RSA	2010-12-02	2015-12-02

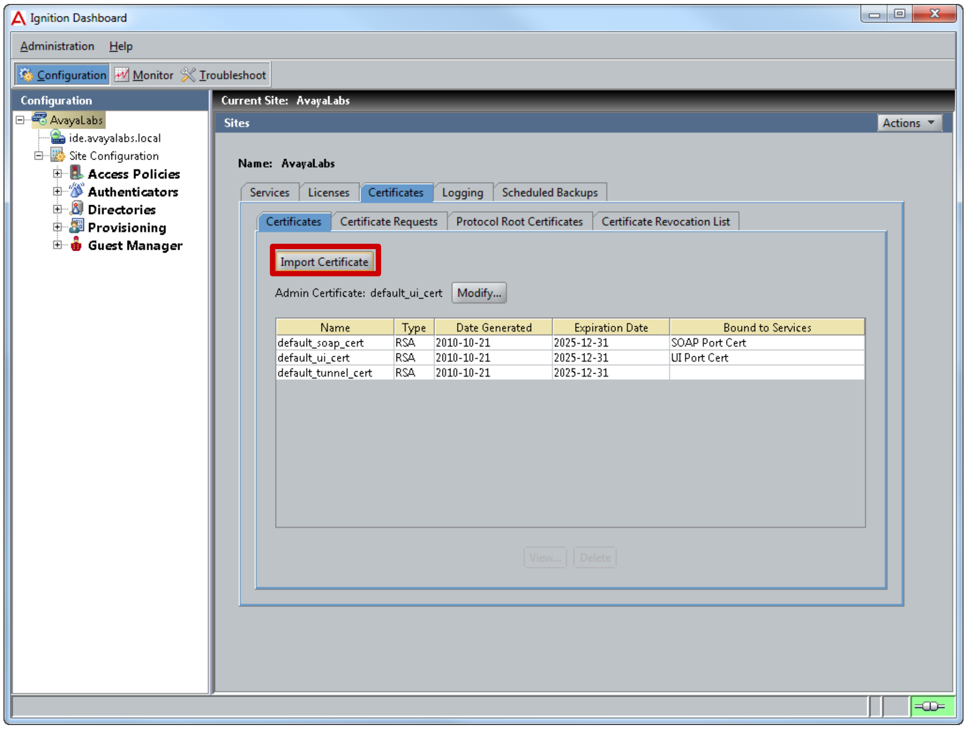
Note – To be installed on the Ignition Server, the CA root certificate must be issued in a base-64 encoded format.

2.3.1.4 Install Signed Server Certificate

Once the server certificate has been signed by the certificate authority (CA), it can be installed on the Ignition Server and used for PEAP authentication and Administration.

To install a signed certificate on the Ignition Server issued from a private or public CA:

1 Within *Ignition Dashboard* select *Site-Name > Certificates > Certificates*. Click *Import Certificate*:

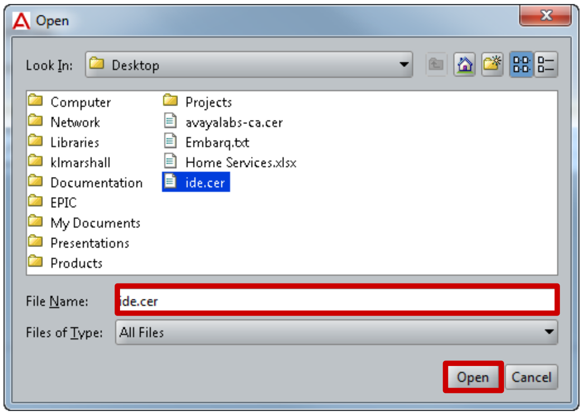


Name: AvayaLabs

Admin Certificate: default_ui_cert

Name	Type	Date Generated	Expiration Date	Bound to Services
default_soap_cert	RSA	2010-10-21	2025-12-31	SOAP Port Cert
default_ui_cert	RSA	2010-10-21	2025-12-31	UI Port Cert
default_tunnel_cert	RSA	2010-10-21	2025-12-31	

2 Select the *path* and *filename* for the base-64 encoded signed server certificate issued by your certificate authority then click *Open*:

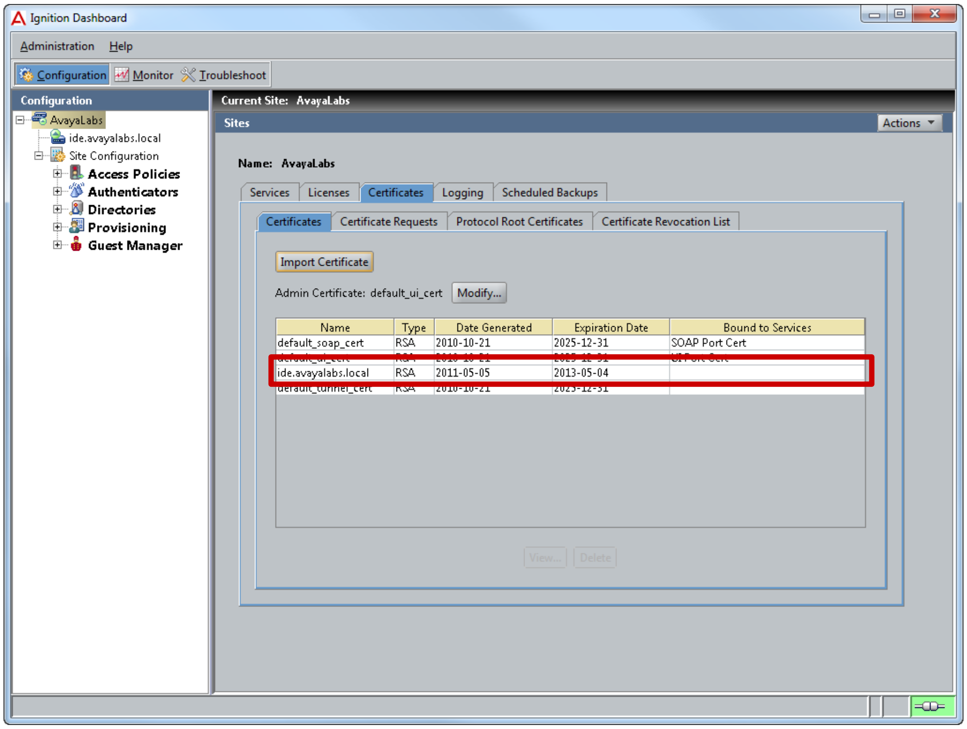


Look In: Desktop

File Name: ide.cer

Files of Type: All Files

3 Your signed server certificate will now be installed:



Name: AvayaLabs

Admin Certificate: default_ui_cert

Name	Type	Date Generated	Expiration Date	Bound to Services
default_soap_cert	RSA	2010-10-21	2025-12-31	SOAP Port Cert
default_ui_cert	RSA	2010-10-21	2025-12-31	UI Port Cert
ide.avayalabs.local	RSA	2011-05-05	2013-05-04	
default_tunnel_cert	RSA	2010-10-21	2025-12-31	

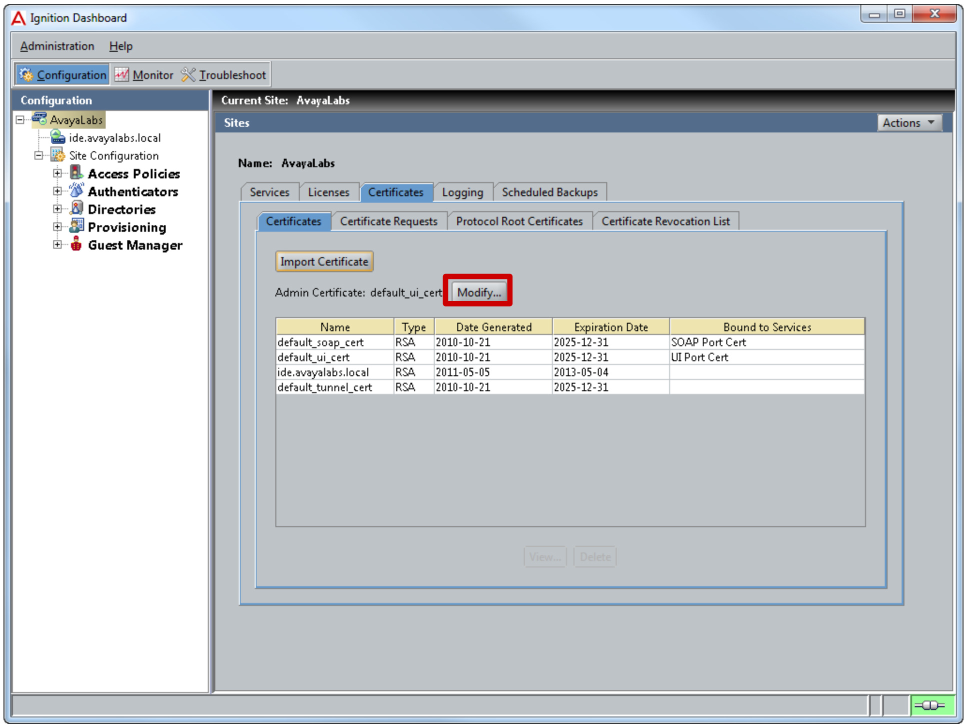
Note – To be installed on the Ignition Server, the signed server certificate must be issued in a base-64 encoded format.

2.3.1.5 Set Admin Certificate (Optional)

The Ignition Dashboard application uses TLS to provide a secure channel between the Ignition Server and Ignition Dashboard application. By default the Ignition Server uses a self-signed certificate which cannot be validated by the Ignition Dashboard application. In addition to being used for PEAP authentication, the signed server certificate can also be used for Ignition Server administration.

To configure the Ignition Server to use the signed certificate for the Admin Certificate:

1 Within *Ignition Dashboard* select *Site-Name* > *Certificates* > *Certificates*. Click *Modify*:



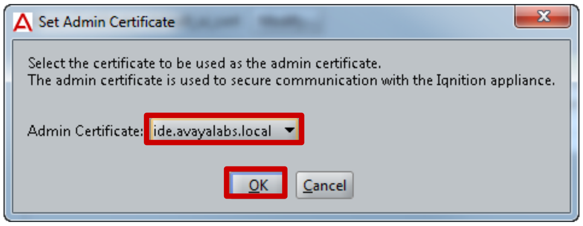
Current Site: AvayaLabs

Name: AvayaLabs

Admin Certificate: default_ui_cert

Name	Type	Date Generated	Expiration Date	Bound to Services
default_soap_cert	RSA	2010-10-21	2025-12-31	SOAP Port Cert
default_ui_cert	RSA	2010-10-21	2025-12-31	UI Port Cert
ide.avayalabs.local	RSA	2011-05-05	2013-05-04	
default_tunnel_cert	RSA	2010-10-21	2025-12-31	

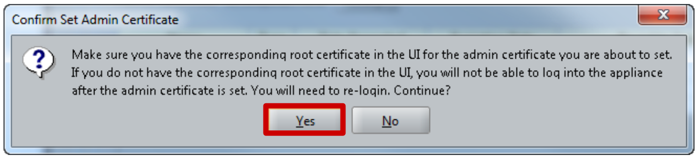
2 Using the *Admin Certificate* pull-down menu select the signed certificate installed in the previous step then click *OK*:



Select the certificate to be used as the admin certificate.
The admin certificate is used to secure communication with the Iqnition appliance.

Admin Certificate: ide.avayalabs.local

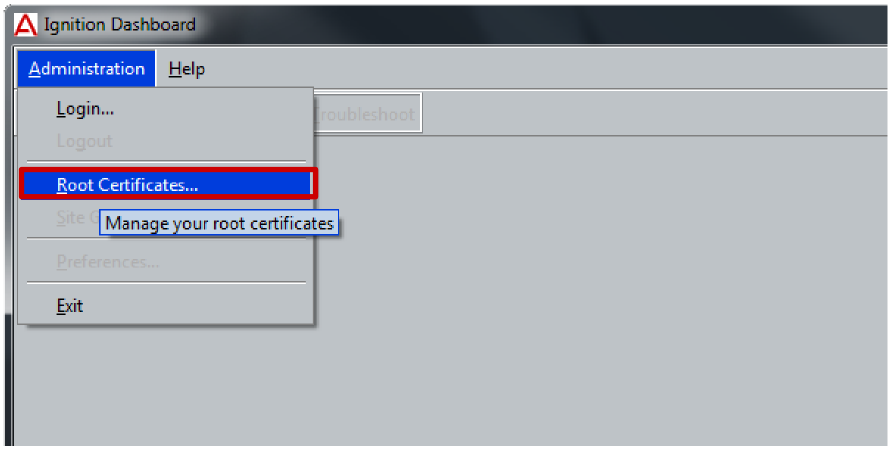
3 Click *Yes* to confirm:



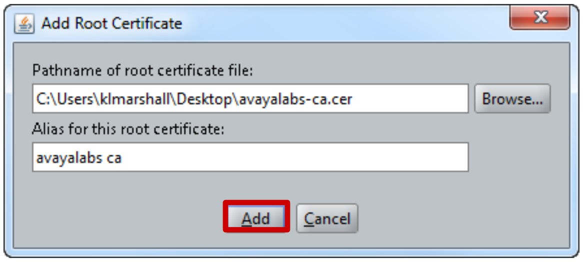
Confirm Set Admin Certificate

Make sure you have the corresponding root certificate in the UI for the admin certificate you are about to set. If you do not have the corresponding root certificate in the UI, you will not be able to log into the appliance after the admin certificate is set. You will need to re-login. Continue?

4 Within Ignition Dashboard select *Administration* > *Root Certificates*:



5 Select the *path* and *filename* for the base-64 encoded CA root certificate issued by your certificate authority and enter an Alias name. Click *Add*:

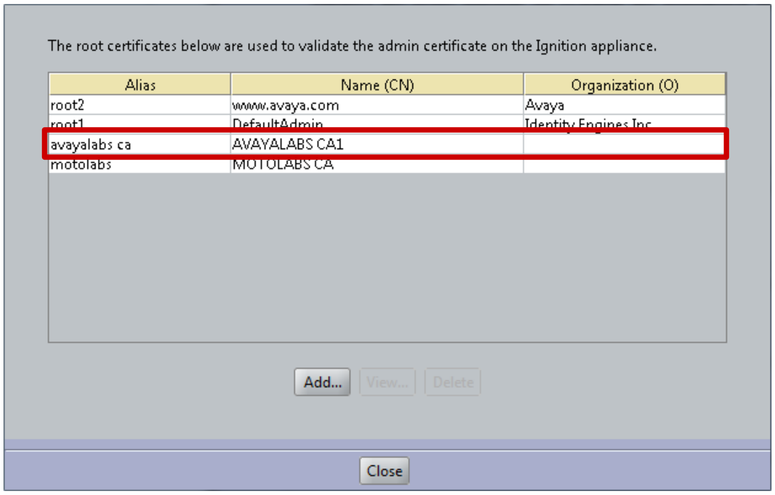


Add Root Certificate

Pathname of root certificate file: C:\Users\klmarshall\Desktop\avayalabs-ca.cer

Alias for this root certificate: avayalabs ca

6 The *CA root certificate* for the CA that issued the server certificate will now be installed:



The root certificates below are used to validate the admin certificate on the Ignition appliance.

Alias	Name (CN)	Organization (O)
root2	www.avaya.com	Avaya
root1	DefaultAdmin	Identity Engines Inc
avayalabs ca	AVAYALABS CA1	
motolabs	MOTOLABS CA	

Note – Once you change the Admin Certificate, you must install the corresponding CA root certificate in the Ignition Dashboard application. Failure to install the correct CA root certificate will result in a connection failure.

2.3.2 Directory Services

Rather than maintain a separate user database on the Ignition Server for each PEAP user, the Ignition Server can query an existing external user directory such as Active Directory. Directory Services defines the necessary configuration parameters that allow the Ignition Server to communicate with an external user directory store such as the Active Directory Server IP address, directory path information and bind parameters.

The Ignition Server can communicate with Active Directory using Lightweight Directory Access Protocol (LDAP) as well as the NT LAN Manager (NTLM) protocol. LDAP is used to validate user's credentials using PAP and CHAP authentication protocols while NTLM is used to validate user's credentials using MSCHAPv2:

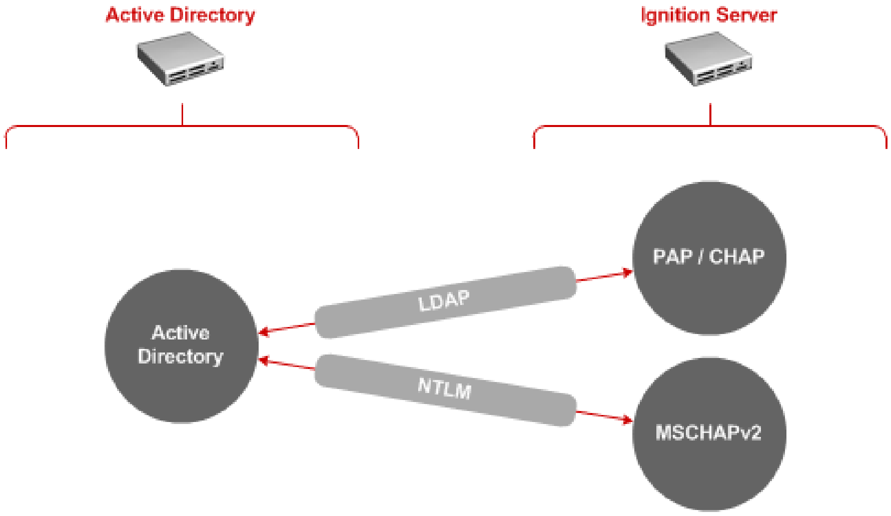


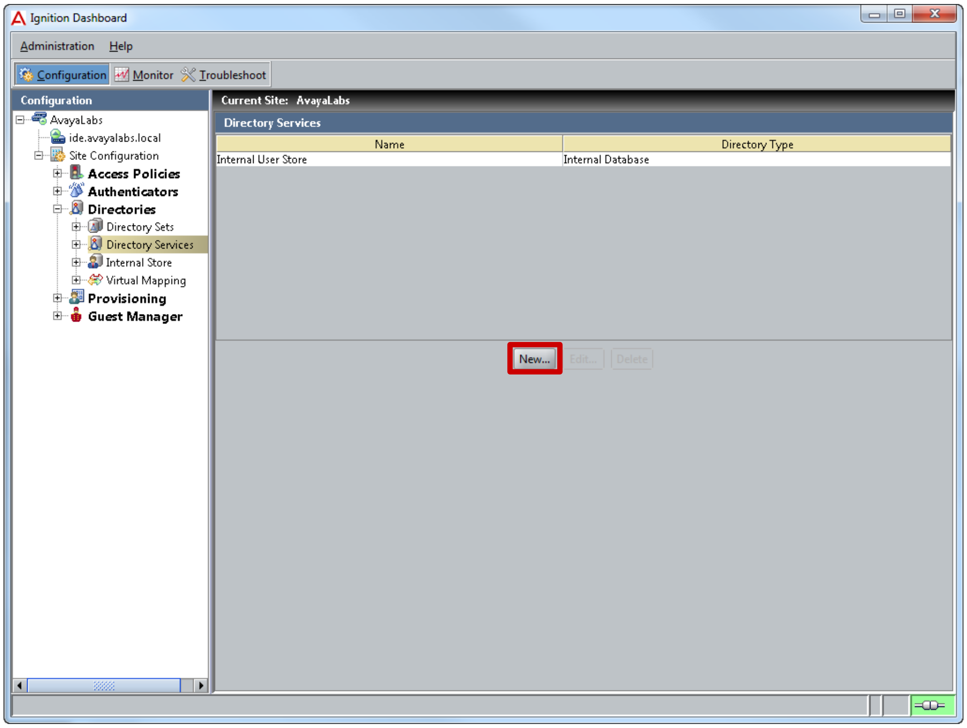
Figure 2.3.2 – Active Directory

2.3.2.1 Configuration Step

For this configuration step a Microsoft Windows Server 2003 Domain Controller will be added to the Directory Services on the Ignition Server with the following parameters defined:

1) The ***Name*** will be set to ***Active Directory*** to match the directory type.
2) The ***Service Account Name*** will be set to ***ide*** which is a bind user account for the Ignition Server created in Active Directory.
3) The ***Service Account Password*** will be set to ***avayalabs*** that matches password defined for the ***ide*** user account predefined in Active Directory.
4) The ***NetBIOS Domain*** will be set to ***AVAYALABS*** which matches the NetBIOS domain name for the Active Directory Domain.
5) The ***AD Domain Name*** will be set to ***avayalabs.local*** which matches the Active Directory Domain name.
6) The ***Directory Root DN*** will be set to the default value ***DC=avayalabs,DC=local***.
7) The ***User Root DN*** will be set to the default value ***DC=avayalabs,DC=local***.
8) The ***Primary Server IP Address*** will be set to ***192.168.10.50*** which is the host IP address assigned to Microsoft Windows Server 2003 Domain Controller.
9) The ***Port*** will be set to the default value ***389***.
10) The ***NETBIOS Server Name*** will be set to ***W3KSERVER-DC1*** which matches the NetBIOS name assigned to the Microsoft Windows Server 2003 Domain Controller.

1 Within *Ignition Dashboard* select *Configuration > Directories > Directory Services*. Click *New*:

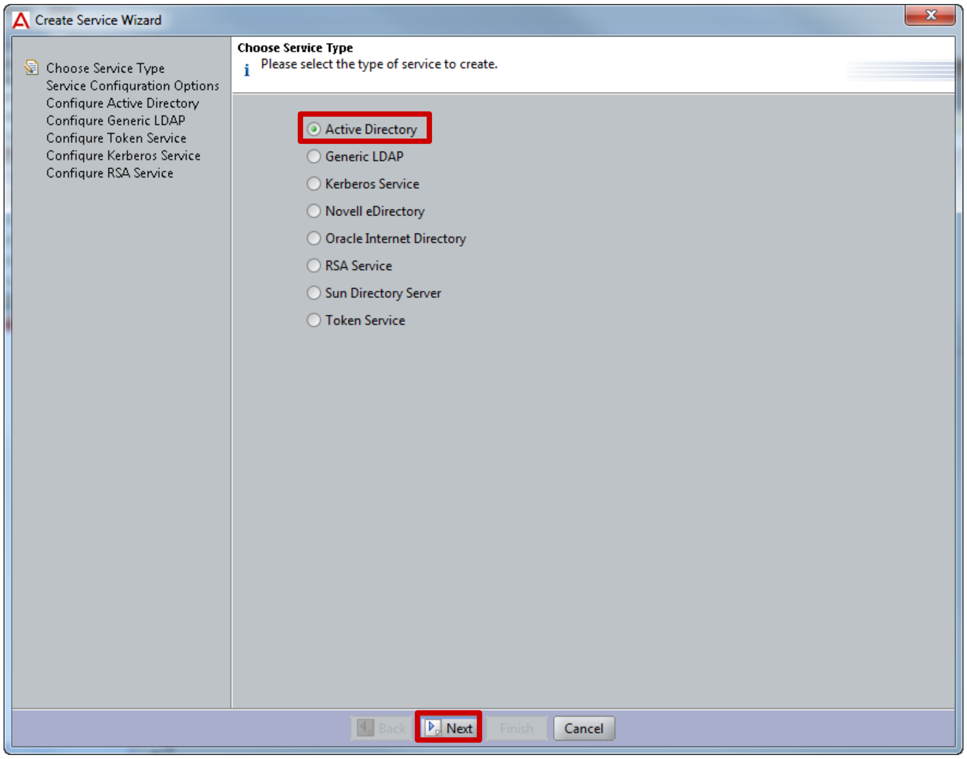


Current Site: AvayaLabs

Directory Services

Name	Directory Type
Internal User Store	Internal Database

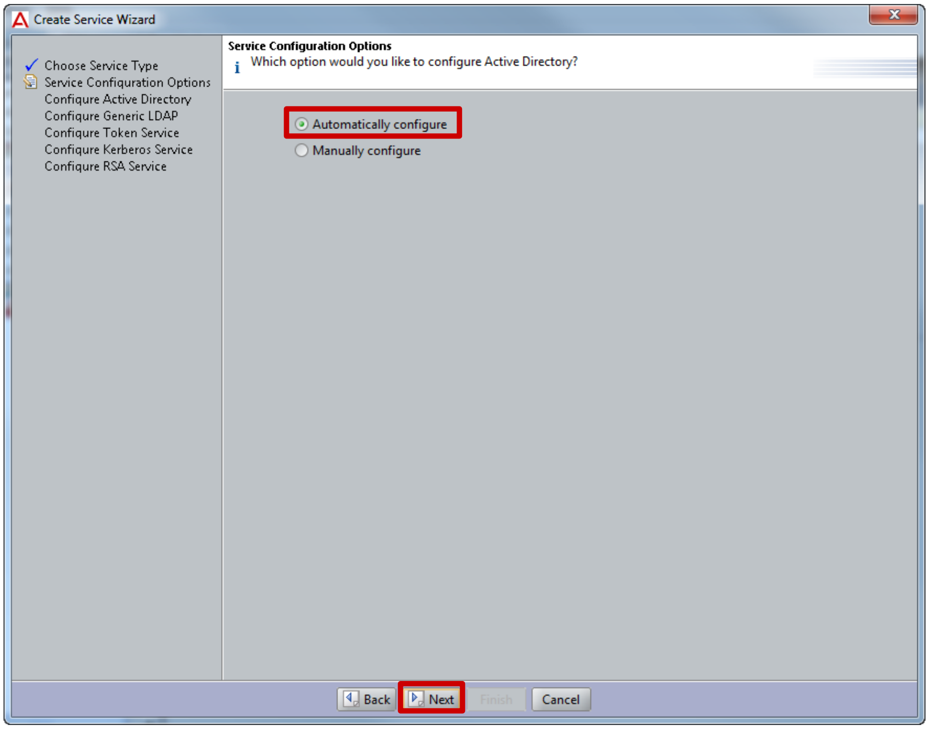
2 In the *Choose Service Type* window select *Active Directory* then click *Next*:



Choose Service Type
Please select the type of service to create.

- ● Active Directory
- ○ Generic LDAP
- ○ Kerberos Service
- ○ Novell eDirectory
- ○ Oracle Internet Directory
- ○ RSA Service
- ○ Sun Directory Server
- ○ Token Service

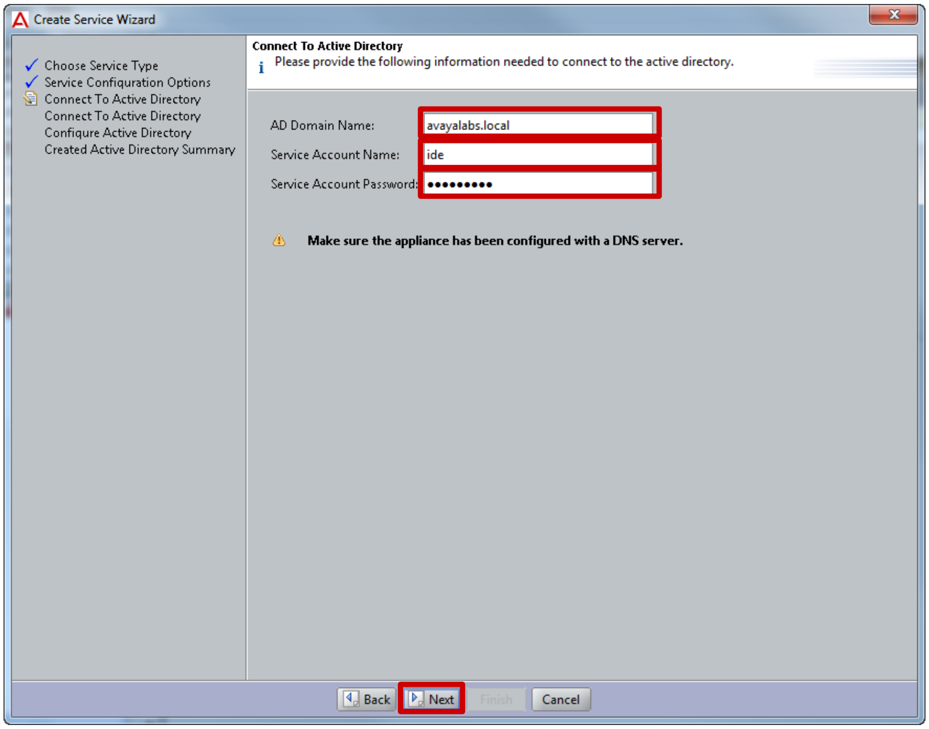
3 In the *Service Configuration Options* window select *Automatically Configure* then click *Next*:



Service Configuration Options
Which option would you like to configure Active Directory?

- ● Automatically configure
- ○ Manually configure

4 In the *Connect To Active Directory* window enter the *AD Domain Name*, *Service Account Name* and *Password*. Click *Next*:


Create Service Wizard
✓ Choose Service Type
✓ Service Configuration Options
Connect To Active Directory
Connect To Active Directory
Configure Active Directory
Created Active Directory Summary
Back
Next
Finish
Cancel

Connect To Active Directory

Please provide the following information needed to connect to the active directory.

AD Domain Name: avayalabs.local

Service Account Name: ide

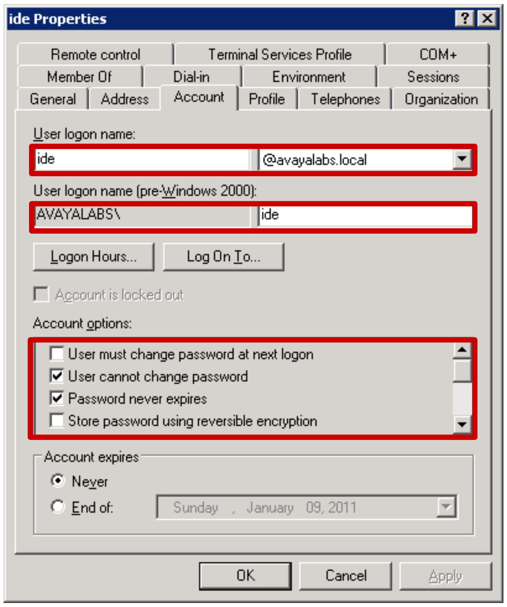
Service Account Password: •••••••••

Make sure the appliance has been configured with a DNS server.

Note – To communicate with Active Directory DNS must be enabled and configured on the Ignition Server. DNS can be configured by clicking ***Appliance-Name > System > DNS***.

Note – In this example an Active Directory account called ***ide*** with the password ***avayalabs*** has been pre-defined in Active Directory and is a member of the ***Domain Admins*** group. Account options have also been set to lock the account password so that it cannot change.

Note – While the bind user account has been made a member of the ***Domain Admins*** group, the bind user account can be a member of the ***Domain Users*** group as long as it has the necessary privileges required to ***Create Computer Objects*** in the domain (http://technet.microsoft.com/en-us/library/cc754478.aspx).



ide Properties

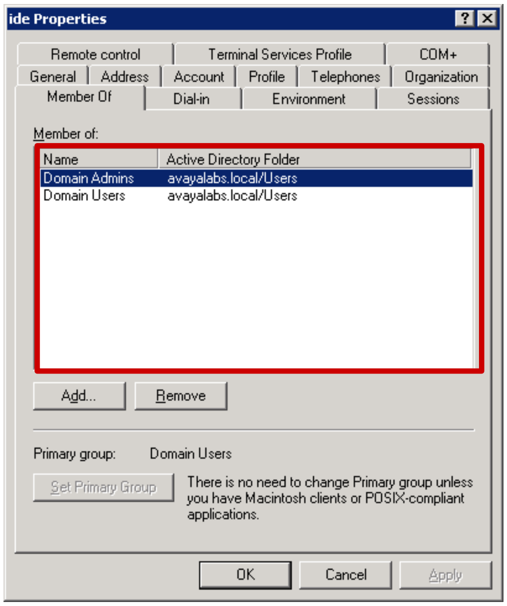
User logon name:
ide @avayalabs.local

User logon name (pre-Windows 2000):
AVAYALABS\ ide

□ Account is locked out

Account options:
- □ User must change password at next logon
- ☑ User cannot change password
- ☑ Password never expires
- □ Store password using reversible encryption

Account expires
- ● Never
- ○ End of: Sunday , January 09, 2011



ide Properties

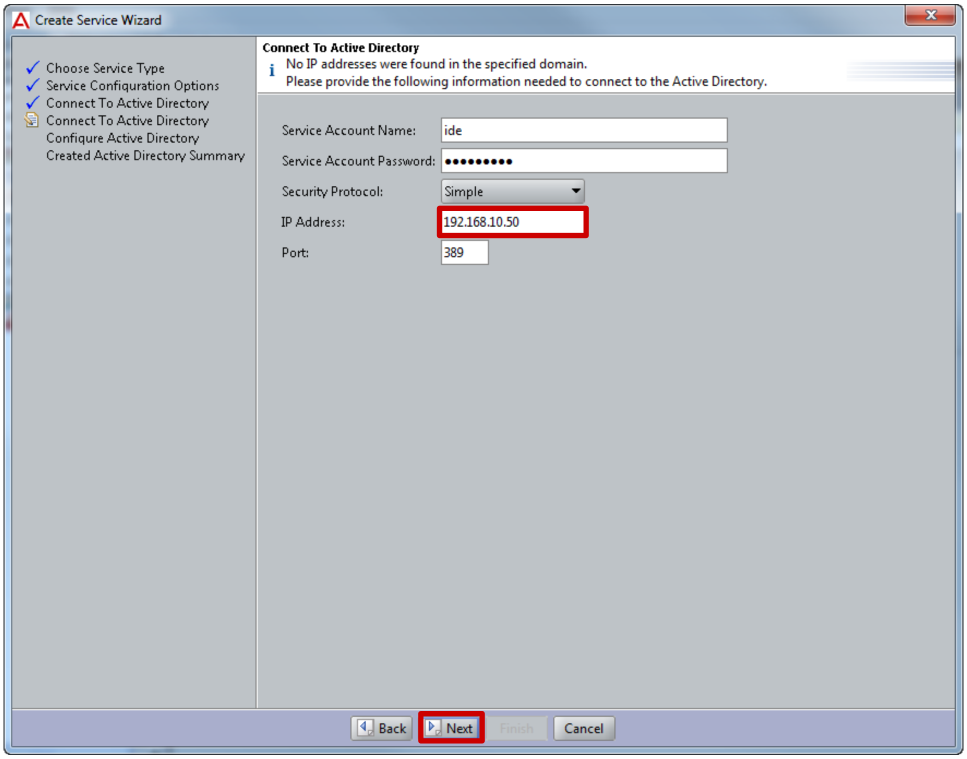
Member of:

Name	Active Directory Folder
Domain Admins	avayalabs.local/Users
Domain Users	avayalabs.local/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

5 In the *Connect to Active Directory* window select the *Security Protocols* type *Simple* then enter the *IP address* of the *Active Directory Domain Controller*. Click *Next*:



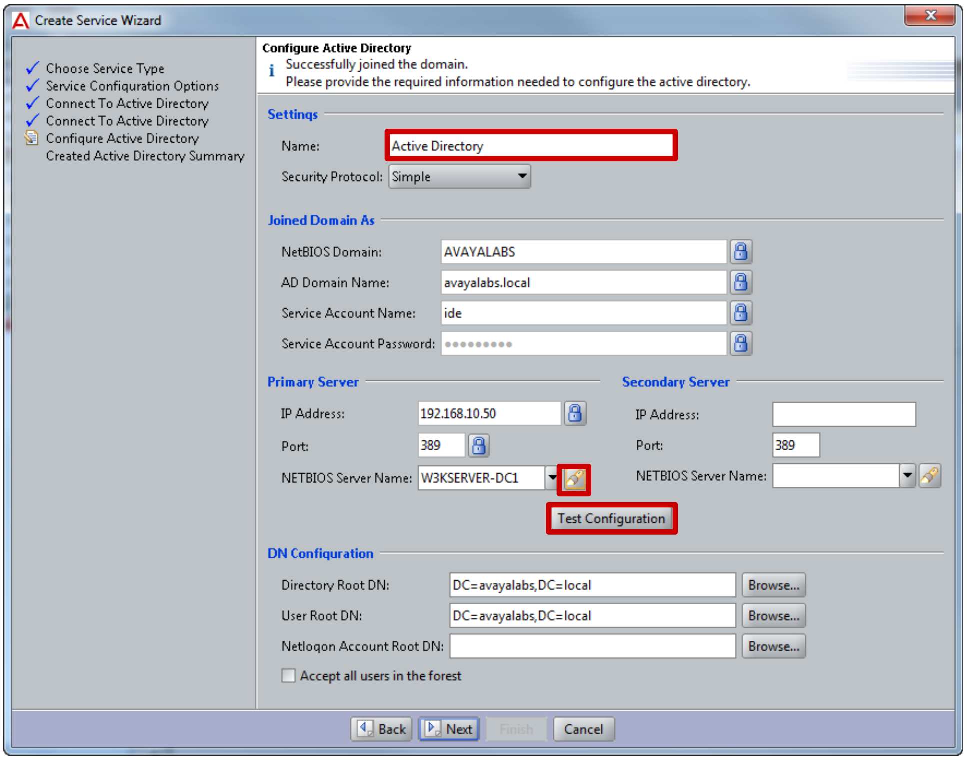
- ✓ Choose Service Type
- ✓ Service Configuration Options
- ✓ Connect To Active Directory
- Connect To Active Directory
- Configure Active Directory
- Created Active Directory Summary

Connect To Active Directory

No IP addresses were found in the specified domain.
Please provide the following information needed to connect to the Active Directory.

Service Account Name: ide
Service Account Password: •••••••••
Security Protocol: Simple
IP Address: 192.168.10.50
Port: 389

6 In the *Configure Active Directory Window* set the *Name* to *Active Directory*. Click the icon next to the *NETBIOS Server Name* field to resolve the NETBIOS server name. Verify the Active Directory configuration by selecting *Test Configuration*:


Create Service Wizard

- ✓ Choose Service Type
- ✓ Service Configuration Options
- ✓ Connect To Active Directory
- ✓ Connect To Active Directory
- Configure Active Directory
- Created Active Directory Summary

Configure Active Directory

Successfully joined the domain.
Please provide the required information needed to configure the active directory.

Settings

Name: Active Directory
Security Protocol: Simple

Joined Domain As

NetBIOS Domain: AVAYALABS
AD Domain Name: avayalabs.local
Service Account Name: ide
Service Account Password: ●●●●●●●●●

Primary Server

IP Address: 192.168.10.50
Port: 389
NETBIOS Server Name: W3KSERVER-DC1

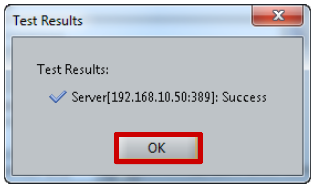
Secondary Server

IP Address:
Port: 389
NETBIOS Server Name:

DN Configuration

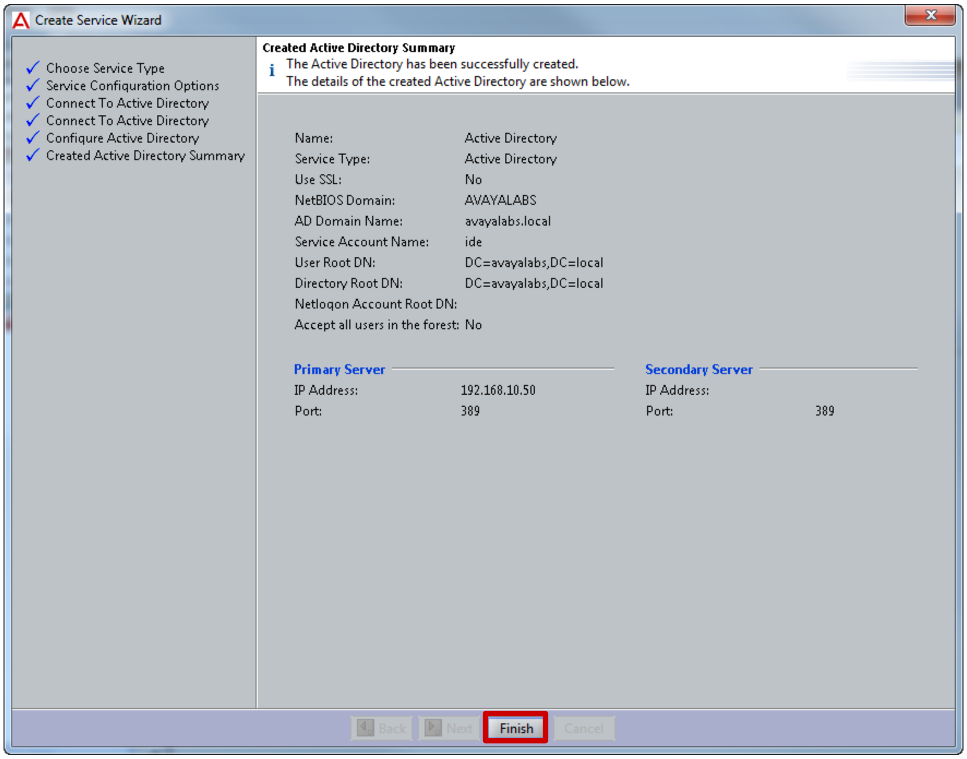
Directory Root DN: DC=avayalabs,DC=local
User Root DN: DC=avayalabs,DC=local
Netlogon Account Root DN:
□ Accept all users in the forest

7 If the Active Directory configuration is correct and the test successful, the following dialog message will be displayed. Click *OK* then *Next*:


Test Results

Test Results:
✓ Server[192.168.10.50:389]: Success

8 A summary of the Active Directory configuration will be displayed. Click *Finish*:


Create Service Wizard
✓ Choose Service Type
✓ Service Configuration Options
✓ Connect To Active Directory
✓ Connect To Active Directory
✓ Configure Active Directory
✓ Created Active Directory Summary
Back
Next
Finish
Cancel

Created Active Directory Summary

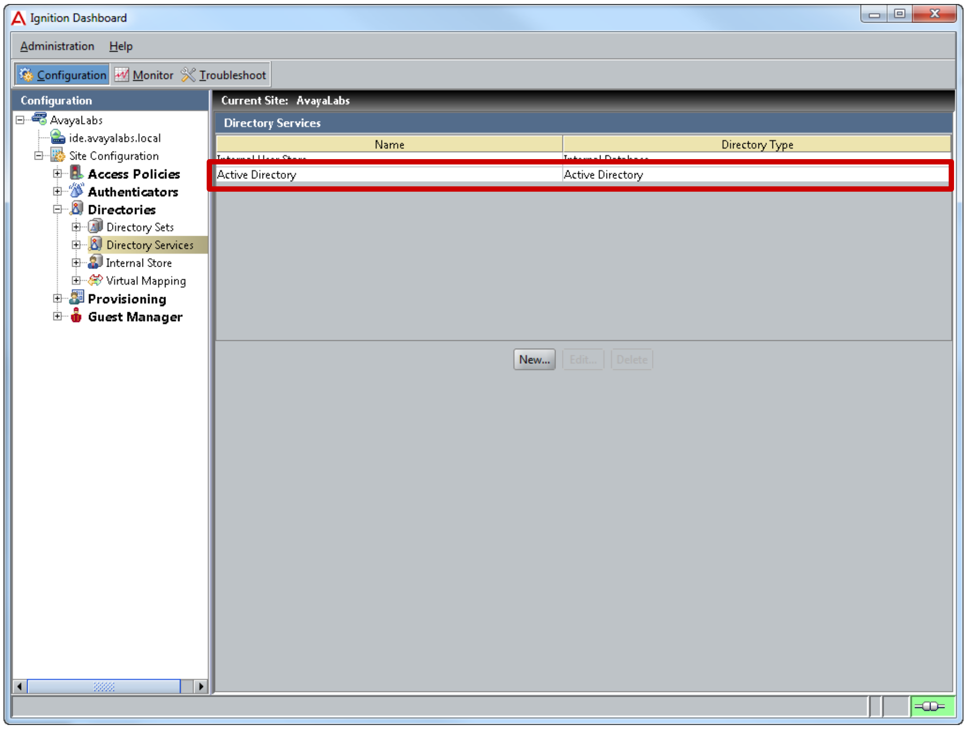
The Active Directory has been successfully created.
The details of the created Active Directory are shown below.

Name:	Active Directory
Service Type:	Active Directory
Use SSL:	No
NetBIOS Domain:	AVAYALABS
AD Domain Name:	avayalabs.local
Service Account Name:	ide
User Root DN:	DC=avayalabs,DC=local
Directory Root DN:	DC=avayalabs,DC=local
Netlogon Account Root DN:	
Accept all users in the forest:	No

Primary Server
IP Address: 192.168.10.50
Port: 389

Secondary Server
IP Address:
Port: 389

9 A *Directory Service* called *Active Directory* has now been added to the Ignition Server:



Current Site: AvayaLabs

Directory Services

Name	Directory Type
Internal User Store	Internal Database
Active Directory	Active Directory

2.3.3 Directory Sets

Directory sets are an ordered list of user lookup services used by the Ignition Server when it processes authentication requests. The directory set determines where the user account information is located (i.e. local, Active Directory, LDAP etc.), which service is used to retrieve the user's account information, and which service is used to retrieve authorization data such as attributes and group membership.

2.3.3.1 Configuration Step

For this configuration step a directory set named ***Active Directory*** will be created that will authenticate and authorize PEAP users against the ***Active Directory*** user store:

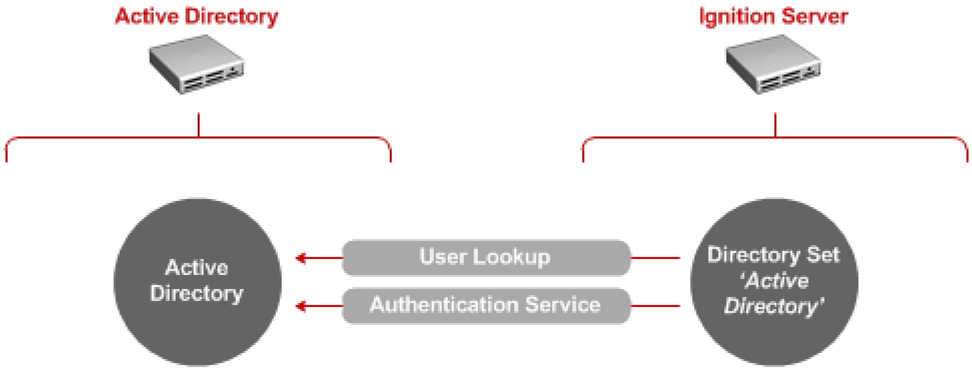
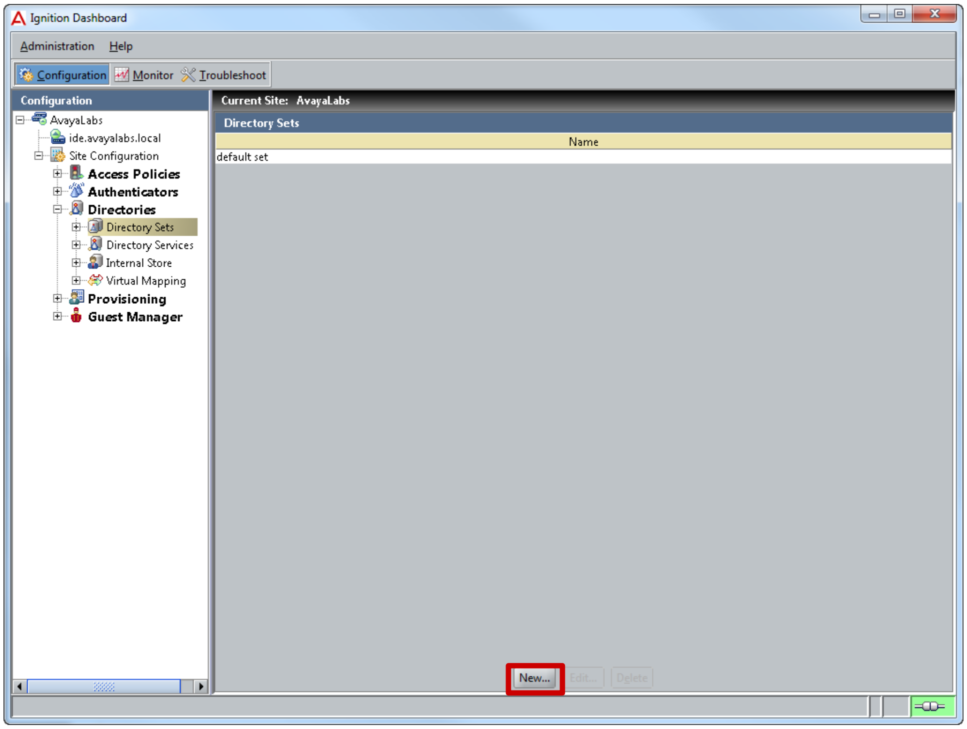


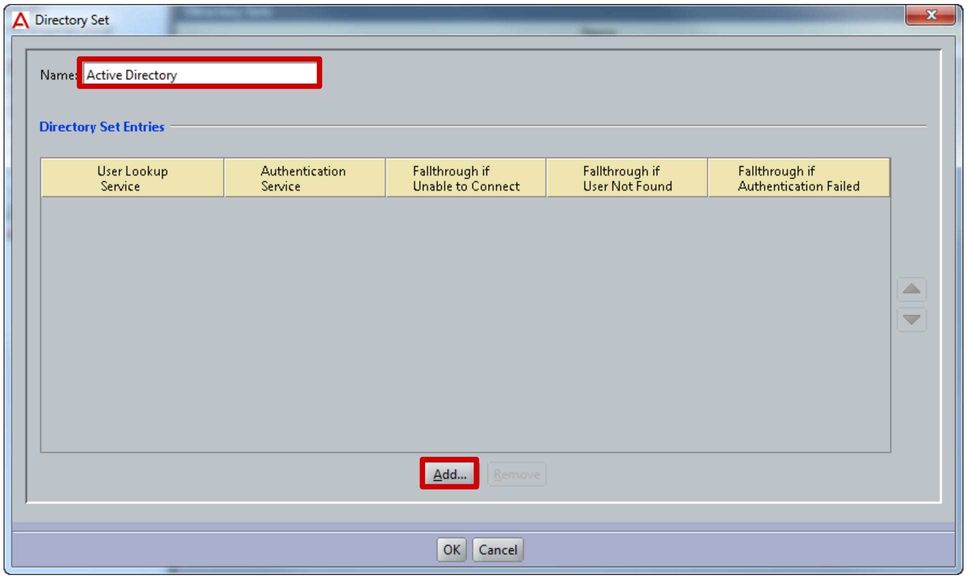
Figure 2.3.3.1 – Directory Sets

1 Within *Ignition Dashboard* select *Configuration* > *Directories* > *Directory Sets*. Click *New*:



Name
default set

2 Set the *Name* to *Active Directory* then click *Add*:



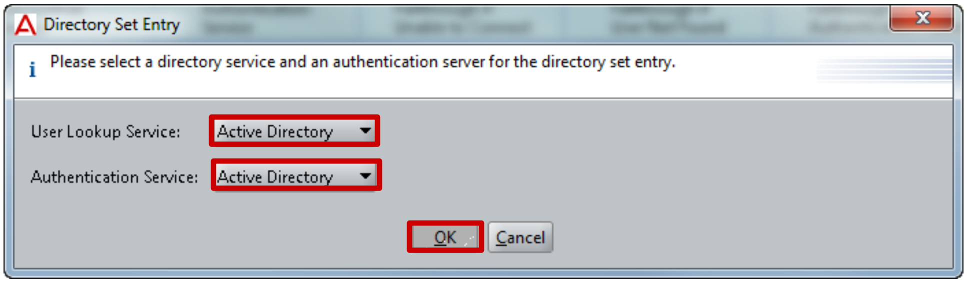
Directory Set

Name: Active Directory

Directory Set Entries

User Lookup Service	Authentication Service	Fallthrough if Unable to Connect	Fallthrough if User Not Found	Fallthrough if Authentication Failed

3 Set the *User Lookup Service* and *Authentication Service* to the Directory Service named *Active Directory* then click *OK*:



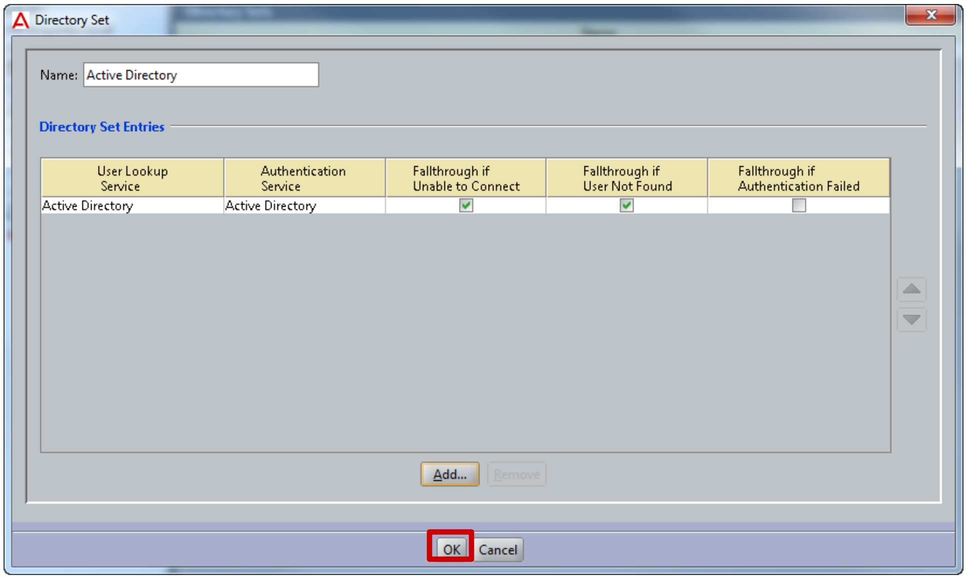
Directory Set Entry

Please select a directory service and an authentication server for the directory set entry.

User Lookup Service: Active Directory

Authentication Service: Active Directory

4 Use the default values then click *OK*:



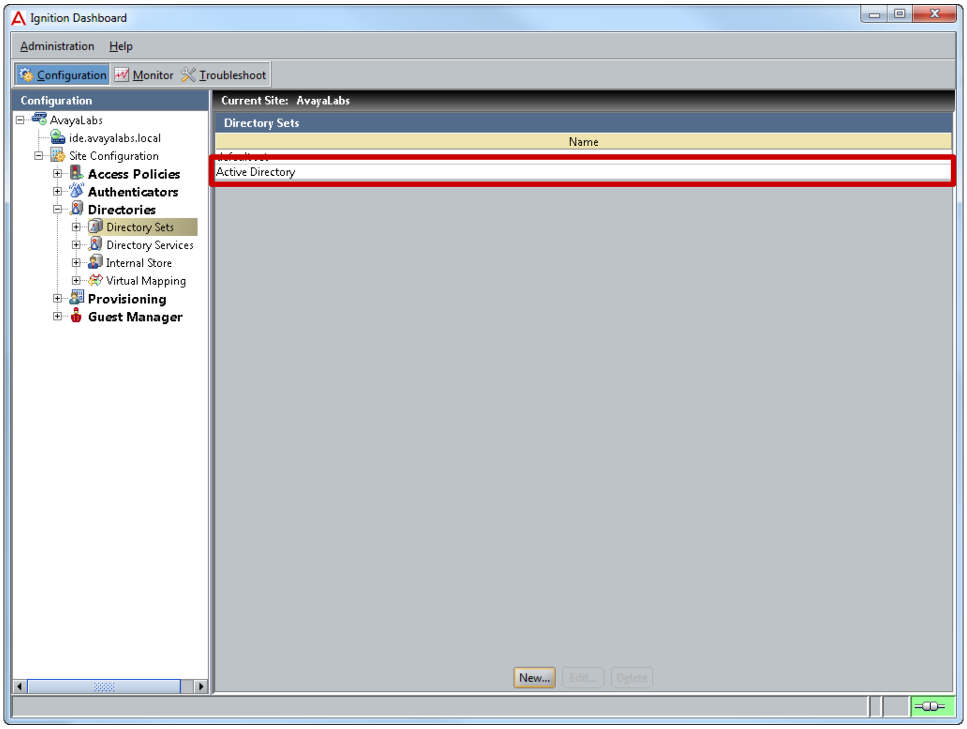
Directory Set

Name: Active Directory

Directory Set Entries

User Lookup Service	Authentication Service	Fallthrough if Unable to Connect	Fallthrough if User Not Found	Fallthrough if Authentication Failed
Active Directory	Active Directory	☑	☑	☐

5 A *Directory Set* called *Active Directory* has now been added to the Ignition Server:



Current Site: AvayaLabs

Directory Sets

Name
Active Directory

2.3.4 Virtual Groups

Virtual groups provide a mechanism that allows the Ignition Server to map external groups stored in the Active Directory tree to virtual groups within the Ignition Server. The virtual groups can be used by the Access Policy to determine if the user is authorized to access the system as well as assign return attributes to the authenticator such as VLAN assignments.

2.3.4.1 Configuration Step

For this configuration step Virtual Groups called ***Sales***, ***Marketing***, ***Engineering*** and ***Domain Computers*** will be created that map to their corresponding Active Directory groups. Based on the computer and users Active Directory group membership, the Access Policy (created later) will apply authorization restrictions as well as assign VLAN membership.

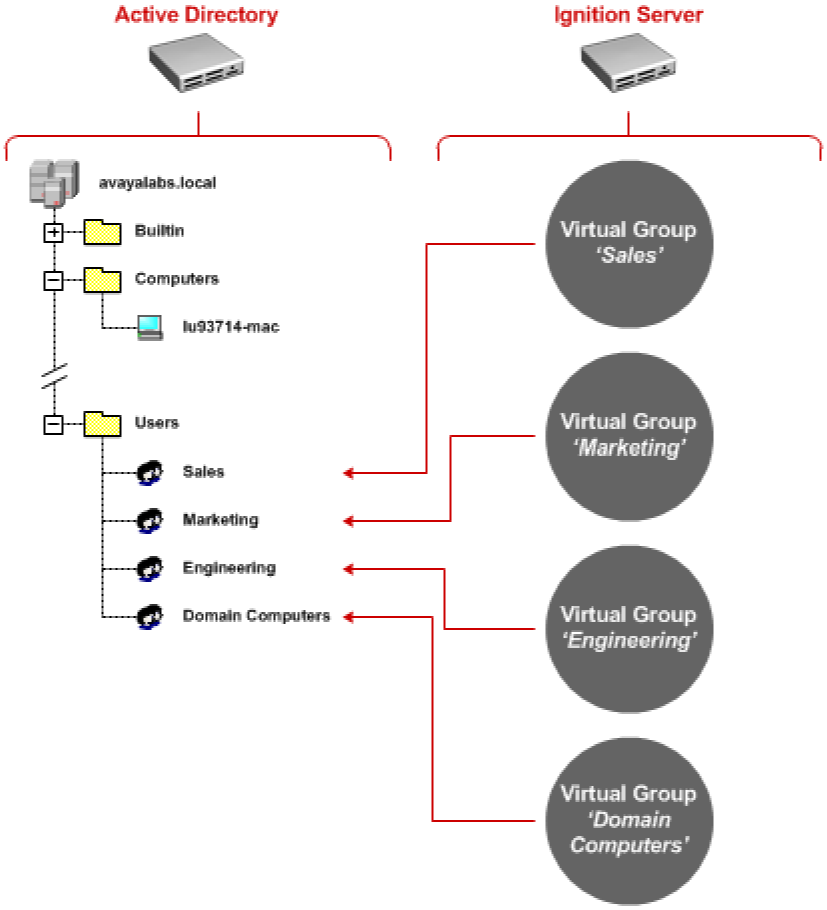
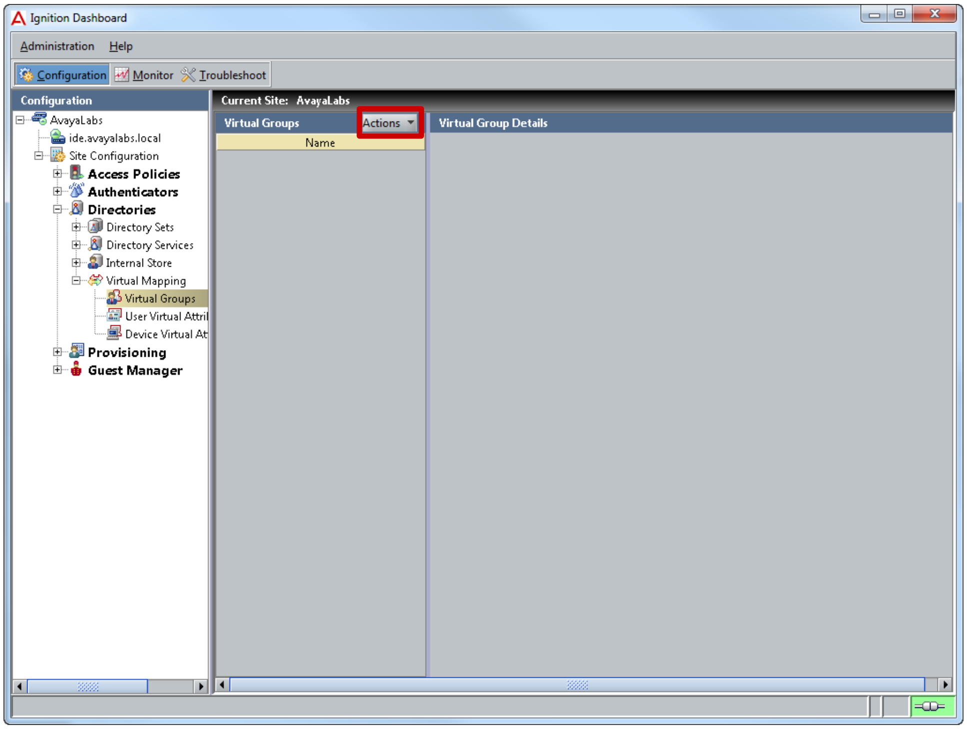


Figure 2.3.4.1 – Virtual Groups

ⓘ Note – The Active Directory Groups must be present in the Active Directory tree prior to mapping the Virtual Groups.

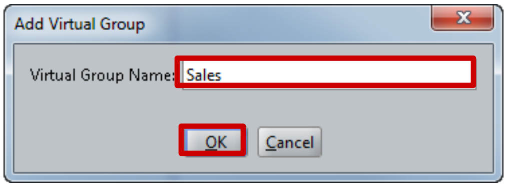
ⓘ Note – If an Active Directory group is not visible on the Ignition Server, you can force a cache refresh by selecting ***Monitor > Ignition-Server-Name > Directory Services Status > Refresh Cache***.

1 Within *Ignition Dashboard* select *Configuration > Virtual Mapping > Virtual Groups*. Click *Actions > Add a New Virtual Group*:

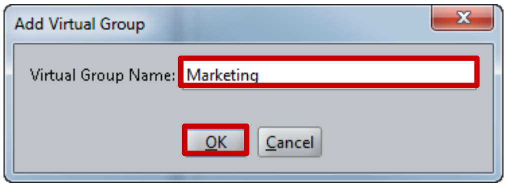


Current Site: AvayaLabs

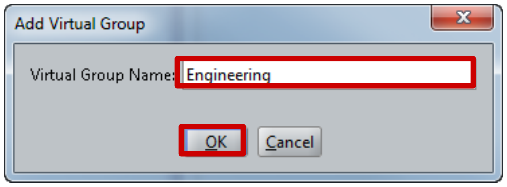
2 Add a virtual group for each Active Directory group which PEAP computers and users are assigned in Active Directory. In this example EAP users are assigned to Active Directory Groups called *Sales*, *Marketing* and *Engineering* while the computers are assigned to the Active Directory group named *Domain Computers*:



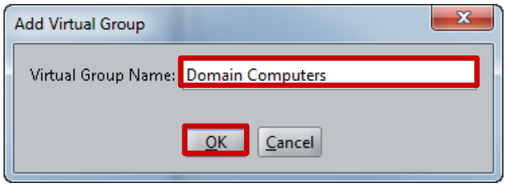
Virtual Group Name: Sales



Virtual Group Name: Marketing

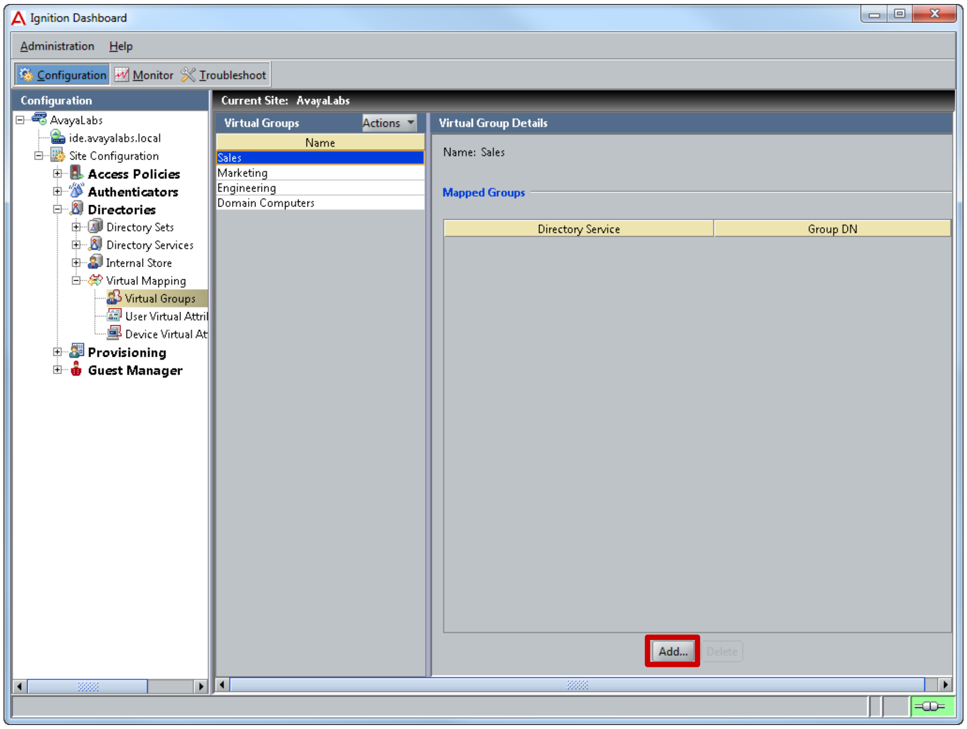


Virtual Group Name: Engineering

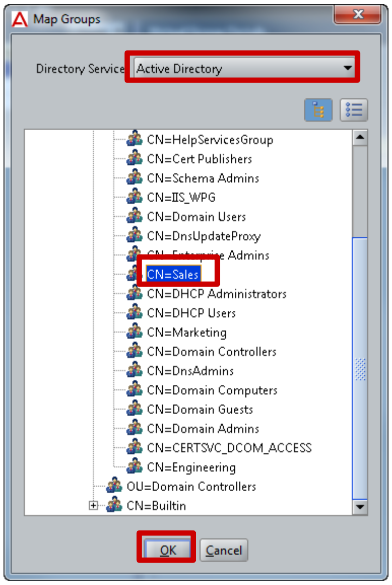


Virtual Group Name: Domain Computers

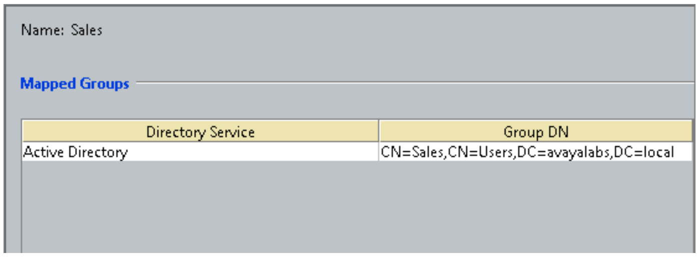
3 Highlight the *Virtual Group* called *Sales* then select a *Add*:



4 Set the *Directory Service* named *Active Directory* then in the Active Directory tree locate the Active Directory group to map the Virtual Group too. Click *OK*. In this example the *Virtual Group* called *Sales* is mapped to its corresponding Active Directory Group *CN=Sales,CN=Users,DC=avayalabs,DC=local*:



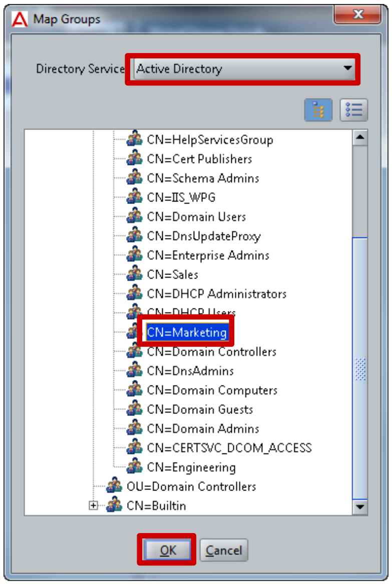
Directory Service: Active Directory


Name: Sales

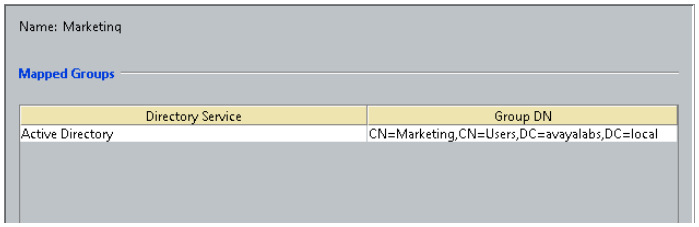
Mapped Groups

Directory Service	Group DN
Active Directory	CN=Sales,CN=Users,DC=avayalabs,DC=local

5 Select the *Marketing* Virtual Group then click *Add*. Select the *Directory Service* named *Active Directory* then in the Active Directory tree locate the Active Directory group name to map the Virtual Group too. Click *OK*. In this example the *Virtual Group* called *Marketing* is mapped to its corresponding Active Directory Group *CN=Marketing,CN=Users,DC=avayalabs,DC=local*:



Directory Service: Active Directory

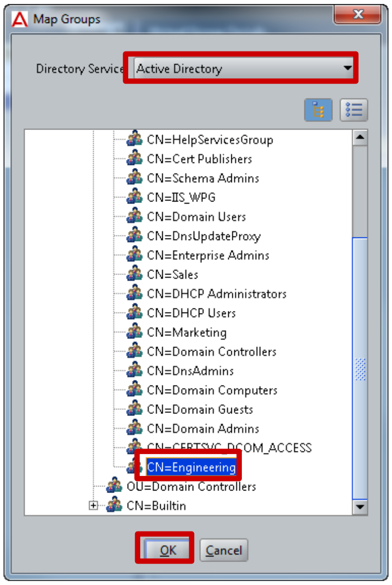


Name: Marketing

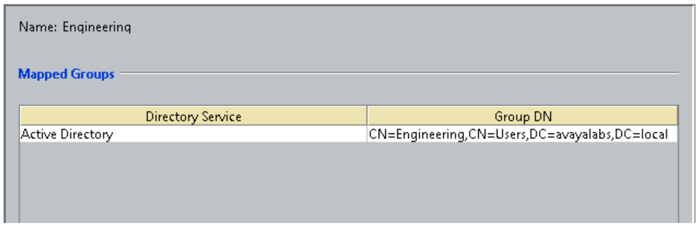
Mapped Groups

Directory Service	Group DN
Active Directory	CN=Marketing,CN=Users,DC=avayalabs,DC=local

6 Select the *Engineering* Virtual Group then click *Add*. Select the *Directory Service* named *Active Directory* then in the Active Directory tree locate the Active Directory group name to map the Virtual Group too. Click *OK*. In this example the *Virtual Group* called *Engineering* is mapped to its corresponding Active Directory Group *CN=Engineering,CN=Users,DC=avayalabs,DC=local*:



Directory Service: Active Directory

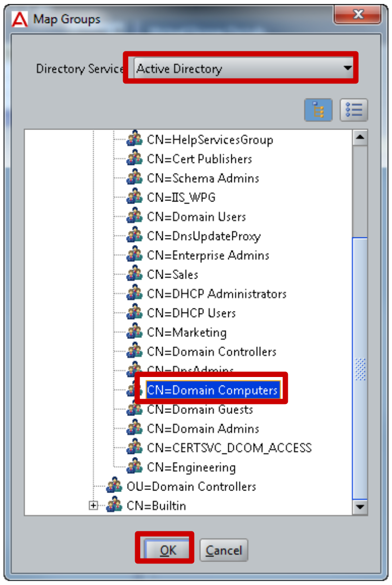


Name: Engineering

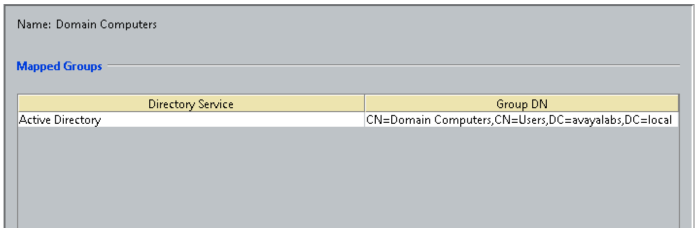
Mapped Groups

Directory Service	Group DN
Active Directory	CN=Engineering,CN=Users,DC=avayalabs,DC=local

7 **Select the *Domain Computers* Virtual Group then click *Add*. Select the *Directory Service* named *Active Directory* then in the Active Directory tree locate the Active Directory group name to map the Virtual Group too. Click *OK*. In this example the *Virtual Group* called *Engineering* is mapped to its corresponding Active Directory Group *CN=Domain Computers,CN=Users,DC=avayalabs,DC=local*:**



Directory Service: Active Directory



Name: Domain Computers

Mapped Groups

Directory Service	Group DN
Active Directory	CN=Domain Computers,CN=Users,DC=avayalabs,DC=local

2.3.5 Virtual LANs

NAP users connected to an Avaya Ethernet Switch or Wireless Access Point can be assigned to a dynamic VLAN based on NAP compliance and Active Directory group membership. VLAN information is forwarded to the Authenticator with the RADIUS ***Access-Accept*** and can include the VLAN ID or VLAN name. Avaya Ethernet Routing Switches support VLAN information using an ID while the Wireless LAN 8180 Wireless Controllers support VLAN names. The Ignition Server determines the format of the VLAN information based on the vendor device template assigned to the Authenticator.

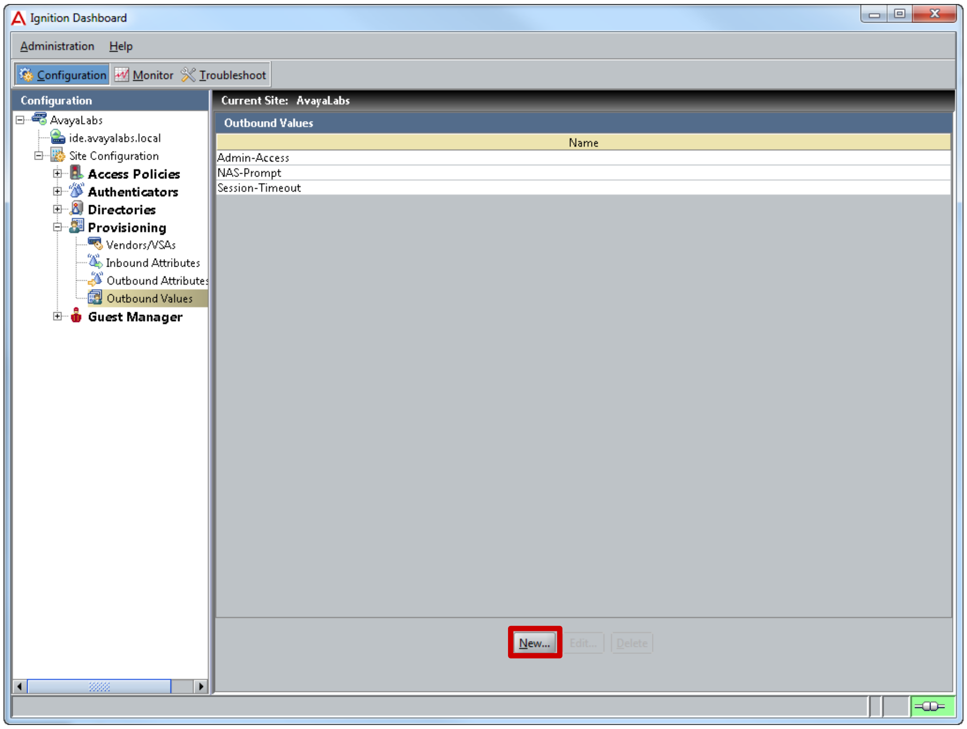
2.3.5.1 Configuration Steps

For this configuration step three VLANs will be defined for NAP compliant ***Sales***, ***Marketing*** and ***Engineering*** users and non-compliant NAP users:

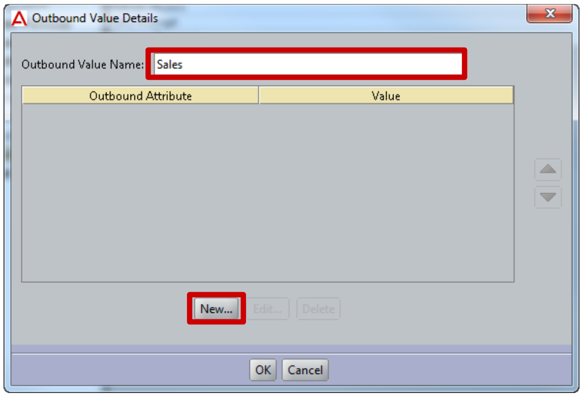
NAP Compliance State	Group Membership	VLAN ID	VLAN Name
Compliant	Sales	11	Sales
Compliant	Marketing	12	Marketing
Compliant	Engineering	13	Engineering
Non-Compliant	N/A	14	Remediated

Table 2.3.5.1 – Dynamic VLANs

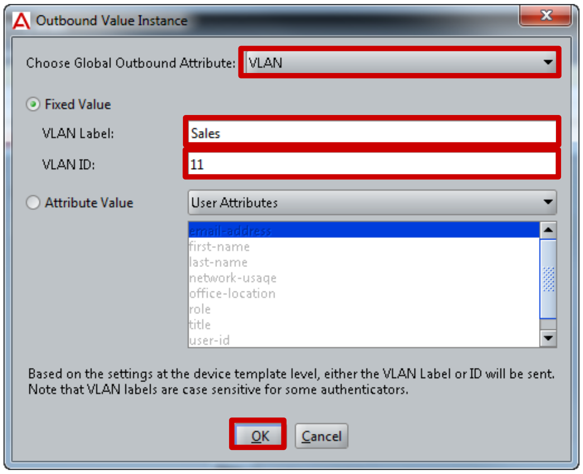
1 Within *Ignition Dashboard* select *Configuration > Provisioning > Outbound Values*. Click *New*:



2 In the *Outbound Value Name* field enter *Sales* then click *New*:



3 Select the *Global Outbound Attribute* type *VLAN*. In the *VLAN Label* field enter *Sales* then in the VLAN ID field enter *11*. Click *OK* then *OK*:



Outbound Value Instance

Choose Global Outbound Attribute: VLAN

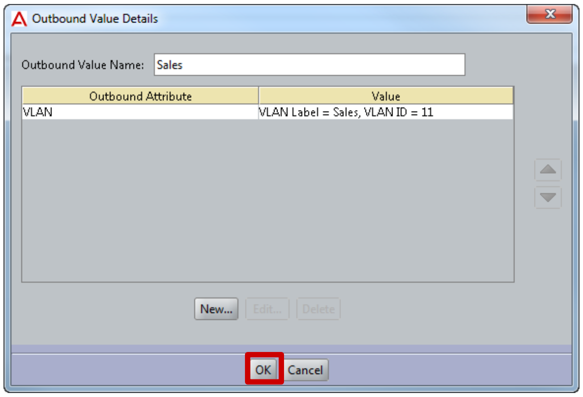
● Fixed Value

VLAN Label: Sales

VLAN ID: 11

○ Attribute Value: User Attributes

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.

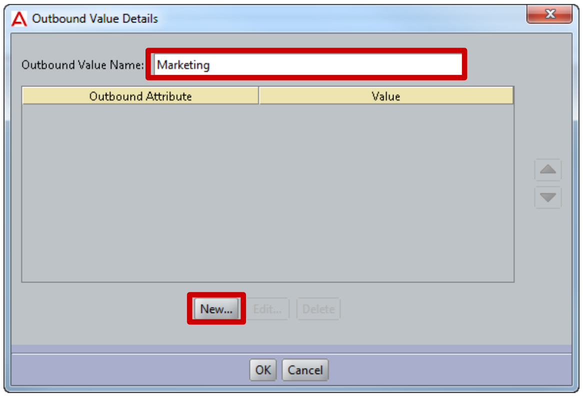


Outbound Value Details

Outbound Value Name: Sales

Outbound Attribute	Value
VLAN	VLAN Label = Sales, VLAN ID = 11

4 Click *New*. In the *Outbound Value Name* field enter *Marketing* then click *New*:

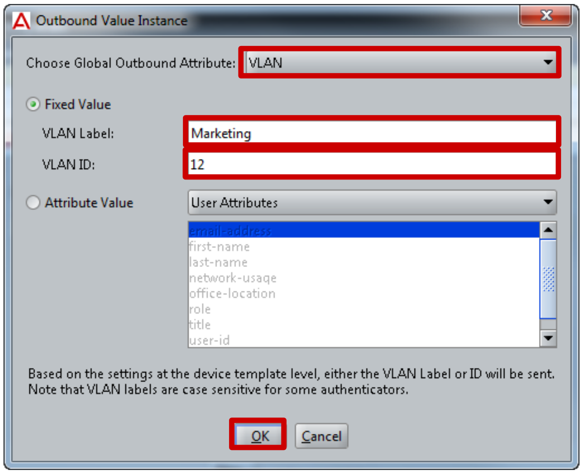


Outbound Value Details

Outbound Value Name: Marketing

Outbound Attribute	Value

5 Select the *Global Outbound Attribute* type *VLAN*. In the *VLAN Label* field enter *Marketing* then in the VLAN ID field enter *12*. Click *OK* then *OK*:



Outbound Value Instance

Choose Global Outbound Attribute: VLAN

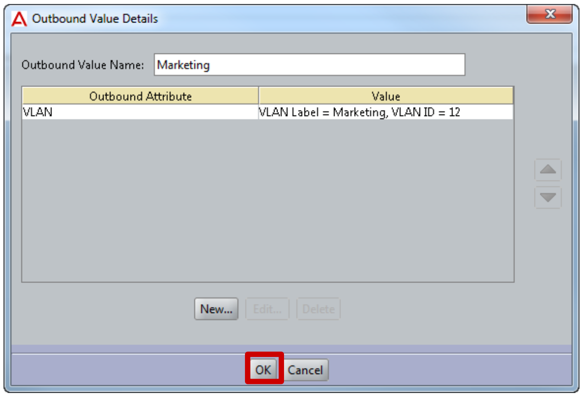
● Fixed Value

VLAN Label: Marketing

VLAN ID: 12

○ Attribute Value: User Attributes

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.

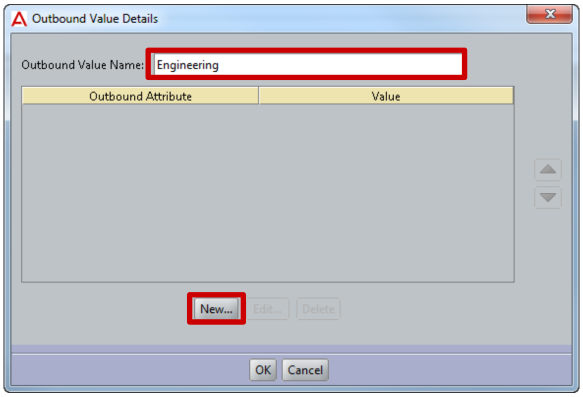


Outbound Value Details

Outbound Value Name: Marketing

Outbound Attribute	Value
VLAN	VLAN Label = Marketing, VLAN ID = 12

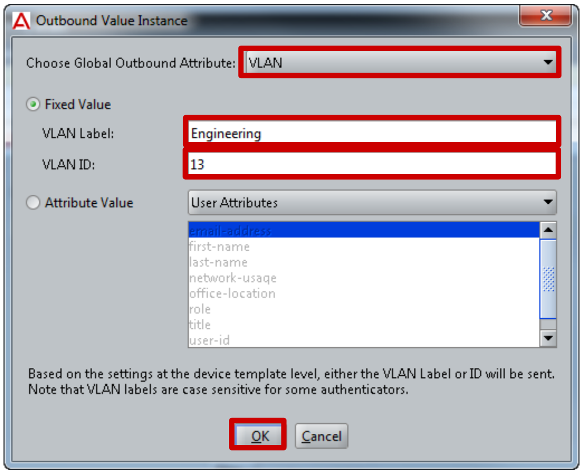
6 Click *New*. In the *Outbound Value Name* field enter *Engineering* then click *New*:



Outbound Value Name: Engineering

Outbound Attribute	Value

7 Select the *Global Outbound Attribute* type *VLAN*. In the *VLAN Label* field enter *Engineering* then in the VLAN ID field enter *13*. Click *OK* then *OK*:



Choose Global Outbound Attribute: VLAN

● Fixed Value

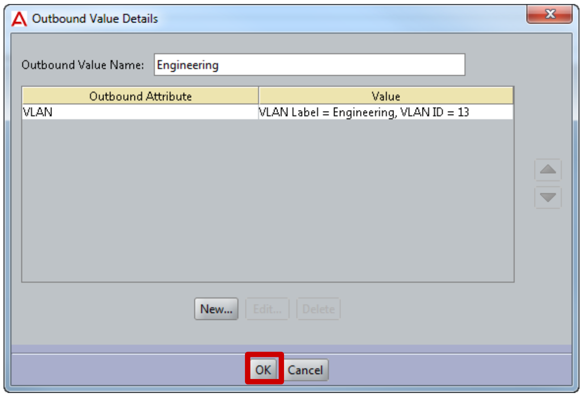
VLAN Label: Engineering

VLAN ID: 13

○ Attribute Value: User Attributes

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

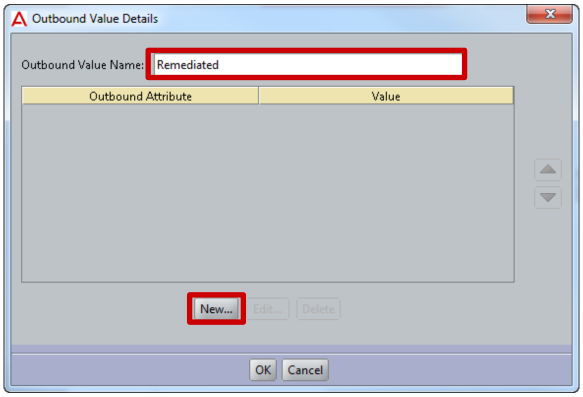
Based on the settings at the device template level, either the VLAN Label or ID will be sent. Note that VLAN labels are case sensitive for some authenticators.



Outbound Value Name: Engineering

Outbound Attribute	Value
VLAN	VLAN Label = Engineering, VLAN ID = 13

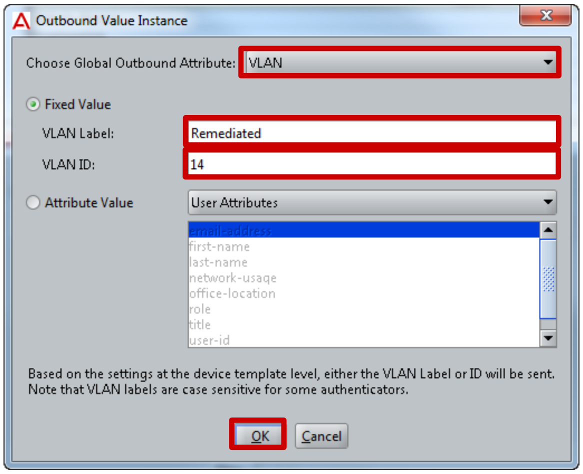
8 Click *New*. In the *Outbound Value Name* field enter *Remediated* then click *New*:



Outbound Value Name: Remediated

Outbound Attribute	Value

9 Select the *Global Outbound Attribute* type *VLAN*. In the *VLAN Label* field enter *Remediated* then in the VLAN ID field enter *14*. Click *OK* then *OK*:



Outbound Value Instance

Choose Global Outbound Attribute: VLAN

● Fixed Value

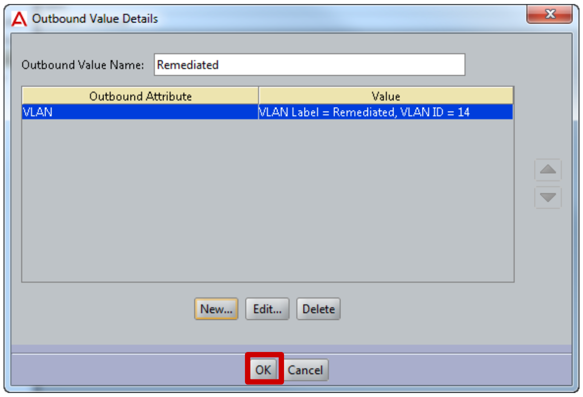
VLAN Label: Remediated

VLAN ID: 14

○ 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.

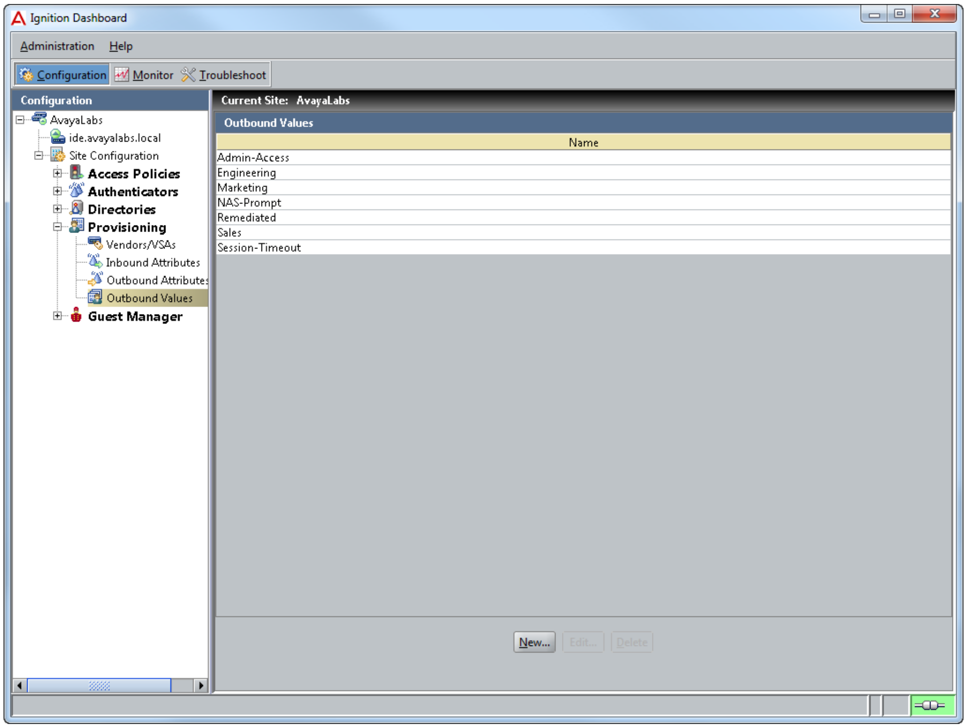


Outbound Value Details

Outbound Value Name: Remediated

Outbound Attribute	Value
VLAN	VLAN Label = Remediated, VLAN ID = 14

10 Outbound VLAN definitions for *Sales*, *Marketing*, *Engineering* and *Remediated* users have now been defined:



Current Site: AvayaLabs

Outbound Values

Name
Admin-Access
Engineering
Marketing
NAS-Prompt
Remediated
Sales
Session-Timeout

Note – For dynamic VLAN assignment to be successful, the VLANs must be present on the Avaya Ethernet Routing Switches and Wireless LAN 8180 Controllers.

Note – Only Windows Vista and Windows 7 support different VLAN IDs for Computers and Users. Windows XP requires both Computers and Users to be assigned to the same VLAN.

2.3.6 Posture Profiles

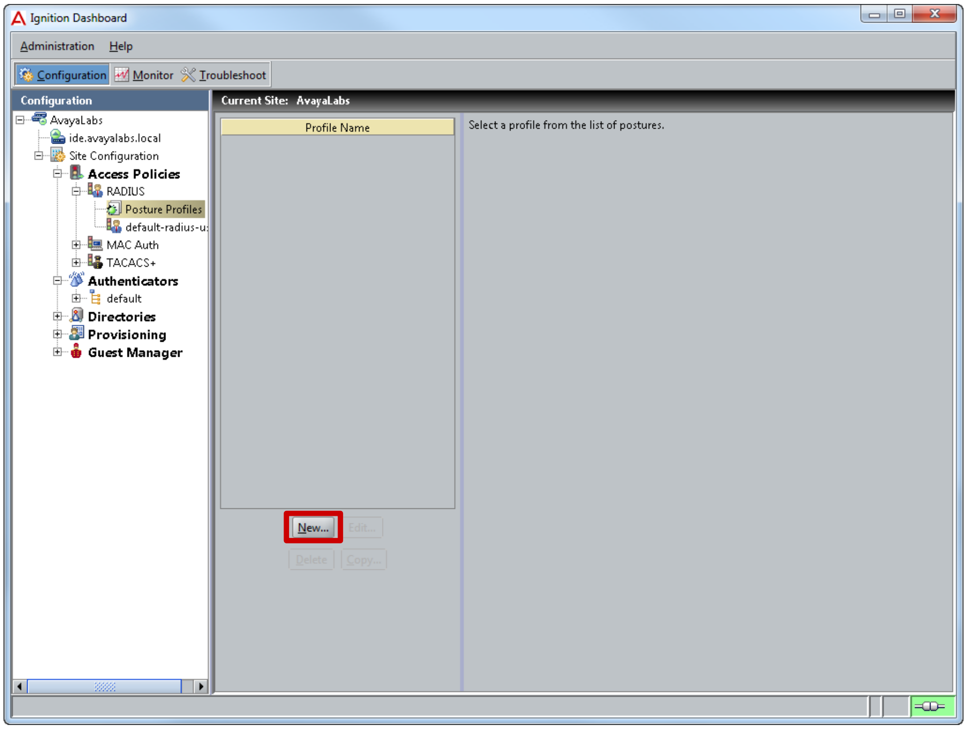
Avaya Identity Engines Ignition Server can be required to verify the health and security of a Windows workstation before a user is permitted access to the network. Posture Profiles defines the criteria that the Ignition Server uses to verify the health and compliance of the Windows workstations. Based on the Statement of Health (SoH) received from the Windows workstation, an Access Policy can permit access or remediate the device.

2.3.6.1 Configuration Steps

For this configuration step a Posture Profile named ***NAP*** will be created with the following parameters defined:

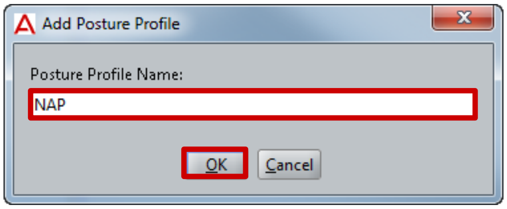
1) Verify ***Anti-Virus***, ***Anti-Spyware***, ***Firewall*** and ***Windows Automatic Updates*** are enabled.
2) Verify ***Anti-Virus*** and ***Anti-Spyware*** software is up to date.
3) Verify ***Critical updates*** are installed.
4) Enable ***Auto remediate*** to automatically correct non-compliant workstations.

1 Within *Ignition Dashboard* select *Configuration* > *Access Policies* > *Posture Profiles*. Click *New*:



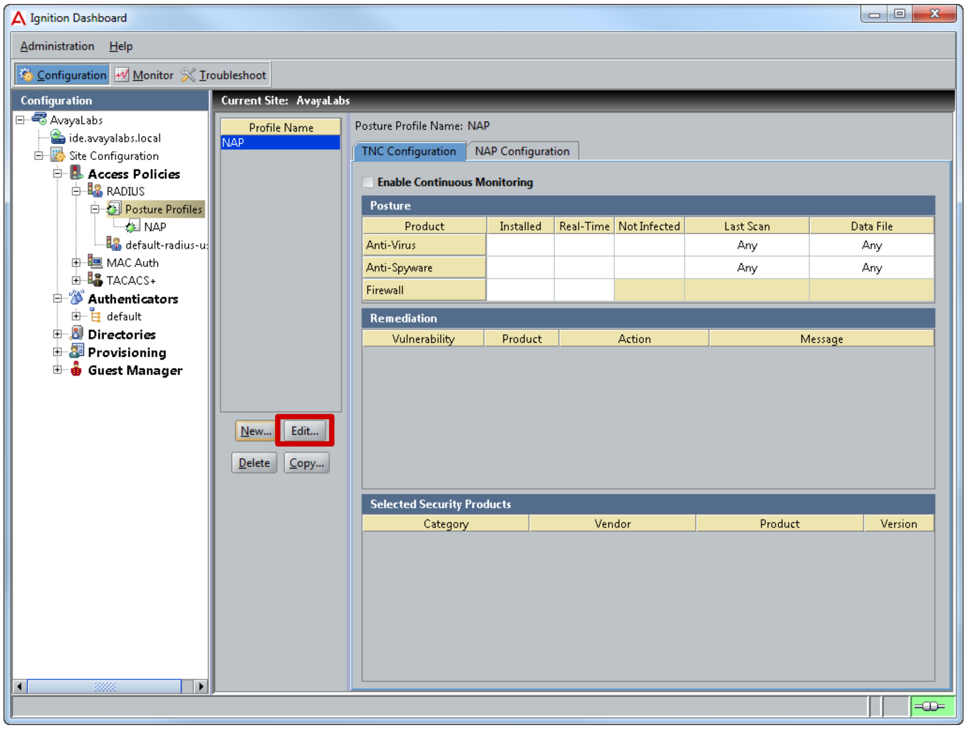
Select a profile from the list of postures.

2 Enter the name *NAP* then click *OK*:



Posture Profile Name: NAP

3 Highlight the *Posture Policy* then select *Edit*:



Current Site: AvayaLabs

Profile Name
NAP

Posture Profile Name: NAP

☐ Enable Continuous Monitoring

Posture

Product	Installed	Real-Time	Not Infected	Last Scan	Data File
Anti-Virus				Any	Any
Anti-Spyware				Any	Any
Firewall					

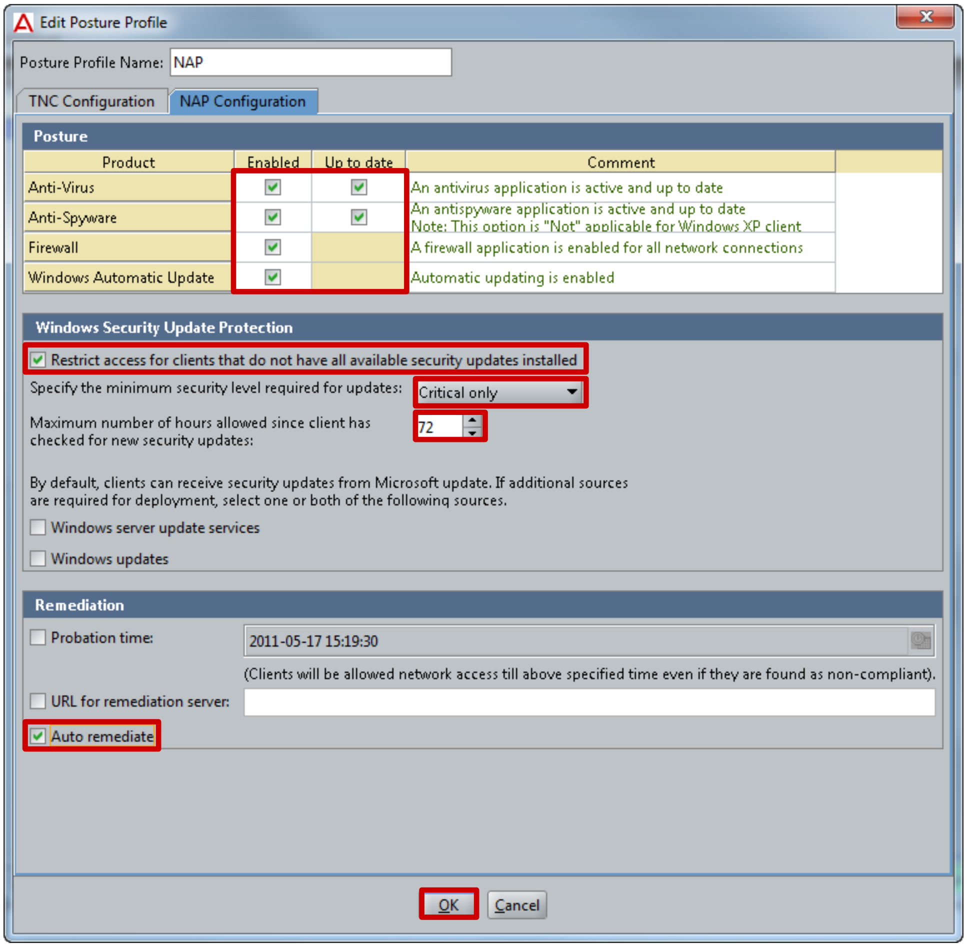
Remediation

Vulnerability	Product	Action	Message

Selected Security Products

Category	Vendor	Product	Version

4 **Select the *NAP Configuration* tab. Enable the appropriate *Postures* to check then enable the option *Restrict access for clients that do not have all available security updates installed*. Select the minimum *Security Level* then specify the number of *Hours* allowed between security updates. Enable the option *Auto remediate* then click *OK*:**



Posture Profile Name: NAP

Posture

Product	Enabled	Up to date	Comment
Anti-Virus	☑	☑	An antivirus application is active and up to date
Anti-Spyware	☑	☑	An antispyware application is active and up to date Note: This option is "Not" applicable for Windows XP client
Firewall	☑		A firewall application is enabled for all network connections
Windows Automatic Update	☑		Automatic updating is enabled

Windows Security Update Protection

☑ Restrict access for clients that do not have all available security updates installed

Specify the minimum security level required for updates: Critical only

Maximum number of hours allowed since client has checked for new security updates: 72

By default, clients can receive security updates from Microsoft update. If additional sources are required for deployment, select one or both of the following sources.

☐ Windows server update services

☐ Windows updates

Remediation

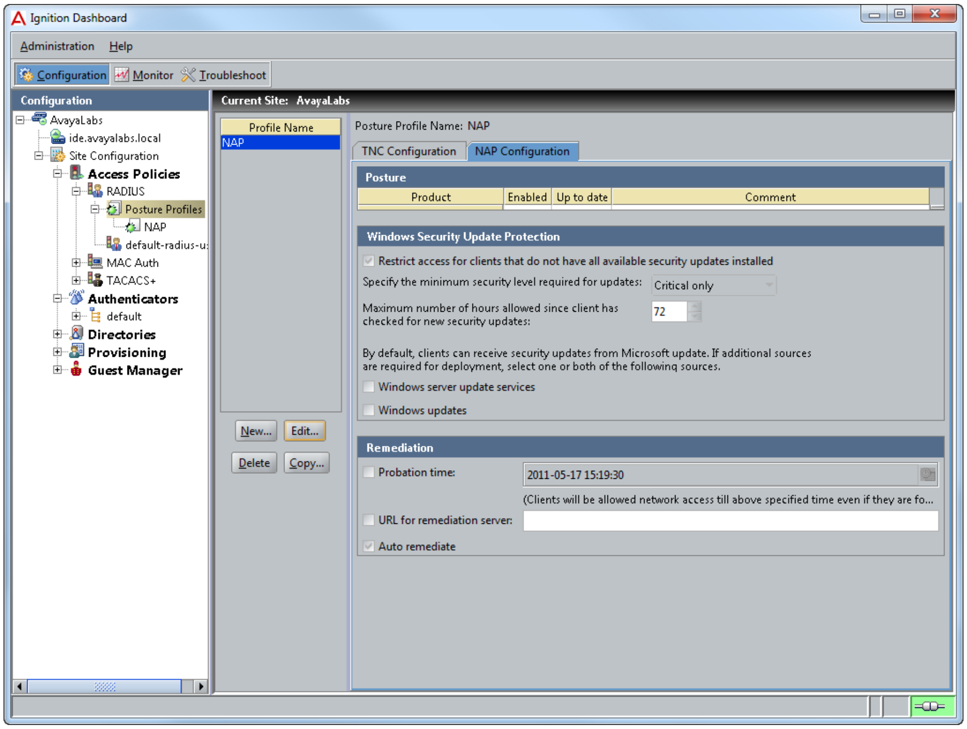
☐ Probation time: 2011-05-17 15:19:30

(Clients will be allowed network access till above specified time even if they are found as non-compliant).

☐ URL for remediation server:

☑ Auto remediate

5 A *Profile Posture* has been created on the Ignition Server:



Posture Profile Name: NAP

Posture

Product	Enabled	Up to date	Comment

Windows Security Update Protection

☑ Restrict access for clients that do not have all available security updates installed

Specify the minimum security level required for updates: Critical only

Maximum number of hours allowed since client has checked for new security updates: 72

By default, clients can receive security updates from Microsoft update. If additional sources are required for deployment, select one or both of the following sources.

□ Windows server update services

□ Windows updates

Remediation

□ Probation time: 2011-05-17 15:19:30

(Clients will be allowed network access till above specified time even if they are fo...

□ URL for remediation server:

☑ Auto remediate

2.3.7 Access Policies

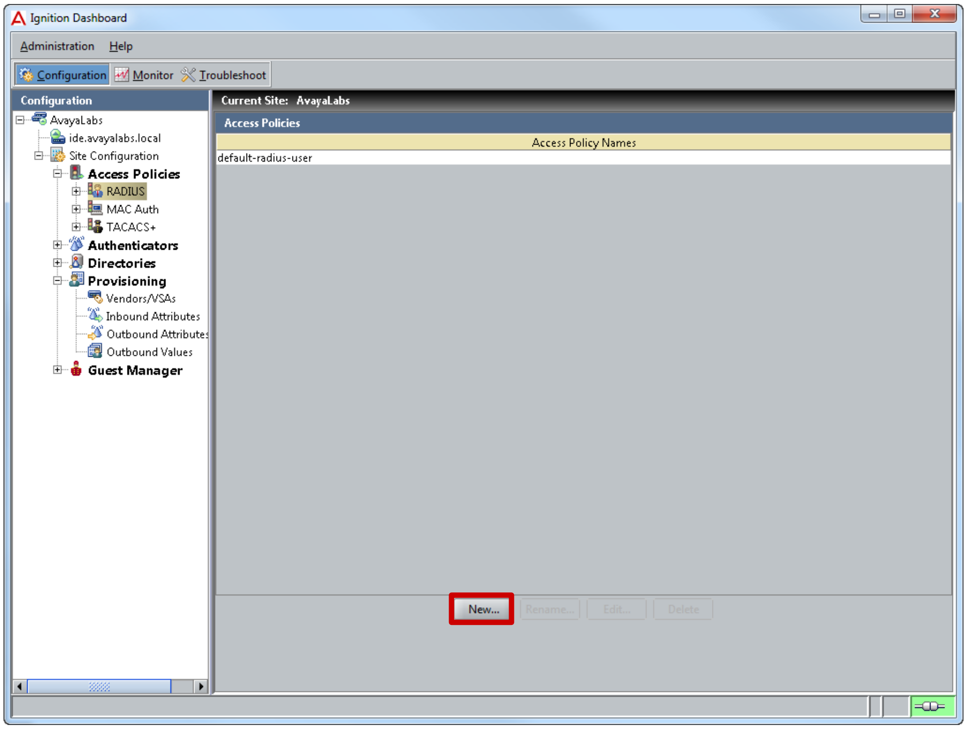
Access Policies contain a set of Authorization Rules that govern user authentication, defines supported EAP types and the search order for user lookups. Access Policies control if a user will be permitted access to the network as well as how the authentication transaction is to be performed.

2.3.7.1 Configuration Steps

For this configuration step an Access Policy named ***EAP Users*** will be created with the following parameters defined:

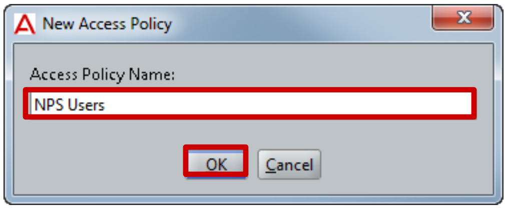
1) ***PEAP*** authentication support will be enabled using ***EAP-MSCHAPv2***.
2) The signed server certificate named ***ide.avayalabs.local*** will be used for TLS.
3) The ***Directory Set*** name ***Active Directory*** will be used for user authentication.

1 Within *Ignition Dashboard* select *Configuration* > *Access Policies* > *RADIUS*. Click *New*:



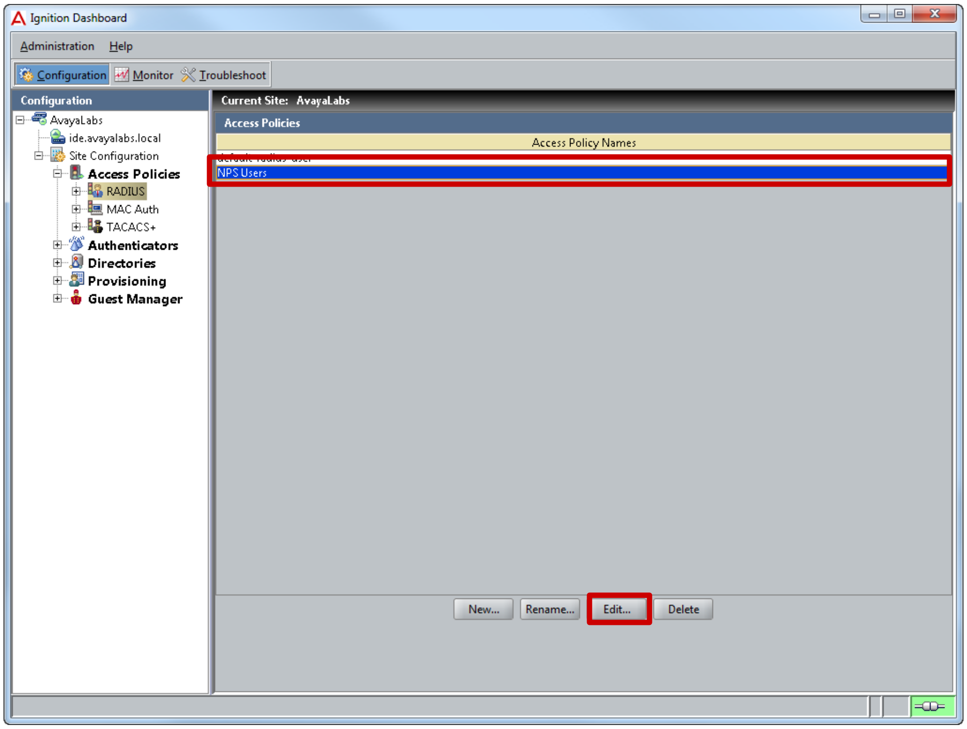
Access Policy Names
default-radius-user

2 Enter the name *NPS Users* then click *OK*:



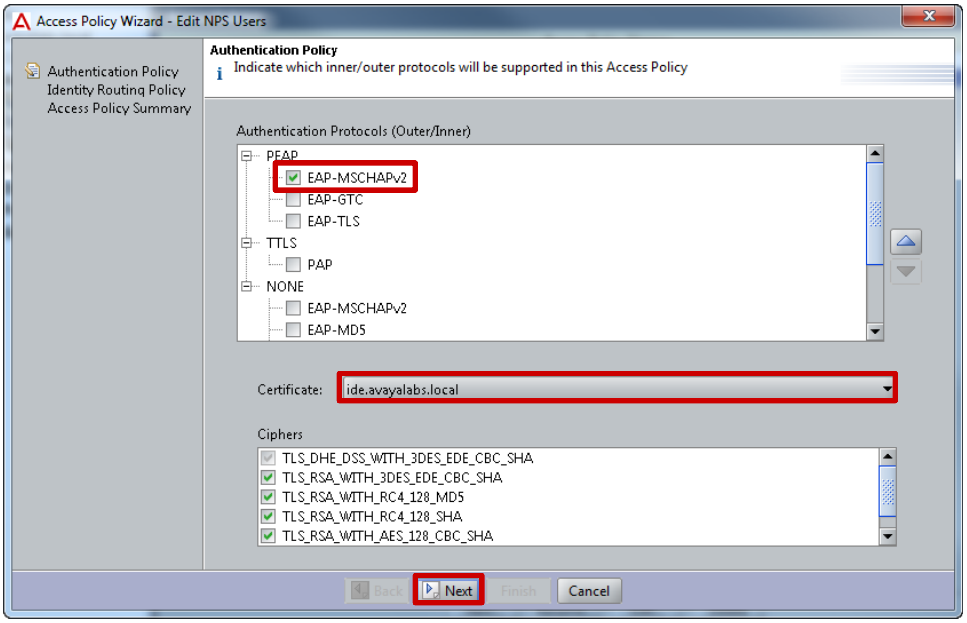
Access Policy Name: NPS Users

3 Highlight the *Access Policy* then click *Edit*:



Access Policy Names:
- default-radius-user
- NPS Users

4 Enable the *PEAP* type *EAP-MSCHAPv2*. Select the signed server *Certificate* installed earlier then click *Next*:



Authentication Policy

Indicate which inner/outer protocols will be supported in this Access Policy

Authentication Protocols (Outer/Inner)

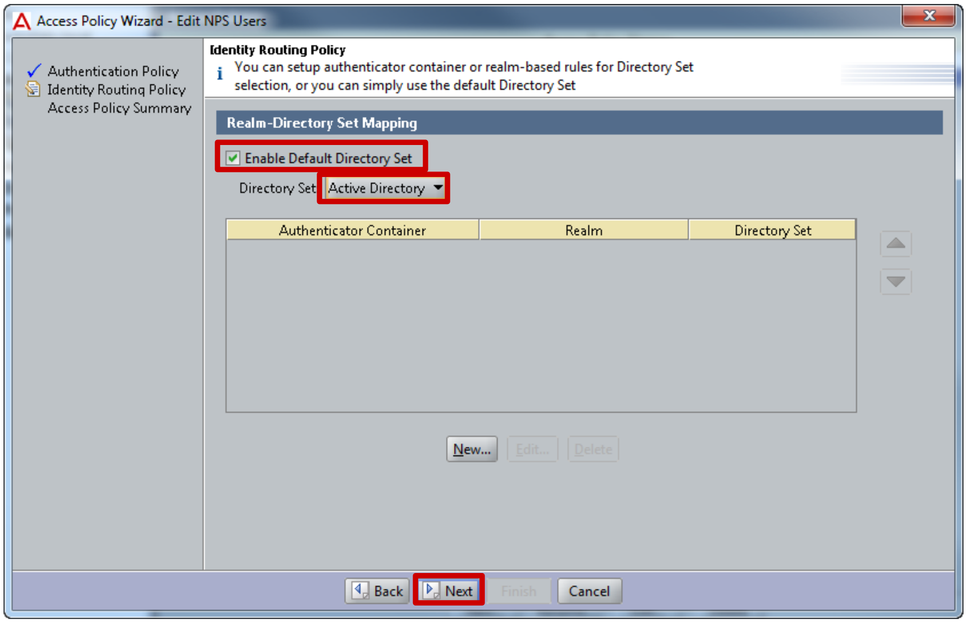
- PEAP
  - ☑ EAP-MSCHAPv2
  - □ EAP-GTC
  - □ EAP-TLS
- TTLS
  - □ PAP
- NONE
  - □ EAP-MSCHAPv2
  - □ EAP-MD5

Certificate: ide.avayalabs.local

Ciphers

- ☑ TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- ☑ TLS_RSA_WITH_3DES_EDE_CBC_SHA
- ☑ TLS_RSA_WITH_RC4_128_MD5
- ☑ TLS_RSA_WITH_RC4_128_SHA
- ☑ TLS_RSA_WITH_AES_128_CBC_SHA

5 Enable the option *Enable Default Directory Set* then select the *Directory Set* named *Active Directory*. Click *Next*:



Access Policy Wizard - Edit NPS Users

✓ Authentication Policy
Identity Routing Policy
Access Policy Summary

Identity Routing Policy

You can setup authenticator container or realm-based rules for Directory Set selection, or you can simply use the default Directory Set

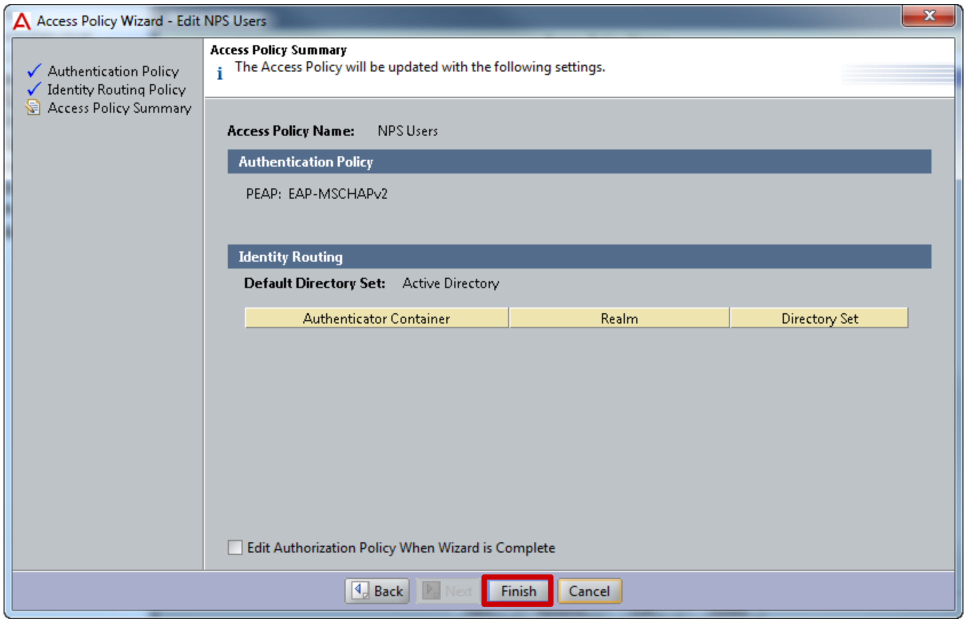
Realm-Directory Set Mapping

☑ Enable Default Directory Set

Directory Set: Active Directory

Authenticator Container	Realm	Directory Set

6 Verify the parameters then click *Finish*:



Access Policy Wizard - Edit NPS Users

✓ Authentication Policy
✓ Identity Routing Policy
Access Policy Summary

Access Policy Summary

The Access Policy will be updated with the following settings.

Access Policy Name: NPS Users

Authentication Policy

PEAP: EAP-MSCHAPv2

Identity Routing

Default Directory Set: Active Directory

Authenticator Container	Realm	Directory Set

☐ Edit Authorization Policy When Wizard is Complete

2.3.8 Authorization Policies

Access Policies contain one or more Authorization Policies that contain a set of rules that govern which computers and users are granted access to the network, restrictions that determine when computers and users can access a network as well as return attributes such as VLAN membership. The Ignition Server can also evaluate user attributes, device attributes, and the context of the access request in order to decide whether to authorize a user.

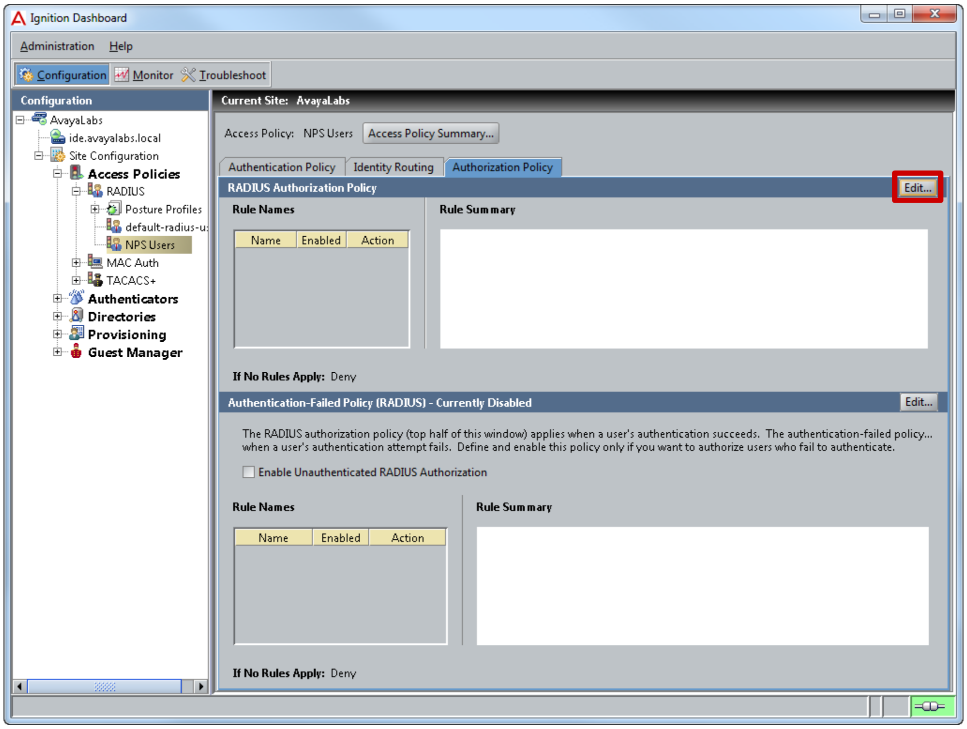
2.3.8.1 Configuration Steps

For this configuration step an ***Authorization Policy*** for ***Sales***, ***Marketing*** and ***Engineering*** users will be added to the ***Access Policy*** named ***NAP Users***. The authorization attributes defined in this example will assign VLAN membership based on Active Directory group membership and NAP compliance state:

Rule Name: Sales	
Action	Check Posture
User Group Member (Exact Match)	Sales
NAP Compliant Outbound Value (VLAN)	Sales
NAP Non-Compliant Outbound Value (VLAN)	Remediated
Rule Name: Marketing	
Action	Check Posture
User Group Member (Exact Match)	Marketing
NAP Compliant Outbound Value (VLAN)	Marketing
NAP Non-Compliant Outbound Value (VLAN)	Remediated
Rule Name: Engineering	
Action	Check Posture
User Group Member (Exact Match)	Engineering
NAP Compliant Outbound Value (VLAN)	Engineering
NAP Non-Compliant Outbound Value (VLAN)	Remediated

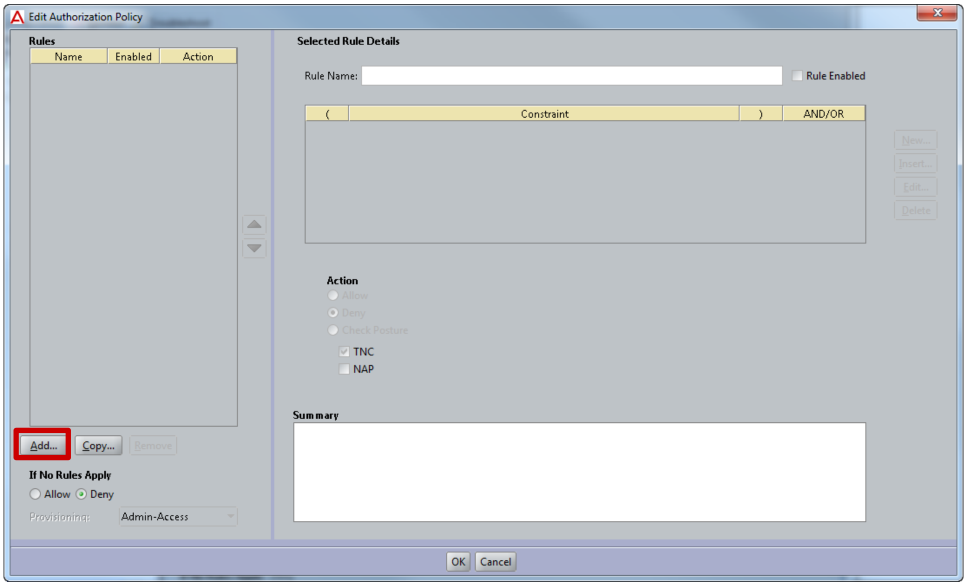
Table 2.3.8.1 – Authorization Policies

1 Within *Ignition Dashboard* select *Configuration > Access Policies > RADIUS > NPS Users*. Under *RADIUS Authorization* Policy click *Edit*:

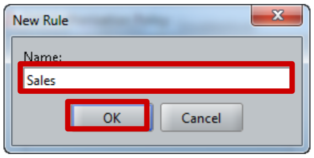


The RADIUS authorization policy (top half of this window) applies when a user's authentication succeeds. The authentication-failed policy... when a user's authentication attempt fails. Define and enable this policy only if you want to authorize users who fail to authenticate.

2 Click *Add*:

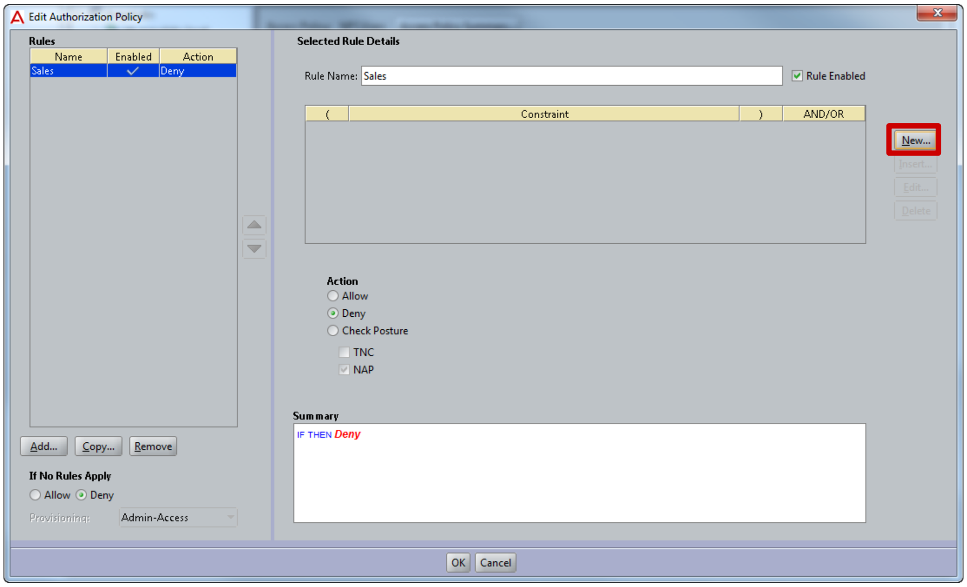


3 Enter the name *Sales* then click *OK*:


New Rule

Name: Sales

4 Click *New* to add constraints:


Edit Authorization Policy

Rules

Name	Enabled	Action
Sales	✓	Deny

Selected Rule Details

Rule Name: Sales ☑ Rule Enabled

(	Constraint	)	AND/OR

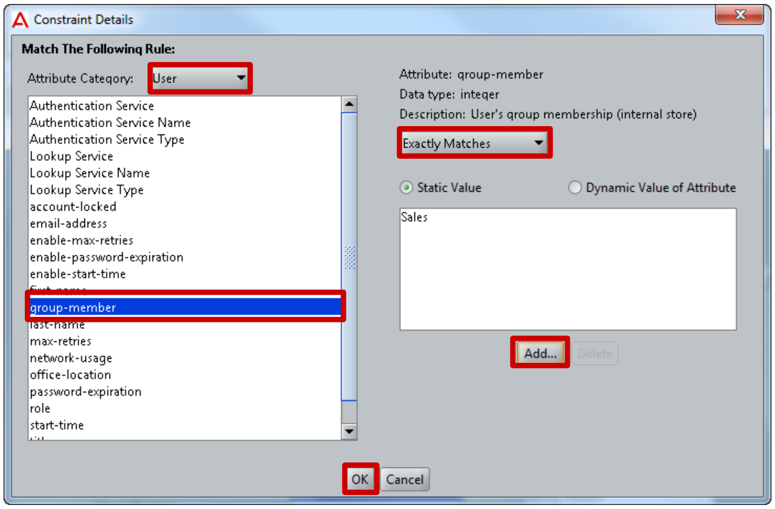
Action
○ Allow
● Deny
○ Check Posture
□ TNC
☑ NAP

Summary
IF THEN *Deny*

If No Rules Apply
○ Allow ● Deny

Provisioning: Admin-Access

5 Select the *Attribute Category* type *User* then the *Attribute* named *group-member*. Select the condition type *Exactly Matches*. Click *Add* then select the *Virtual Group* named *Sales*. Click *OK* then *OK*:


Constraint Details

Match The Following Rule:

Attribute Category: User

Authentication Service
Authentication Service Name
Authentication Service Type
Lookup Service
Lookup Service Name
Lookup Service Type
account-locked
email-address
enable-max-retries
enable-password-expiration
enable-start-time
first-name
group-member
last-name
max-retries
network-usage
office-location
password-expiration
role
start-time

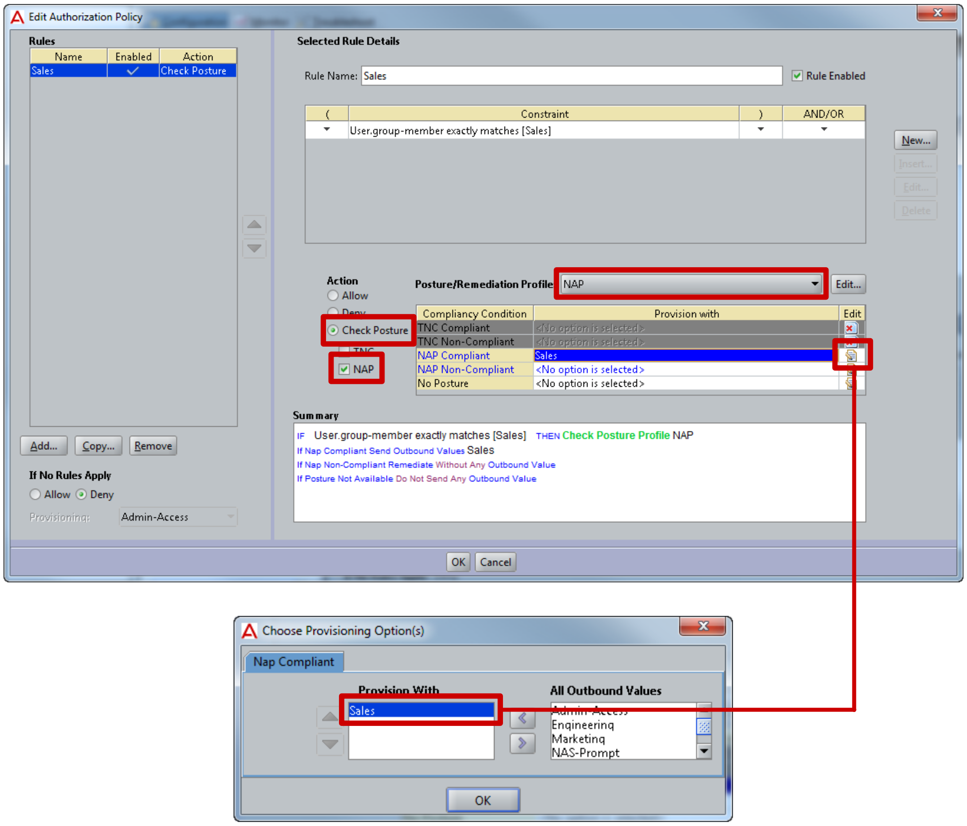
Attribute: group-member
Data type: integer
Description: User's group membership (internal store)

Exactly Matches

● Static Value ○ Dynamic Value of Attribute

Sales

6 Check the option type *Check Posture* and enable the *Check Posture* option *NAP* and disable the *Check Posture* option *TNC*. Assign the *Posture/Remediation Profile* named *NAP*. Edit the *NAP Compliant* provisioning option and assign the *Outbound Value* called *Sales*:



Edit Authorization Policy

Rules

Name	Enabled	Action
Sales	✓	Check Posture

Selected Rule Details

Rule Name: Sales ☑ Rule Enabled

(	Constraint	)	AND/OR
	User.group-member exactly matches [Sales]		

Action
○ Allow
○ Deny
● Check Posture
□ TNC
☑ NAP

Posture/Remediation Profile: NAP

Compliancy Condition	Provision with	Edit
TNC Compliant	<No option is selected>	
TNC Non-Compliant	<No option is selected>	
NAP Compliant	Sales	
NAP Non-Compliant	<No option is selected>	
No Posture	<No option is selected>	

Summary

IF User.group-member exactly matches [Sales] THEN Check Posture Profile NAP
If Nap Compliant Send Outbound Values Sales
If Nap Non-Compliant Remediate Without Any Outbound Value
If Posture Not Available Do Not Send Any Outbound Value

If No Rules Apply
○ Allow ● Deny

Provisioning: Admin-Access

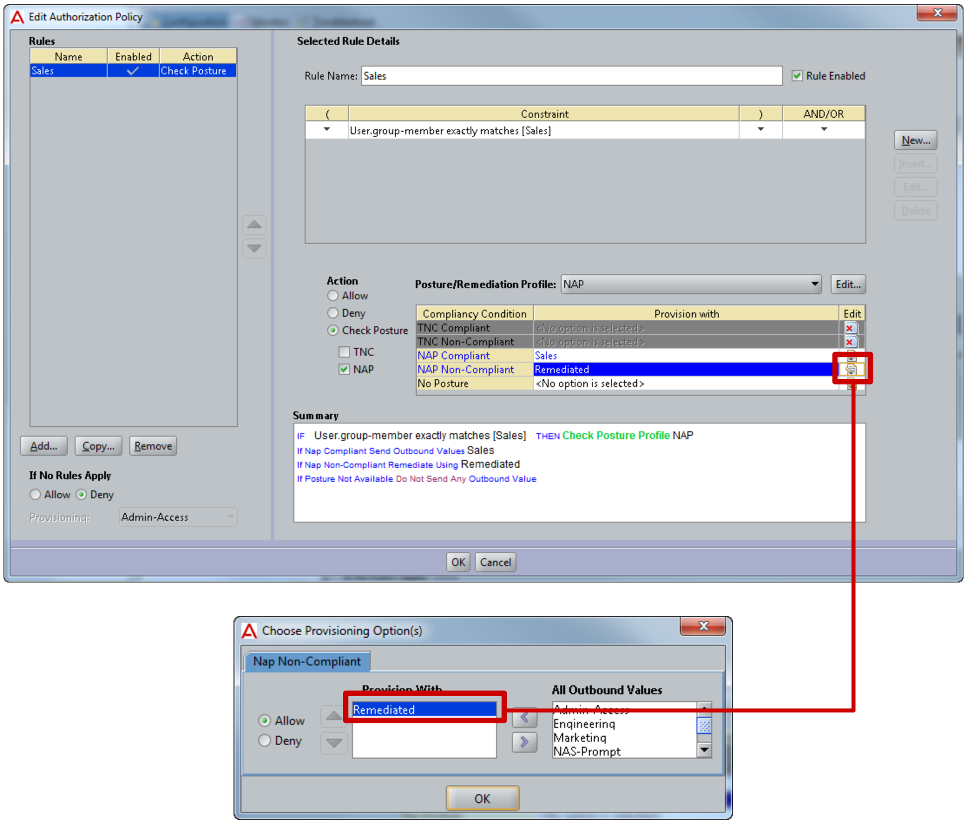
Choose Provisioning Option(s)

Nap Compliant

Provision With: Sales

All Outbound Values:
Admin-Access
Engineering
Marketing
NAS-Prompt

7 Edit the *NAP Non-Compliant* provisioning option and assign the *Outbound Value* called *Remediated*:



Edit Authorization Policy

Rules

Name	Enabled	Action
Sales	✓	Check Posture

Selected Rule Details

Rule Name: Sales ☑ Rule Enabled

(	Constraint	)	AND/OR
	User.group-member exactly matches [Sales]		

Action

○ Allow

○ Deny

● Check Posture

□ TNC

☑ NAP

Posture/Remediation Profile: NAP

Compliancy Condition	Provision with	Edit
TNC Compliant	<No option is selected>	
TNC Non-Compliant	<No option is selected>	
NAP Compliant	Sales	
NAP Non-Compliant	Remediated	
No Posture	<No option is selected>	

Summary

IF User.group-member exactly matches [Sales] THEN Check Posture Profile NAP

If Nap Compliant Send Outbound Values Sales

If Nap Non-Compliant Remediate Using Remediated

If Posture Not Available Do Not Send Any Outbound Value

If No Rules Apply

○ Allow ● Deny

Provisioning: Admin-Access

Choose Provisioning Option(s)

Nap Non-Compliant

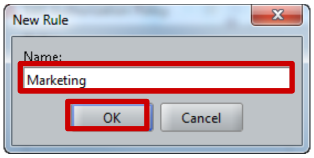
● Allow

○ Deny

Provision With: Remediated

All Outbound Values: Admin-Access, Engineering, Marketing, NAS-Prompt

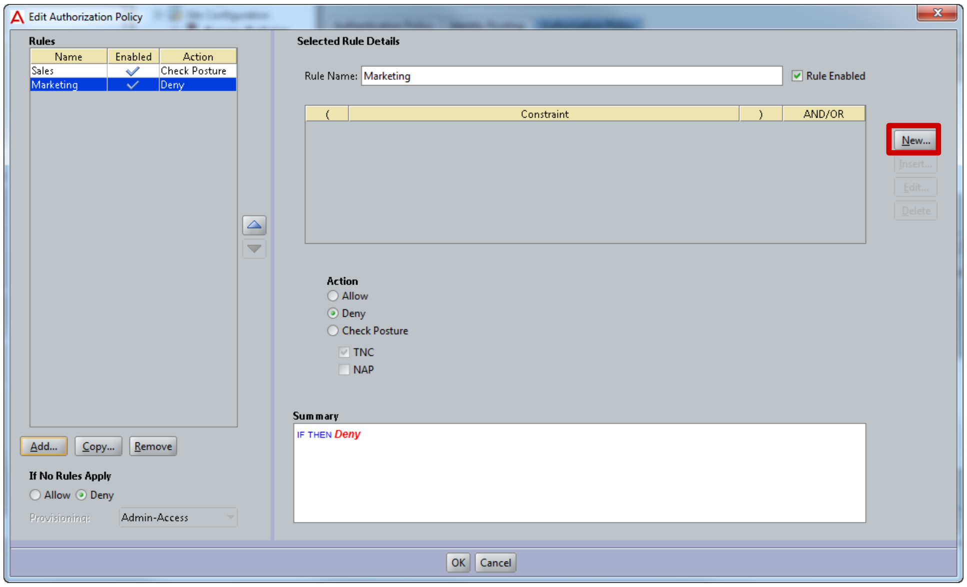
8 Click *Add* to create a new rule. Enter the name *Marketing* then click *OK*:



New Rule

Name: Marketing

9 Click *New* to add constraints:



Edit Authorization Policy

Rules

Name	Enabled	Action
Sales	✓	Check Posture
Marketing	✓	Deny

Selected Rule Details

Rule Name: Marketing ☑ Rule Enabled

(	Constraint	)	AND/OR

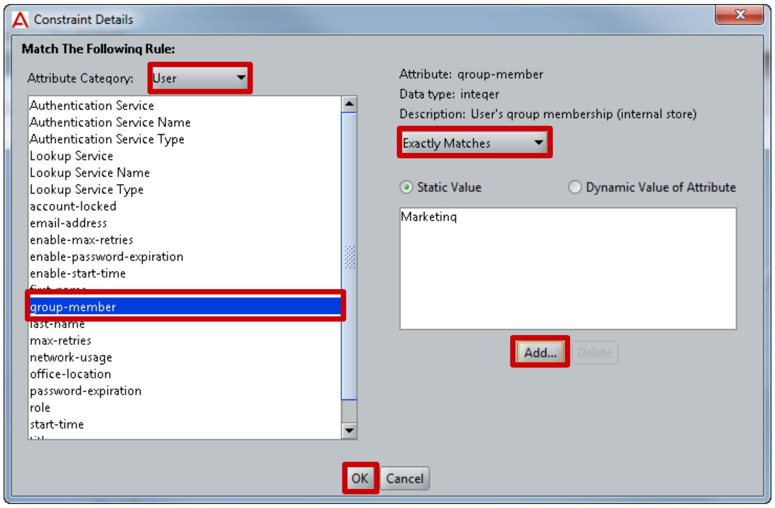
Action
○ Allow
● Deny
○ Check Posture
☑ TNC
□ NAP

Summary
IF THEN *Deny*

If No Rules Apply
○ Allow ● Deny

Provisioning: Admin-Access

10 Select the *Attribute Category* type *User* then the *Attribute* named *group-member*. Select the condition type *Exactly Matches*. Click *Add* then select the *Virtual Group* named *Marketing*. Click *OK* then *OK*:



Constraint Details

Match The Following Rule:

Attribute Category: User

Authentication Service
Authentication Service Name
Authentication Service Type
Lookup Service
Lookup Service Name
Lookup Service Type
account-locked
email-address
enable-max-retries
enable-password-expiration
enable-start-time
first-name
group-member
last-name
max-retries
network-usage
office-location
password-expiration
role
start-time
title

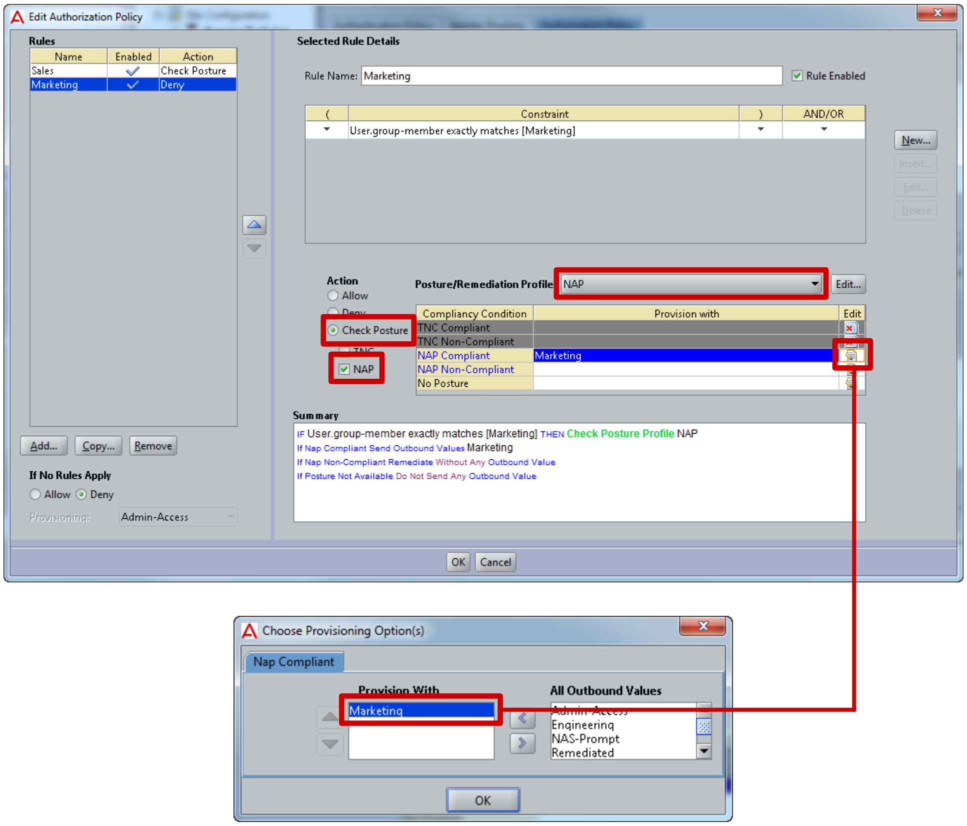
Attribute: group-member
Data type: integer
Description: User's group membership (internal store)

Exactly Matches

● Static Value ○ Dynamic Value of Attribute

Marketing

11 **Check the option type *Check Posture* and enable the *Check Posture* option *NAP* and disable the *Check Posture* option *TNC*. Assign the *Posture/Remediation Profile* named *NAP*. Edit the *NAP Compliant* provisioning option and assign the *Outbound Value* called *Marketing*:**


Edit Authorization Policy
Rules
Add... Copy... Remove
New... Insert... Edit... Delete
OK Cancel
Choose Provisioning Option(s)
Nap Compliant
OK

Name	Enabled	Action
Sales	✓	Check Posture
Marketing	✓	Deny

If No Rules Apply: ○ Allow ● Deny

Provisioning: Admin-Access

Selected Rule Details

Rule Name: Marketing ☑ Rule Enabled

(	Constraint	)	AND/OR
	User.group-member exactly matches [Marketing]		

Action: ○ Allow ○ Deny ● Check Posture ☐ TNC ☑ NAP

Posture/Remediation Profile: NAP

Compliancy Condition	Provision with	Edit
TNC Compliant		
TNC Non-Compliant		
NAP Compliant	Marketing	
NAP Non-Compliant		
No Posture		

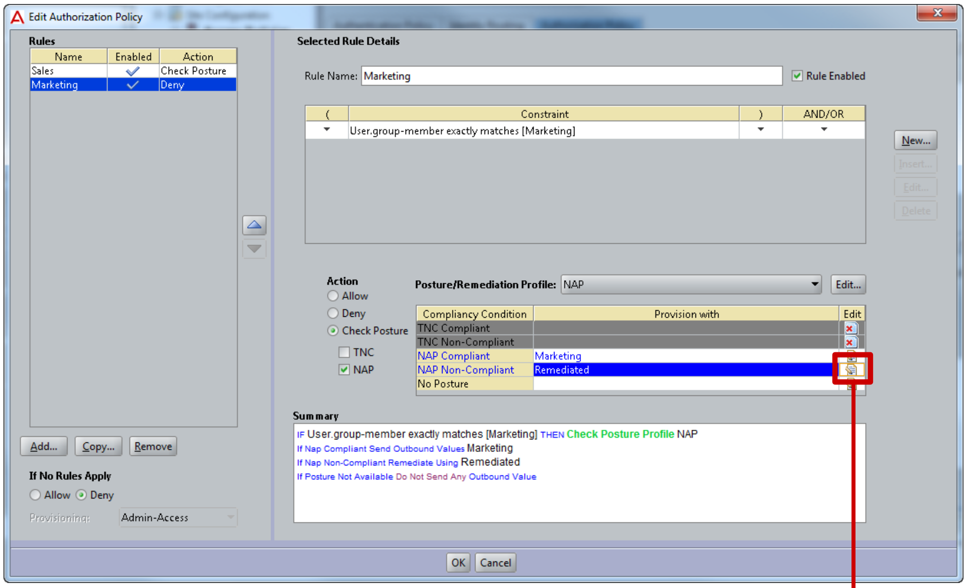
Summary

IF User.group-member exactly matches [Marketing] THEN Check Posture Profile NAP
If Nap Compliant Send Outbound Values Marketing
If Nap Non-Compliant Remediate Without Any Outbound Value
If Posture Not Available Do Not Send Any Outbound Value

Provision With: Marketing

All Outbound Values: Admin-Access, Engineering, NAS-Prompt, Remediated

12 Edit the *NAP Non-Compliant* provisioning option and assign the *Outbound Value* called *Remediated*. Click *OK*:



Edit Authorization Policy

Rules

Name	Enabled	Action
Sales	✓	Check Posture
Marketing	✓	Deny

Selected Rule Details

Rule Name: Marketing ☑ Rule Enabled

(	Constraint	)	AND/OR
	User.group-member exactly matches [Marketing]		

Action
○ Allow
○ Deny
● Check Posture
□ TNC
☑ NAP

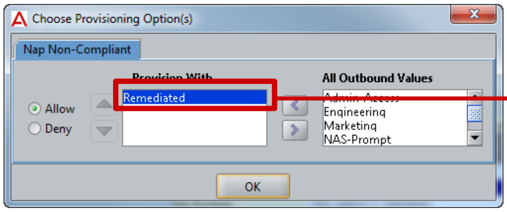
Posture/Remediation Profile: NAP

Compliancy Condition	Provision with	Edit
TNC Compliant		
TNC Non-Compliant		
NAP Compliant	Marketing	
NAP Non-Compliant	Remediated	
No Posture		

Summary

IF User.group-member exactly matches [Marketing] THEN Check Posture Profile NAP
If Nap Compliant Send Outbound Values Marketing
If Nap Non-Compliant Remediate Using Remediated
If Posture Not Available Do Not Send Any Outbound Value

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



Choose Provisioning Option(s)

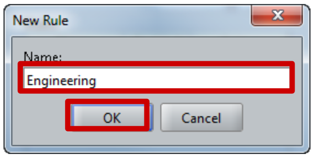
Nap Non-Compliant

● Allow
○ Deny

Provision With: Remediated

All Outbound Values: Admin-Access, Engineering, Marketing, NAS-Prompt

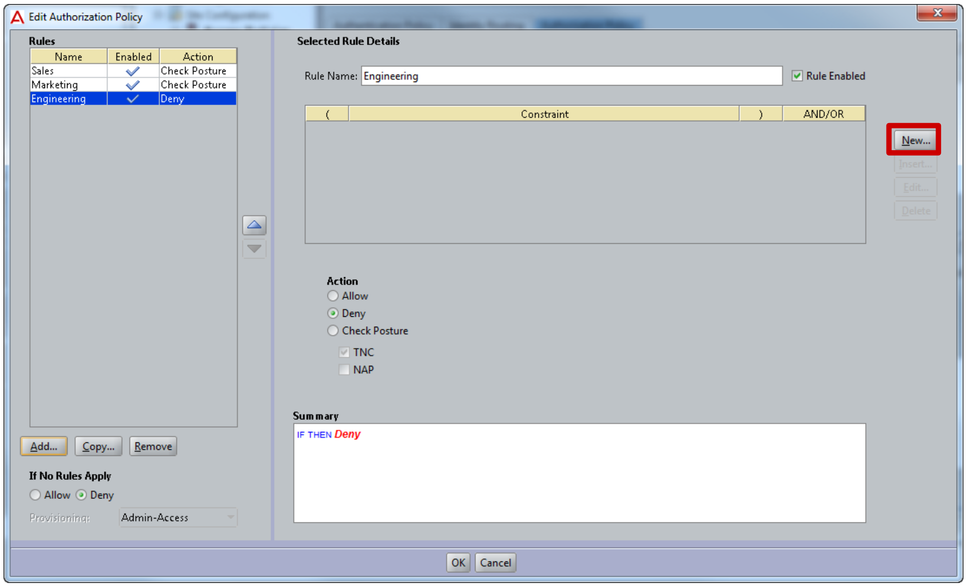
13 Click *Add* to create a new rule. Enter the name *Engineering* then click *OK*:



New Rule

Name: Engineering

14 Click *New* to add constraints:



Edit Authorization Policy

Rules

Name	Enabled	Action
Sales	✓	Check Posture
Marketing	✓	Check Posture
Engineering	✓	Deny

Selected Rule Details

Rule Name: Engineering ☑ Rule Enabled

(	Constraint	)	AND/OR

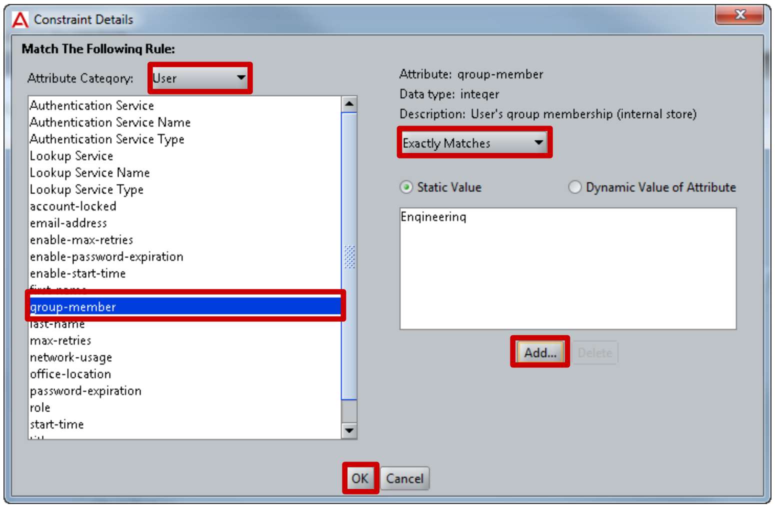
Action
○ Allow
● Deny
○ Check Posture
☑ TNC
□ NAP

Summary
IF THEN *Deny*

If No Rules Apply
○ Allow ● Deny

Provisioning: Admin-Access

15 Select the *Attribute Category* type *User* then the *Attribute* named *group-member*. Select the condition type *Exactly Matches*. Click *Add* then select the *Virtual Group* named *Engineering*. Click *OK* then *OK*:



Constraint Details

Match The Following Rule:

Attribute Category: User

- Authentication Service
- Authentication Service Name
- Authentication Service Type
- Lookup Service
- Lookup Service Name
- Lookup Service Type
- account-locked
- email-address
- enable-max-retries
- enable-password-expiration
- enable-start-time
- first-name
- group-member
- last-name
- max-retries
- network-usage
- office-location
- password-expiration
- role
- start-time

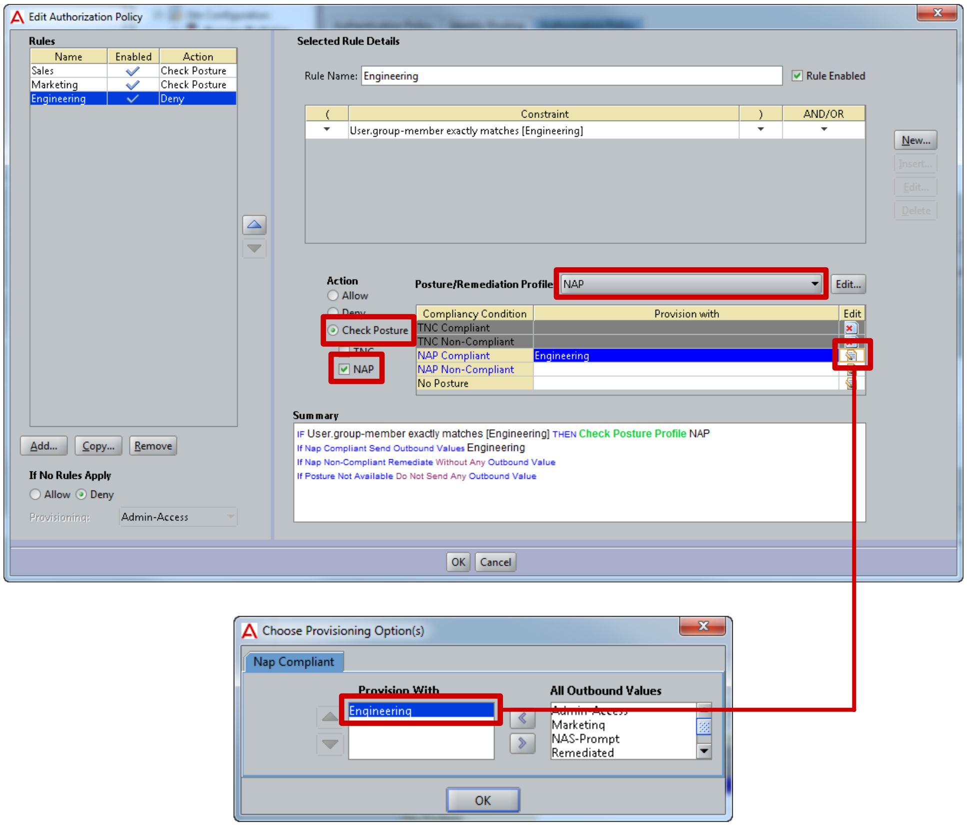
Attribute: group-member
Data type: integer
Description: User's group membership (internal store)

Exactly Matches

● Static Value ○ Dynamic Value of Attribute

Engineering

16 Check the option type *Check Posture* and enable the *Check Posture* option *NAP* and disable the *Check Posture* option *TNC*. Assign the *Posture/Remediation Profile* named *NAP*. Edit the *NAP Compliant* provisioning option and assign the *Outbound Value* called *Engineering*:



Edit Authorization Policy

Rules

Name	Enabled	Action
Sales	✓	Check Posture
Marketing	✓	Check Posture
Engineering	✓	Deny

If No Rules Apply

○ Allow ● Deny

Provisioning: Admin-Access

Selected Rule Details

Rule Name: Engineering ☑ Rule Enabled

(	Constraint	)	AND/OR
	User.group-member exactly matches [Engineering]		

Action

○ Allow
○ Deny
● Check Posture
□ TNC
☑ NAP

Posture/Remediation Profile: NAP

Compliancy Condition	Provision with	Edit
TNC Compliant		
TNC Non-Compliant		
NAP Compliant	Engineering	
NAP Non-Compliant		
No Posture		

Summary

IF User.group-member exactly matches [Engineering] THEN Check Posture Profile NAP
If Nap Compliant Send Outbound Values Engineering
If Nap Non-Compliant Remediate Without Any Outbound Value
If Posture Not Available Do Not Send Any Outbound Value

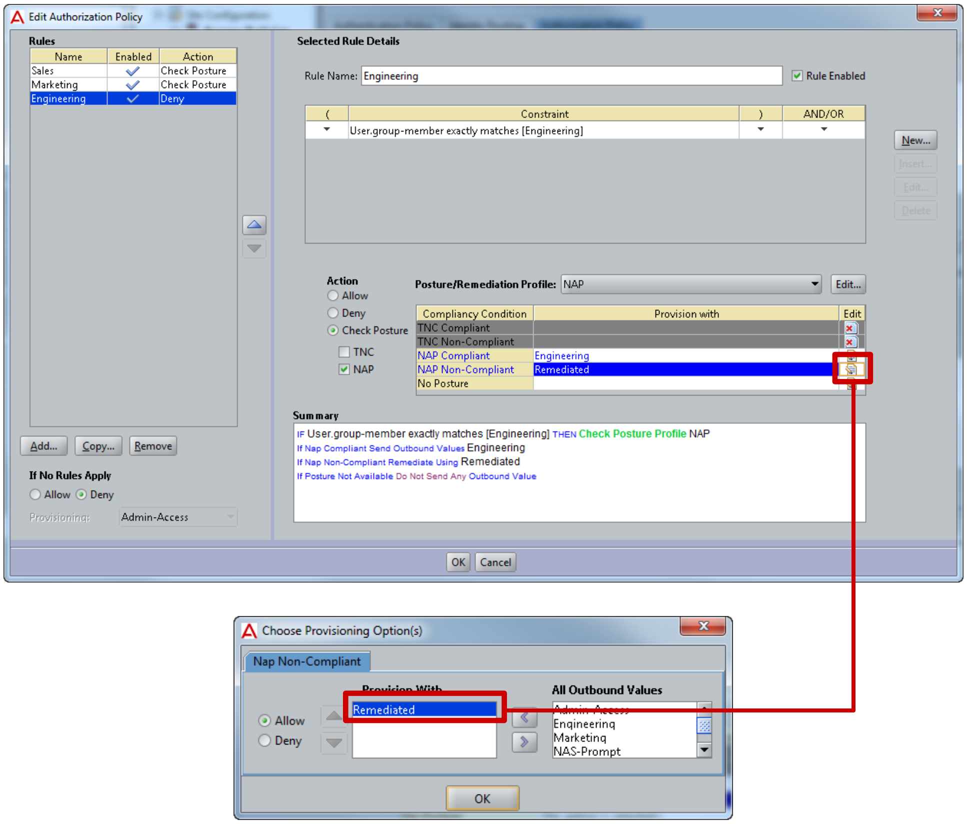
Choose Provisioning Option(s)

Nap Compliant

Provision With: Engineering

All Outbound Values: Admin-Access, Marketing, NAS-Prompt, Remediated

17 Edit the *NAP Non-Compliant* provisioning option and assign the *Outbound Value* called *Remediated*. Click *OK* then *OK*:



Edit Authorization Policy

Rules

Name	Enabled	Action
Sales	✓	Check Posture
Marketing	✓	Check Posture
Engineering	✓	Deny

If No Rules Apply

○ Allow ● Deny

Provisioning: Admin-Access

Selected Rule Details

Rule Name: Engineering ☑ Rule Enabled

(	Constraint	)	AND/OR
	User.group-member exactly matches [Engineering]		

Action

○ Allow

○ Deny

● Check Posture

□ TNC

☑ NAP

Posture/Remediation Profile: NAP

Compliancy Condition	Provision with	Edit
TNC Compliant		
TNC Non-Compliant		
NAP Compliant	Engineering	
NAP Non-Compliant	Remediated	
No Posture		

Summary

IF User.group-member exactly matches [Engineering] THEN Check Posture Profile NAP
If Nap Compliant Send Outbound Values Engineering
If Nap Non-Compliant Remediate Using Remediated
If Posture Not Available Do Not Send Any Outbound Value

Choose Provisioning Option(s)

Nap Non-Compliant

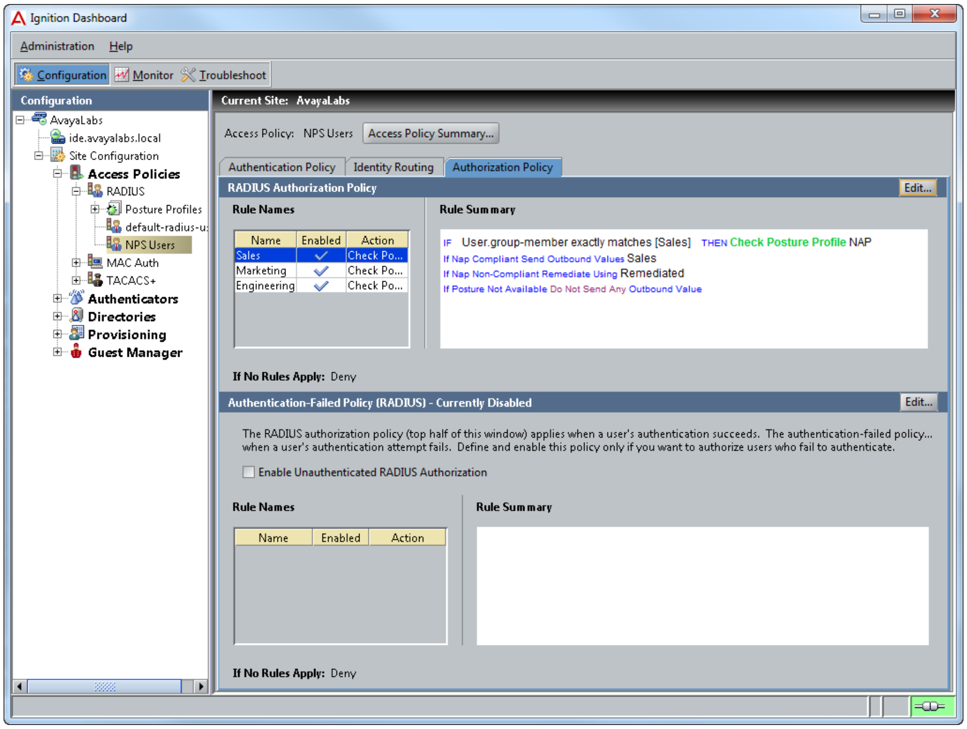
● Allow

○ Deny

Provision With: Remediated

All Outbound Values:
Admin-Access
Engineering
Marketing
NAS-Prompt

18 Authorization rules for *Sales*, *Marketing* and *Engineering* users have now been added to the Access Policy:



Current Site: AvayaLabs

Access Policy: NPS Users

RADIUS Authorization Policy

Rule Names

Name	Enabled	Action
Sales	✓	Check Po...
Marketing	✓	Check Po...
Engineering	✓	Check Po...

Rule Summary

IF User.group-member exactly matches [Sales] THEN Check Posture Profile NAP
If Nap Compliant Send Outbound Values Sales
If Nap Non-Compliant Remediate Using Remediated
If Posture Not Available Do Not Send Any Outbound Value

If No Rules Apply: Deny

Authentication-Failed Policy (RADIUS) - Currently Disabled

The RADIUS authorization policy (top half of this window) applies when a user's authentication succeeds. The authentication-failed policy... when a user's authentication attempt fails. Define and enable this policy only if you want to authorize users who fail to authenticate.

☐ Enable Unauthenticated RADIUS Authorization

Rule Names

Name	Enabled	Action

Rule Summary

If No Rules Apply: Deny

2.3.9 Authenticators

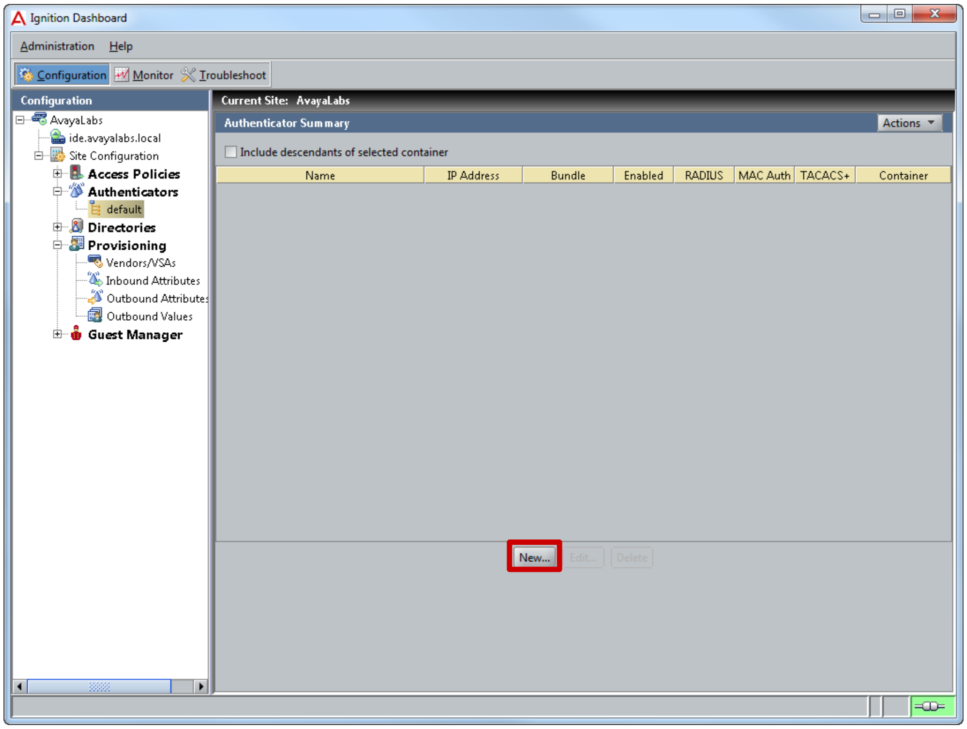
Avaya Ethernet Routing Switches and Wireless LAN 8180 Wireless Controllers that forward RADIUS authentication requests to the Ignition Server are called Authenticators. Each Avaya Ethernet Routing Switch or Wireless LAN 8180 Wireless Controller that uses the Ignition Server to authenticate PEAP users and computers must be defined as an authenticator. One entry can be created for each Authenticator or alternatively for larger deployments a bundle can be created which allows one Authenticator entry to service multiple Authenticators.

Each Authenticator entry includes a friendly name, IP address, RADIUS shared secret, authenticator type, Access Policy association and vendor information which defines the check and return attributes and VLAN format the device supports.

2.3.9.1 Configuration Steps

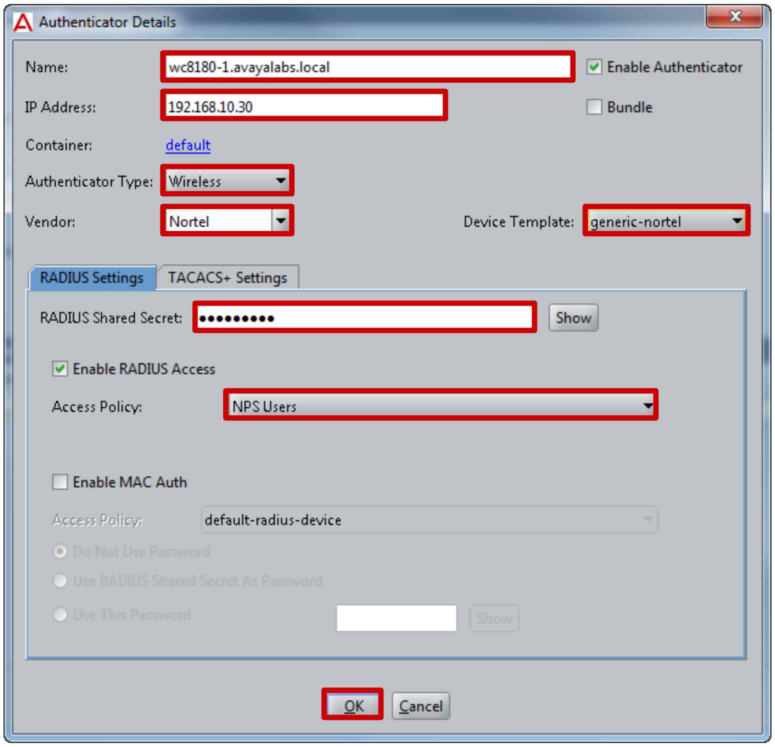
For this configuration an Authenticator entry will be defined for a stack of Ethernet Routing Switch 4500s and a Wireless LAN 8180 Controller:

1 Within *Ignition Dashboard* select *Configuration* > *Authenticators* > *default*. Click *New*:



2 Enter the required parameters for the Wireless LAN 8180 Controller (example below) then click *OK*:

Name	Set to the ***hostname*** of the Wireless LAN 8180 Controller.
IP Address	Set to the ***Wireless System Interface*** IP Address on the Wireless LAN 8180 Controller.
Authenticator Type	Set to ***Wireless***.
Vendor	Set to ***Nortel***.
Device Template	Set to ***generic-nortel*** which forwards the VLAN information as a Name.
RADIUS Shared Secret	Set to ***avayalabs*** which matches the shared secret defined on the Wireless LAN 8180 Controller.
Access Policy	Set to ***NAP Users***.



Authenticator Details

Name: wc8180-1.avayalabs.local

☑ Enable Authenticator

IP Address: 192.168.10.30

□ Bundle

Container: default

Authenticator Type: Wireless

Vendor: Nortel

Device Template: generic-nortel

RADIUS Shared Secret: ●●●●●●●●●

☑ Enable RADIUS Access

Access Policy: NPS Users

□ Enable MAC Auth

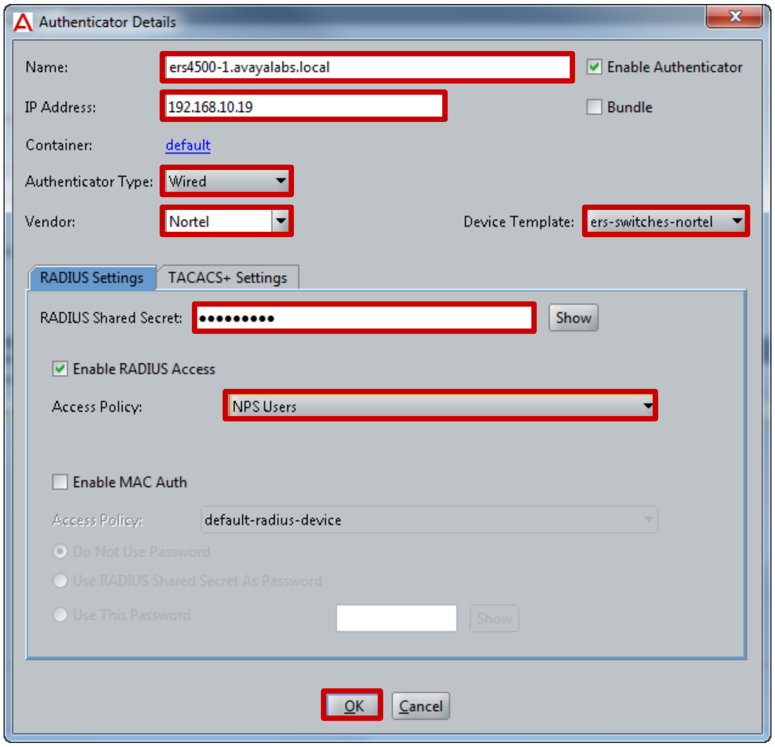
Access Policy: default-radius-device

● Do Not Use Password

○ Use RADIUS Shared Secret As Password

○ Use This Password

3	Click New to define an additional Authenticator. Enter the required parameters for the Ethernet Routing Switch 4500 (example below) then click *OK*:
Name	Set to the ***hostname*** of the Ethernet Routing Switch 4500 or Stack.
IP Address	Set to the ***management*** IP Address assigned to the Ethernet Routing Switch 4500 or Stack.
Authenticator Type	Set to ***Wired***.
Vendor	Set to ***Nortel***.
Device Template	Set to ***ers-switches-nortel*** which forwards the VLAN information as an ID.
RADIUS Shared Secret	Set to ***avayalabs*** which matches the shared secret defined on the Ethernet Routing Switch 4500 or Stack.
Access Policy	Set to ***NAP Users***.


Authenticator Details

Name: ers4500-1.avayalabs.local ☑ Enable Authenticator

IP Address: 192.168.10.19 □ Bundle

Container: default

Authenticator Type: Wired

Vendor: Nortel

Device Template: ers-switches-nortel

RADIUS Settings | TACACS+ Settings

RADIUS Shared Secret: ••••••••• Show

☑ Enable RADIUS Access

Access Policy: NPS Users

□ Enable MAC Auth

Access Policy: default-radius-device

● Do Not Use Password

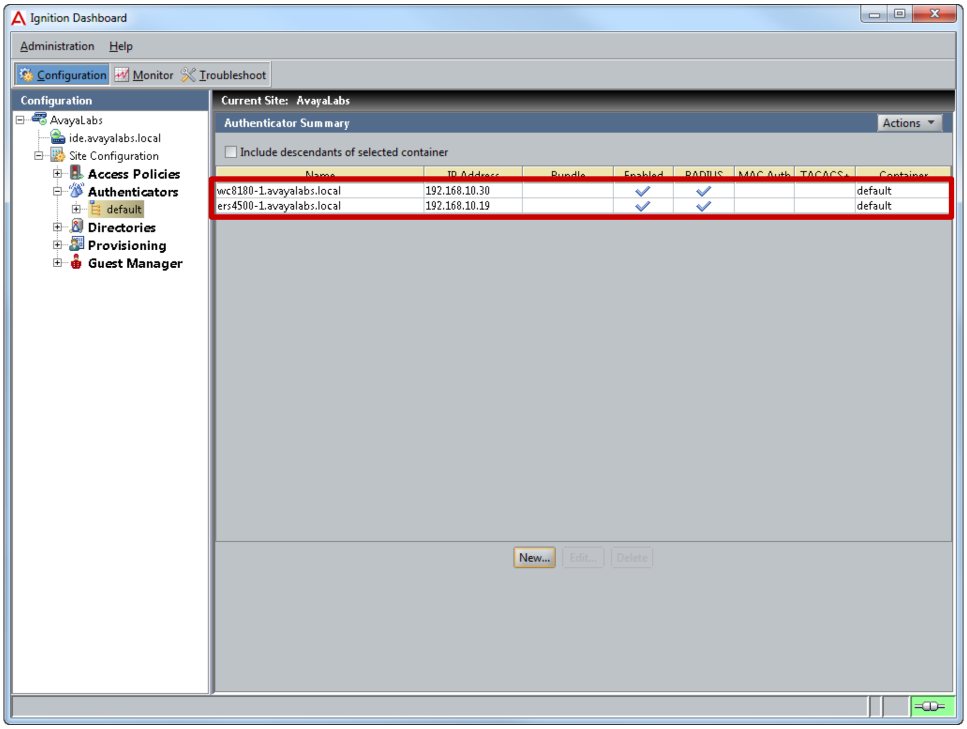
○ Use RADIUS Shared Secret As Password

○ Use This Password Show

OK Cancel

Note – When adding a stack of switches as an Authenticator, you must define the stack IP address and not the switch IP address.

4 The Wireless LAN 8180 Wireless Controller and Avaya Ethernet Routing Switch 4500 have now been added as Authenticators to the Ignition Server:



□ Include descendants of selected container

Name	IP Address	Bundle	Enabled	RADIUS	MAC Auth	TACACS+	Container
wc8180-1.avayalabs.local	192.168.10.30		✓	✓			default
ers4500-1.avayalabs.local	192.168.10.19		✓	✓			default

2.4 Avaya Wireless LAN 8100

The following section outlines the configuration steps required to configure the Avaya WC8180 wireless controller to provide secure 802.1X authenticated access to wireless PEAP users and computers with dynamic VLAN assignments using the Ignition Server for RADIUS services:

2.4.1 Base Configuration

The Avaya 8100 series Wireless Controller requires basic network configuration before it can provide wireless services to users. The Wireless Controller will be configured with the necessary management and user VLANs as well as the virtual IP addresses required for management and Access Point communications. In addition wireless services need to be configured and enabled so that the Avaya 8100 series Wireless Controller can manage Avaya 8100 series Access Points and serve Wireless LANs.

2.4.1.1 Configuration Steps

For this configuration step a factory defaulted WC8180 Wireless Controller will be configured with the following basic parameters:

1. ***Management*** VLAN ID ***10***, ***Sales*** VLAN ID ***11***, ***Marketing*** VLAN ID ***12***, ***Engineering*** VLAN ID ***13*** and ***Remediated*** VLAN ID ***14*** will be created:
    a. VLAN ***10*** will be assigned the IP address ***192.168.10.30/24*** and will be assigned to uplink port ***26***.
    b. IP routing will be ***enabled***.
2. A static default route will be defined pointing to the ***192.168.10.1*** IP address assigned to the private internal interface on the firewall.
3. A valid license file will be uploaded.
4. Wireless services will be enabled:
    a. The ***Interface-ip address*** will be set to the management IP address ***192.168.10.30***.
    b. The WC8180 will be configured as ***MDC capable*** with the password ***AvayaLabs12!@*** assigned.
    c. The WC8180 will join the wireless domain named ***AVAYALABS***.
    d. The wireless domain will be configured with the country code ***US***.
    e. The wireless domain will be configured to automatically ***promote-discovered-aps***.
    f. Mobility VLANs named ***Sales***, ***Marketing, Engineering*** and ***Computers*** will be created and mapped to their respective VLAN IDs.

1 Using the *AACLI* access the *global* configuration context:

```
WC8180# configure terminal

WC8180(config)#
```

2 Create VLANs 10-14 and assign port membership:

```
WC8180(config)# vlan create 10 name Mgmt type port
WC8180(config)# vlan create 11 name Sales type port
WC8180(config)# vlan create 12 name Marketing type port
WC8180(config)# vlan create 13 name Engineering type port
WC8180(config)# vlan create 14 name Remediated type port
WC8180(config)# vlan members remove 1 1-26
WC8180(config)# vlan members add 10-14 26
WC8180(config)# vlan mgmt 10
WC8180(config)# show vlan

Id  Name                 Type      Protocol         User PID  Active IVL/SVL  Mgmt
--- -------------------- --------- ---------------- --------- ------ -------- ----
1   VLAN #1              Port      None             0x0000    Yes    IVL      No
        Port Members: NONE
10  Mgmt                 Port      None             0x0000    Yes    IVL      Yes
        Port Members: 26
11  Sales                Port      None             0x0000    Yes    IVL      No
        Port Members: 26
12  Marketing            Port      None             0x0000    Yes    IVL      No
        Port Members: 26
13  Engineering          Port      None             0x0000    Yes    IVL      No
        Port Members: 26
14  Remediated           Port      None             0x0000    Yes    IVL      No
        Port Members: 26
Total VLANs: 6
```

3 Assign virtual IP addresses to VLAN *10* and mark VLAN *10* for *management*:

```
WC8180(config)# interface vlan 10
WC8180(config-if)# ip address 192.168.10.30 255.255.255.0
WC8180(config-if)# exit
WC8180(config)# show vlan ip

==============================================================================
Vid  ifIndex Address         Mask            MacAddress        Offset Routing
==============================================================================
Primary Interfaces
------------------------------------------------------------------------------
10   10010   192.168.10.30   255.255.255.0   00:1B:4F:CA:19:80 1      Enabled
------------------------------------------------------------------------------
% Total of Primary Interfaces: 1
```

4 Globally enable *IP Routing*:

```
WC8180(config)# ip routing
WC8180(config)# show ip routing

IP Routing is enabled
IP ARP life time is 21600 seconds
```

5 Define a static *Default Route* that points to the core router on VLAN *10*:

```
WC8180(config)# ip route 0.0.0.0 0.0.0.0 192.168.10.1 1
WC8180(config)# show ip route

===============================================================================
                                        Ip Route
===============================================================================
DST             MASK            NEXT            COST    VLAN PORT PROT TYPE PRF
-------------------------------------------------------------------------------
0.0.0.0         0.0.0.0         192.168.10.1    1        14   12    S  IB     5
192.168.10.0    255.255.255.0   192.168.10.30   1        10   ----  C  DB     0
Total Routes: 2
-------------------------------------------------------------------------------
```

6 If necessary upload a license file. Once installed the WC8180 will need to be reset:

```
WC8180(config)# copy tftp license address 192.168.10.6 filename license.dat

License successfully downloaded.
NOTE:  system must be rebooted to activate license.

WC8180(config)# boot
```

7 Using the *AACLI* access the *wireless* configuration context. Set the *interface-ip* to the virtual IP Address assigned to VLAN *10* and enable wireless services:

```
WC8180> enable
WC8180# configure terminal
WC8180(config)# wireless
WC8180(config-wireless)# interface-ip 192.168.10.30
WC8180(config-wireless)# enable
WC8180(config-wireless)# show wireless

Status            : Enabled
Interface IP      : 192.168.10.30
TCP/UDP base port : 61000
```

8 Configure the WC8180 as *MDC-Capable* and define a *password*:

```
WC8180(config-wireless)# controller mdc-capable

% Domain password should be between 10-15 characters long.
% Password must contain a minimum of 2 upper, 2 lowercase letters
% 2 numbers and 2 special characters like !@#$%^&*()

Enter domain password: AvayaLabs12!@
Verify Domain password: AvayaLabs12!@
```

9 Create and join the *Wireless Domain* using the password defined in the previous step:

```
WC8180(config)# end
WC8180# wireless controller join-domain domain-name AVAYALABS mdc-address
192.168.10.30

Enter Domain Secret: AvayaLabs12!@

WC8180# show wireless controller domain-membership

Domain Name              : AVAYALABS
Domain Role              : Active MDC
Domain Action Status     : Join Success
Action Failure Reason    : None
```

10 Access the *wireless* configuration context. Create a *Mobility VLAN* for the *Sales*, *Marketing* and *Engineering* users and *Remediated*:

```
WC8180# configure terminal
WC8180(config)# wireless
WC8180(config-wireless# domain mobility-vlan Sales
WC8180(config-wireless# domain mobility-vlan Marketing
WC8180(config-wireless# domain mobility-vlan Engineering
WC8180(config-wireless# domain mobility-vlan Remediated
WC8180(config-wireless# show wireless domain mobility-vlan

  ---------------------------------------------------
  Mobility VLAN Name                 Status
  --------------------------------   -----------------
  default-MVLAN                      Active
  Sales                              Active
  Marketing                          Active
  Engineering                        Active
  Remediated                         Active
  ---------------------------------------------------
```

11 Map the *Mobility VLANs* to the *Local VLANs*:

```
WC8180(config-wireless# switch vlan-map Sales lvid 11
WC8180(config-wireless# switch vlan-map Marketing lvid 12
WC8180(config-wireless# switch vlan-map Engineering lvid 13
WC8180(config-wireless# switch vlan-map Remediated lvid 14
WC8180(config-wireless# show wireless switch vlan-map

------------------------------------------------------------------
Mobility VLAN Name              LVID  Role    Weight  Track
------------------              ----- -----   -------- -----
Sales                           11    None     1      NONE
Marketing                       12    None     1      NONE
Engineering                     13    None     1      NONE
Remediated                      14    None     1      NONE
default-MVLAN                   0     None     1      NONE
------------------------------------------------------------------
```

12 Define a *country-code* and enable then option to *Automatically Promote Discovered APs*. Finally *synchronize* the configuration:

```
WC8180(config-wireless# domain
WC8180(config-wireless# country-code us
WC8180(config-wireless# domain auto-promote-discovered-ap
WC8180(config-wireless# end
WC8180# wireless controller config-sync
WC8180# show wireless domain info

  Country                            : US
  AP QoS Mode                        : Disabled
  Roaming Timeout                    : 30 seconds
  TSPEC Violation Report Interval    : 300 seconds
  Auto Promote Discovered AP         : Enabled
  AP Image Update Download Group Size : 5 %
  AP Image Update Reset Group Size   : 5 %
  AP Reset Group Size                : 5 %
```

2.4.2 RADIUS Profiles

The Avaya 8100 series Wireless Controller can authenticate guest users against one or more RADIUS servers assigned to a RADIUS profile. The RADIUS profiles are then assigned to one or more network profiles that require 802.1X, MAC or captive-portal authentication. The Avaya 8100 series Wireless Controller will then direct all RADIUS authentication requests to the available servers defined in the RADIUS profile.

2.4.2.1 Configuration Steps

For this configuration step a RADIUS authentication profile named ***IDE*** will be created with the Ignition Server added as a RADIUS server. The following RADIUS parameters will be defined:

1) The ***IP Address*** set to ***192.168.10.52*** which matches the ***IP Address*** assigned to the ***Admin Port*** on the ***Ignition Server***.
2) The ***RADIUS Shared Secret*** set to ***avayalabs*** which matches the RADIUS shared secret defined on the Ignition Server in section 2.3.8.

1 Using the *AACLI* access the *Wireless* Security configuration context:

```
WC8180(config-wireless)# security
```

2 Create a *RADIUS Profile* with the id *1* named *IDE* and set the *type* to *Auth*:

```
WC8180(config-security)# radius profile IDE type auth

WC8180(config-security)# show wireless security radius profile

Total radius profiles: 1, auth: 1, acct: 0
Radius Profile                   Type
-------------------------------- --------------
IDE                              Authentication
```

3 Create a *RADIUS Server* entry with the *IP Address* assigned to the *Ignition Server* and assign it to the RADIUS Profile named *IDE*. When asked enter and confirm the secret *avayalabs*:

```
WC8180(config-security)# radius server 192.168.10.52 IDE secret

Enter server secret: avayalabs
Verify server secret: avayalabs

WC8180(config-security)# show wireless security radius server

Total radius servers: 1
Server IP       Radius Profile                   Port# Priority
--------------- -------------------------------- ----- --------
192.168.10.52   IDE                              1812  1
```

2.4.3 Network Profiles

Network Profiles define the wireless service parameters that radios advertise to wireless users. Each network profile defines the SSID name advertised to users, the mobility VLAN users are assigned, the authentication type and encryption ciphers. In addition the network profile defines the QoS mode and parameters for the wireless service.

2.4.3.1 Configuration Steps

For this configuration step ***Network Profile 2*** will be created with the following parameters will be defined:

1) The ***Profile Name*** set to ***AVAYA-IDE*** which for consistency matches the SSID name.
2) The ***SSID*** set to ***AVAYA-IDE*** which is advertised to wireless clients.
3) ***User Validation*** set to ***RADIUS*** and the ***RADIUS profile*** named ***IDE*** assigned.
4) ***WPA2*** security with ***CCMP*** encryption will be enabled.

1 Using the *AACLI* access the *Wireless Network Profile 2* configuration context:

```
WC8180(config-security)# network-profile 2
```

2 Set the *Profile Name* and *SSID Name* to *AVAYA-DOT1X* and define the *Mobility VLAN* name:

```
WC8180(config-network-profile)# profile-name AVAYA-DOT1X

WC8180(config-network-profile)# ssid AVAYA-DOT1X
```

3 Set the *User Validation* mode to *RADIUS* and assign the *RADIUS Profile* named *IDE*:

```
WC8180(config-network-profile)# user-validation radius

WC8180(config-network-profile)# radius authentication-profile IDE
```

4 Enable 802.11i security with CCMP encryption:

```
WC8180(config-network-profile)# security-mode wpa-enterprise

WC8180(config-network-profile)# wpa2 versions-supported WPA2 cipher-suite CCMP

WC8180(config-network-profile)# show wireless network-profile 2 detail
```

```
Network Profile ID: 2
Name : AVAYA-DOT1X
SSID : AVAYALAB-DOT1X
Hide SSID : No
Mobility Vlan Name :
No Response to Probe Request : Disabled
User Validation : RADIUS
Local User Group : Default
RADIUS Authentication Profile Name : IDE
RADIUS Accounting Profile Name :
RADIUS Accounting Mode : Disabled
Security Mode : WPA-Enterprise
MAC Validation : Disabled
WPA Versions : WPA2
WPA Encryption : CCMP
WPA2 Pre-Authentication : Enabled
WPA2 Pre-Authentication Limit : 0
WPA2 Key Caching Holdtime (minutes) : 10
Session Key Refresh Period (seconds) : 0
Group Key Refresh Period (seconds) : 0
Wireless ARP Suppression : Disabled
```

2.4.4 AP Profiles

Administrator's provision managed Access Points using AP profiles. AP profiles allow a common set of configuration parameters to be defined and applied to large groups of APs. Each AP profile is AP model specific and assigns radio profiles, network profiles and QoS mappings to Access Points assigned to the AP profile.

Each Access Point radio supports up to 16 Virtual Access Points (VAPs) each of with are assigned a unique MAC address and look like a single Access Point. Each radio can support a maximum of 16 network profile assignments.

2.4.4.1 Configuration Steps

For this configuration step ***Network Profile 2*** will be assigned to radios using the default ***AP Profile 1***:

1) ***Network Profile 2*** will be assigned to ***VAP 1*** on ***Radio 1*** (5GHz).
2) ***Network Profile 2*** assigned to ***VAP 1*** on ***Radio 2*** (2.4GHz).

1 Using the *AACLI* access the *Wireless AP Profile 1* configuration context:

```
WC8180(config-wireless)# ap-profile 1
```

2 Assign *Network Profile 2* to *VAP 1* on *Radios 1* & *2*:

```
WC8180(config-ap-profile)# network 1 1 profile-id 2

WC8180(config-ap-profile)# network 2 1 profile-id 2

WC8180(config-ap-profile)# show wireless ap-profile network 1

------------------------------------------------------------------
AP Profile Id  Radio Id  VAP Id  Network Profile Id  Radio Operation
-------------  --------  ------  ------------------  ---------------
          1         1       1                   2    On
          1         2       1                   2    On
------------------------------------------------------------------
```

3 Connect the Avaya 8100 series Access Points to the network and verify they are *managed*:

```
WC8180(config-wireless)# show wireless ap status

----------------------------------------------------------------------------
AP MAC             AP IP            Controller IP    Status         Need Image
                                                                     Upgrade
-----------------  ---------------  ---------------  -------------  ----------
5C:E2:86:0F:A3:C0  192.168.10.110   192.168.10.30    Managed          No
5C:E2:86:0F:C6:20  192.168.10.111   192.168.10.30    Managed          No
5C:E2:86:10:4A:C0  192.168.10.112   192.168.10.30    Managed          No
----------------------------------------------------------------------------
```

2.5 Avaya Ethernet Routing Switch

The following section outlines the configuration steps required to configure an Avaya Ethernet Routing Switch to provide secure PEAP authenticated access with dynamic VLAN assignments to wired hosts using the Ignition Server for RADIUS services.

ⓘ Note – This configuration example only provides the basic configuration parameters only. Please reference the Small, Medium, Large and Super Large Campus Technical Solution Guides available athttp://support.avaya.com/css/Products/P0846/All_Documents for Avaya's Ethernet Routing Switch best practices and implementation recommendations.

2.5.1 Base Configuration

The stack of Avaya Ethernet Routing Switches requires basic network configuration before it can provide wired services to users. The stack of Avaya Ethernet Routing Switches will be configured with the necessary management and users VLANs as well as a stack IP address which will be used for management access and RADIUS communications.

2.5.1.1 Configuration Steps

For this configuration step a factory defaulted stack of Avaya Ethernet Routing Switch 4500s will be configured with the following basic parameters:

1. ***Management*** VLAN ID ***10***, ***Sales*** VLAN ID ***11***, ***Marketing*** VLAN ID ***12***, ***Engineering*** VLAN ID ***13*** and ***Remediated*** VLAN ID ***14*** will be created:
   a. VLAN ***10*** will be defined as the management VLAN.
   b. The IP address ***192.168.10.19/24*** and will be assigned to the stack.
   c. A default gateway ***192.168.10.1*** will be assigned to the stack.

1 Using the *AACLI* access the *global* configuration context:

```
ERS4500# configure terminal
```

2 Create the Management, Sales, Marketing and Engineering VLANs *10 – 14*:

```
ERS4500(config)# vlan create 10 name Mgmt type port
ERS4500(config)# vlan create 11 name Sales type port
ERS4500(config)# vlan create 12 name Marketing type port
ERS4500(config)# vlan create 13 name Engineering type port
ERS4500(config)# vlan create 14 name Remediated type port
```

3 Assign VLAN *10* as the Management VLAN:

```
ERS4500(config)# vlan mgmt 10
```

3 Remove all ports from the default VLAN *1*:

```
ERS4500(config)# vlan members remove 1 all
```

4 Enable 802.1Q tagging on uplink port *1/48*:

```
ERS4500(config)# vlan ports 1/48 tagging tagall
ERS4500(config)# vlan ports 1/48 filter-untagged-frame enable
```

5 Add VLANs *10 – 13* to the uplink port *1/48* then set the PVID to *10*:

```
ERS4500(config)# vlan members add 10-14 1/48
ERS4500(config)# vlan ports 1/48 pvid 10
ERS4500(config)# show vlans
```

6 Verify VLAN configuration:

```
ERS4500(config)# show vlans

Id  Name                 Type     Protocol         User PID Active IVL/SVL Mgmt
--- -------------------- -------- ---------------- -------- ------ ------- ----
1   VLAN #1              Port     None             0x0000   Yes    IVL     No
        Port Members: NONE
10  Mgmt                 Port     None             0x0000   Yes    IVL     Yes
        Port Members: 1/48
11  Sales                Port     None             0x0000   Yes    IVL     No
        Port Members: 1/48
12  Marketing            Port     None             0x0000   Yes    IVL     No
        Port Members: 1/48
13  Engineering          Port     None             0x0000   Yes    IVL     No
        Port Members: 1/48
14  Remediated           Port     None             0x0000   Yes    IVL     No
        Port Members: 1/48
Total VLANs: 6

ERS4500(config)# show vlan interface vids 1/48

           Filter     Filter
          Untagged Unregistered
Unit/Port  Frames     Frames     PVID PRI    Tagging    Name
--------- -------- ------------ ---- --- ------------- --------------
1/48      Yes      Yes          10   0   TagAll        Unit 1,Port 48

ERS4500(config)# show vlan interface info 1/48

Unit/Port VLAN VLAN Name         VLAN VLAN Name         VLAN VLAN Name
--------- ---- ---------------- ---- ---------------- ---- ----------------
1/48      10   Mgmt             11   Sales            12   Marketing
          13   Engineering      14   Remediated
--------- ---- ---------------- ---- ---------------- ---- ----------------
```

7 Assign a stack IP address, mask and default gateway:

```
ERS4500(config)# ip address stack 192.168.10.19

ERS4500(config)# ip address netmask 255.255.255.0

ERS4500(config)# ip default-gateway 192.168.10.1

ERS4500(config)# show ip

Bootp/DHCP Mode: BootP When Needed

                      Configured       In Use         Last BootP/DHCP
                    --------------- --------------- --------------------
Stack IP Address:   192.168.10.19   192.168.10.19   0.0.0.0
Switch IP Address:  0.0.0.0                         0.0.0.0
Stack Subnet Mask:  255.255.255.0   255.255.255.0   0.0.0.0
Default Gateway:    192.168.10.1    192.168.10.1    0.0.0.0
```

2.5.2 RADIUS

Avaya Ethernet Routing Switches support RADIUS authentication servers which can be used to provide secure authenticated management access in addition to port based access control. The stack of Avaya Ethernet Routing Switches require a primary RADIUS server to be defined before wired EAPOL authentication can be enabled on the access layer ports. The Avaya Ethernet Routing Switches will be configured with the necessary RADIUS parameters that will allow the stack of Avaya Ethernet Routing Switches to communicate and forward EAPOL authentication requests to the Ignition Server.

2.5.2.1 Configuration Steps

For this configuration step the Ignition Server will be defined as a RADIUS server on the stack of Avaya Ethernet Routing Switch 4500s:

1. The Ignition Server's Admin IP address ***192.168.10.52*** will be added as the ***Primary RADIUS Server***.
2. The RADIUS shared secret ***avayalabs*** will be defined which matches the RADIUS shared secret defined on the Ignition Server in section 2.3.8.

1 Configure the Ignition Server's Admin IP address *192.168.10.52* as the primary RADIUS server IP and specify the RADIUS shared secret *avayalabs*:

```
ERS4500(config)# radius-server host 192.168.10.52

ERS4500(config)# radius-server key

Enter key: avayalabs

Confirm key: avayalabs
```

2 Verify the RADIUS server configuration:

```
ERS4500(config)# show radius-server
```

```
Password Fallback:  Disabled
Primary Host: 192.168.10.52
Secondary Host: 0.0.0.0
Port:  1812
Time-out:  2
Key:  ***************
Radius Accounting is  Disabled
AcctPort:  1813
```

2.5.3 EAPOL

Avaya Ethernet Routing Switches support the Extensible Authentication Protocol over LAN (EAPOL) encapsulation standard to provide port based access control. This concept uses the Extensible Authentication Protocol (EAP) as described in the IEEE 802.1X standard. EAPOL filters traffic based on source MAC address. Unauthorized hosts are unable to receive traffic from authorized devices or the network until the host successfully authenticate. Authentication hosts can be assigned to the native VLAN assigned to the access port or alternatively can be assigned to a dynamic VLAN provided by the RADIUS server.

By default Avaya Ethernet Routing Switches support a single EAPOL host per port; however Avaya includes support for a number of EAPOL enhancements which allows a port to assign Guest VLANs, support multiple EAPOL hosts, support a mix of EAPOL and non EAPOL hosts and support non EAPOL enabled hosts such as Printers or Access Points.

2.5.3.1 Configuration Steps

For this configuration step the access layer ports 1/1-47 and 2/1-24 on the stack of Avaya Ethernet Routing Switch 4500s will be enabled for EAPOL authentication with re-authentication support. For this example the default Single Host Single Authentication (SHSA) implementation will be used:

1. EAPOL on access layer ports ***1/1-47*** and ***2/1-24*** will be configured as ***Auto***.
2. EAPOL ***re-authentication*** will be enabled on access layer ports ***1/1-47*** and ***2/1-24*** using the default timer ***3600*** seconds.
3. EAPOL will remain disabled on the uplink port ***1/48*** which will be set to the default value ***Forced Authorized***.

1 Enable EAPOL on access ports 1/1-47,2/1-24 and enabled re-authentication:

```
ERS4500(config)# interface fastEthernet all
ERS4500(config-if)# eapol port 1/1-47,2/1-24 status auto
ERS4500(config-if)# eapol port 1/1-47,2/1-24 re-authentication enable
```

2 Configure the uplink port 1/47 as Forced Authorized:

```
ERS4500(config-if)# eapol port 1/48 status authorized
ERS4500(config-if)# exit
ERS4500(config)# show eapol
```

```
Admin Status:  Auto
Auth:  No
Admin Dir:  Both
Oper Dir:  Both
ReAuth Enable:  Yes
ReAuth Period:  3600
Quiet Period:  60
Xmit Period:  30
Supplic Timeout:  30
Server Timeout:  30
Max Req:  2
RDS DSE:  No
```

Access Ports 1/1-48,2/1-24

```
Admin Status:  F Auth
Auth:  Yes
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
```

Uplink Port 1/48

3 Globally enable EAPOL:

```
ERS4500(config)# eapol enable
ERS4500(config)# show eapol

EAPOL Administrative State:  Enabled
Port-mirroring on EAP ports: Disabled
```

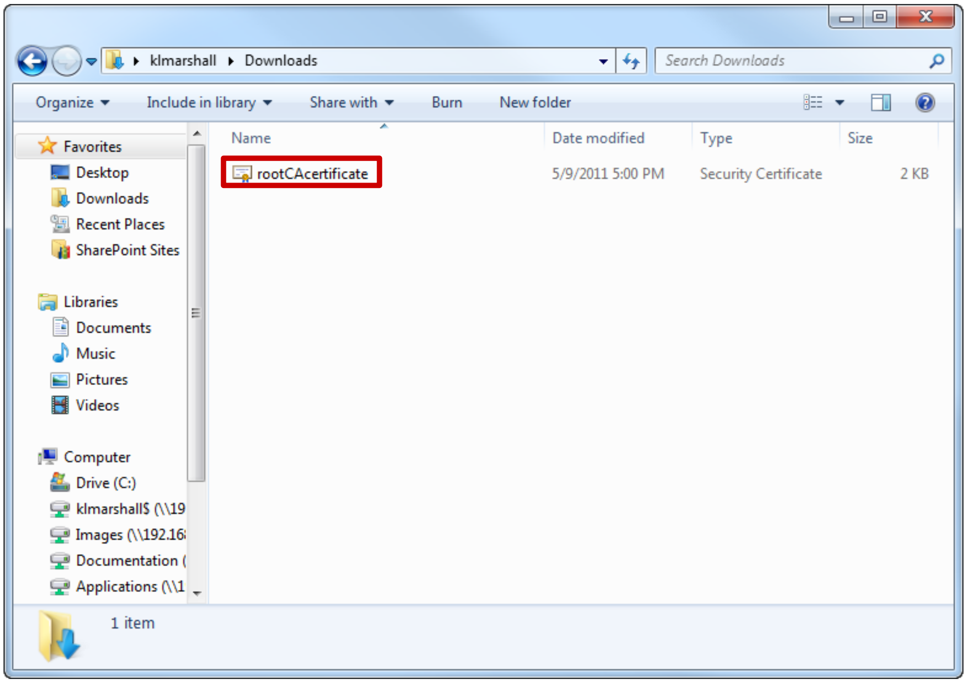
ⓘ Note – Details for enabling multihost EAPOL options can be located in the product documentation as well as various technical configuration guides available for download at http://support.avaya.com/css/Products/P0846/All_Documents.

2.6 Microsoft Windows 7

2.6.1 Root CA Certificate Installation

For this configuration step a base-64 encoded CA root certificate will be installed in Windows 7 so that Windows 7 can validate the signed server certificate issued to the Ignition Server during PEAP authentication:

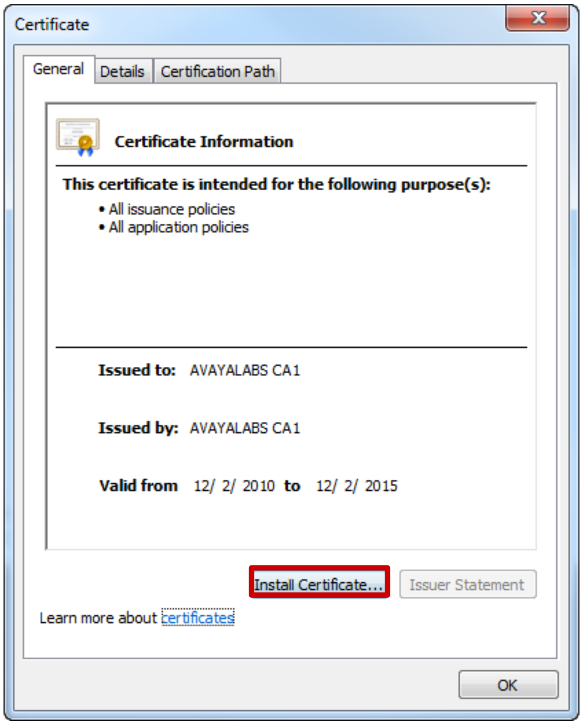
1 Using *Explorer* double click the CA root certificate to install. This will open the *Certificate*:



Name	Date modified	Type	Size
rootCAcertificate	5/9/2011 5:00 PM	Security Certificate	2 KB

1 item

2 Verify the CA root certificate you are installing is correct then click *Install Certificate*:



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

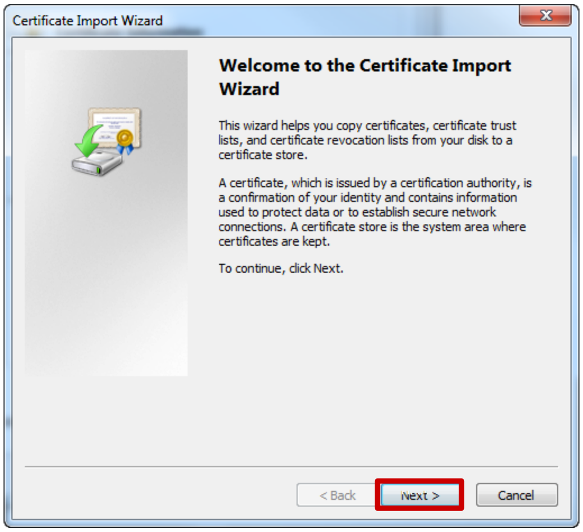
Issued to: AVAYALABS CA1

Issued by: AVAYALABS CA1

Valid from 12/ 2/ 2010 to 12/ 2/ 2015

Learn more about certificates

3 Click *Next*:



Certificate Import Wizard

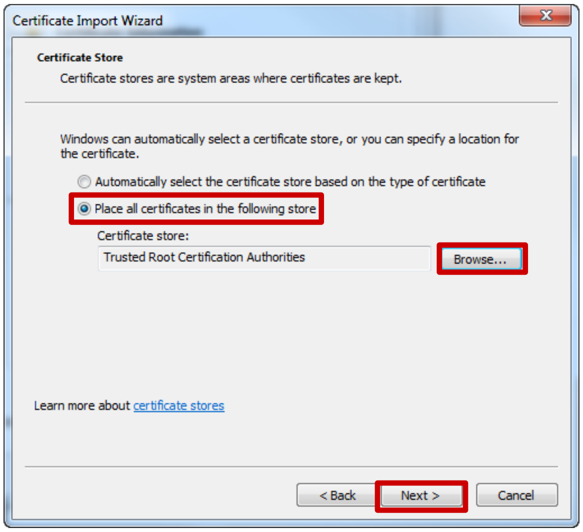
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

4 Select the option *Place all certificates in the following store* then click *Browse*. Select *Trusted Root Certificate Authorities* then click *OK*. Click *Next*:



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

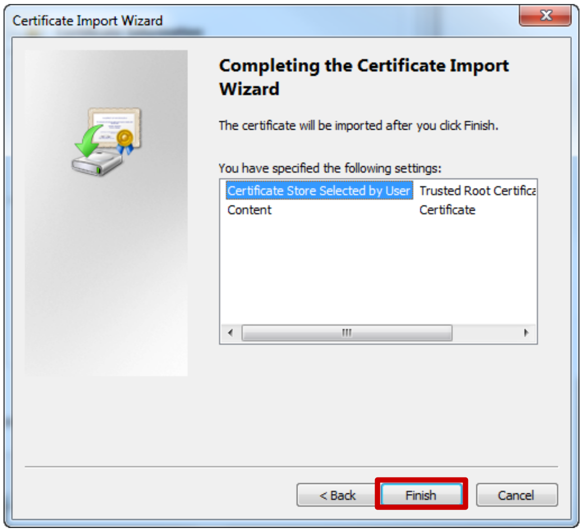
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

5 Click *Finish* to add the CA root certificate to the users *Trusted Root Certificate Authorities* certificate store:



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

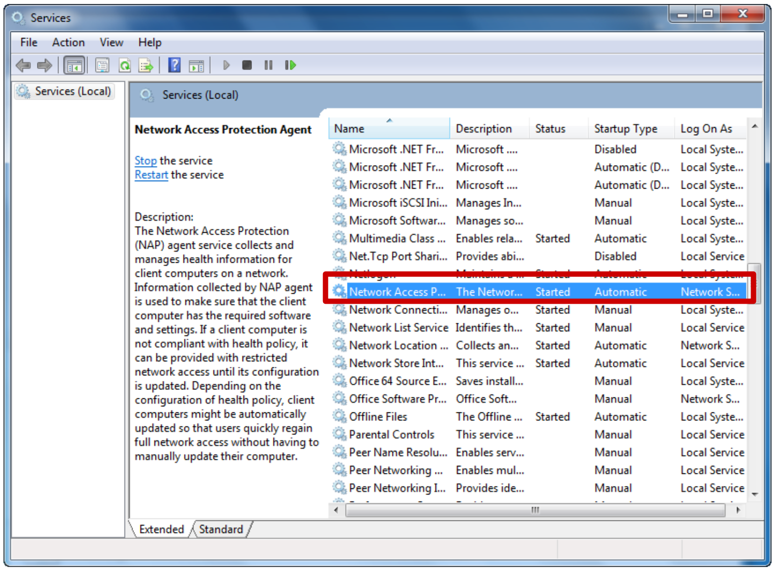
Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate

Note – If the server certificate installed on the Ignition Server was issued from Microsoft Certificate Services configured as an Enterprise Root CA and the Windows 7 workstation was added to the domain after Certificate Services was installed, the CA root certificate will be been automatically installed when the Windows 7 workstation was added to the domain.

2.6.2 Network Access Protection Agent Service

The Network Access Protection Agent service must be enabled before the Windows 7 workstation can participate in a network with Network Access Protection (NAP) enforcement enabled. The Network Access Protection Agent Service is disabled by default but can be stated on an individual Windows 7 workstation using the following procedure:

1 In Windows 7 click *Start > All Programs > Accessories > Run*. Enter *SERVICES.MSC* then click *OK*. Locate the service *Network Access Protection Agent*, right-click then select *Properties*:



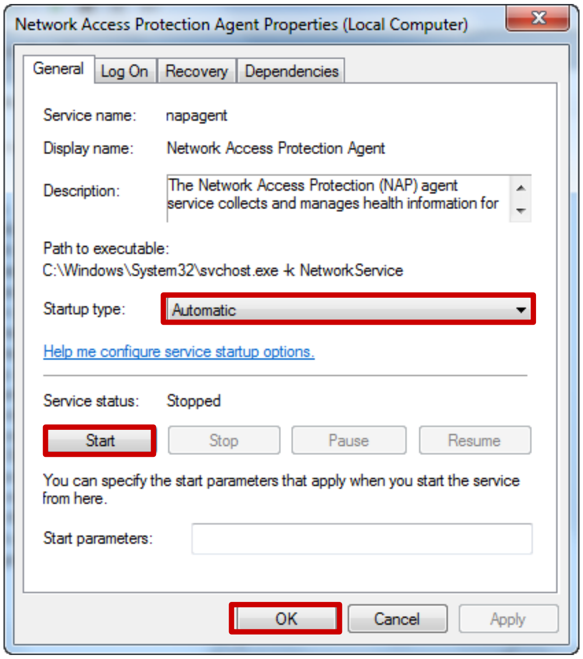
Network Access Protection Agent

Stop the service
Restart the service

Description:
The Network Access Protection (NAP) agent service collects and manages health information for client computers on a network. Information collected by NAP agent is used to make sure that the client computer has the required software and settings. If a client computer is not compliant with health policy, it can be provided with restricted network access until its configuration is updated. Depending on the configuration of health policy, client computers might be automatically updated so that users quickly regain full network access without having to manually update their computer.

Name	Description	Status	Startup Type	Log On As
Microsoft .NET Fr...	Microsoft		Disabled	Local Syste...
Microsoft .NET Fr...	Microsoft		Automatic (D...	Local Syste...
Microsoft .NET Fr...	Microsoft		Automatic (D...	Local Syste...
Microsoft iSCSI Ini...	Manages In...		Manual	Local Syste...
Microsoft Softwar...	Manages so...		Manual	Local Syste...
Multimedia Class ...	Enables rela...	Started	Automatic	Local Syste...
Net.Tcp Port Shari...	Provides abi...		Disabled	Local Service
Netlogon	Maintains a ...	Started	Automatic	Local Syste...
Network Access P...	The Networ...	Started	Automatic	Network S...
Network Connecti...	Manages o...	Started	Manual	Local Syste...
Network List Service	Identifies th...	Started	Manual	Local Service
Network Location ...	Collects an...	Started	Automatic	Network S...
Network Store Int...	This service ...	Started	Automatic	Local Service
Office 64 Source E...	Saves install...		Manual	Local Syste...
Office Software Pr...	Office Soft...		Manual	Network S...
Offline Files	The Offline ...	Started	Automatic	Local Syste...
Parental Controls	This service ...		Manual	Local Service
Peer Name Resolu...	Enables serv...		Manual	Local Service
Peer Networking ...	Enables mul...		Manual	Local Service
Peer Networking I...	Provides ide...		Manual	Local Service

2 Set the *Startup type* to *Automatic* then click *Start*. The *Service status* will change to *Started*. Click *OK*:


Network Access Protection Agent Properties (Local Computer)
General
Log On
Recovery
Dependencies
Help me configure service startup options.
Start
Stop
Pause
Resume
OK
Cancel
Apply

Service name: napagent

Display name: Network Access Protection Agent

Description: The Network Access Protection (NAP) agent service collects and manages health information for

Path to executable:
C:\Windows\System32\svchost.exe -k NetworkService

Startup type: Automatic

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

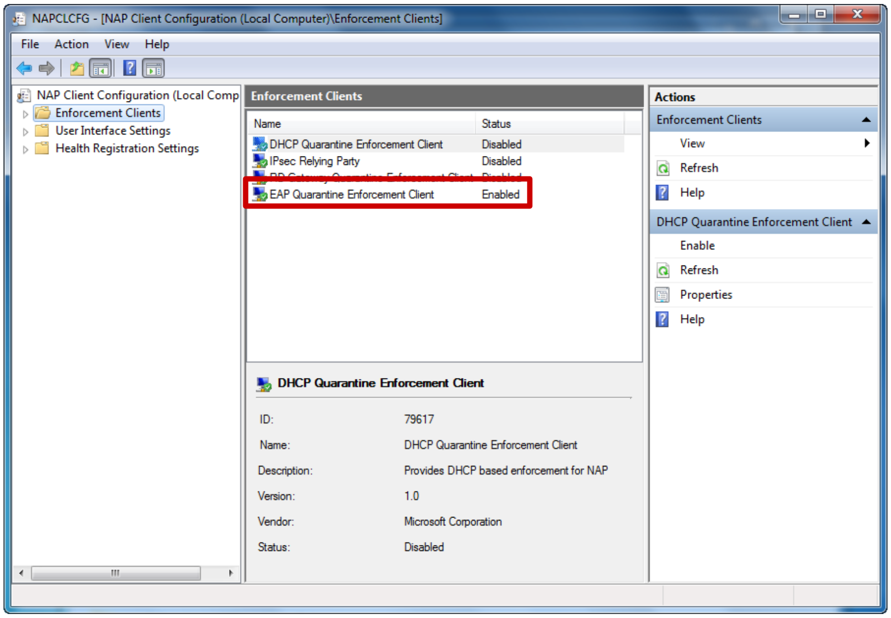
Start parameters:

2.6.3 EAP Quarantine Enforcement Client

Network Access Protection (NAP) requires the Windows workstations to run a Quarantine Enforcement Client for the specific NAP implementation that is being enabled. Windows 7 supports Quarantine Enforcement Clients for DHCP, IPsec, RD Gateway and EAP and by default all Quarantine Enforcement Clients are disabled.

The ***EAP Quarantine Enforcement Client*** can be enabled on an individual Windows 7 workstation using the following procedure:

1 In Windows 7 click *Start > All Programs > Accessories > Run*. Enter *NAPCLCFG.MSC* then click *OK*. Select *Enforcement Clients* then right-click on *EAP Quarantine Enforcement Client* and select *Enable*:


NAPCLCFG - [NAP Client Configuration (Local Computer)\Enforcement Clients]
File
Action
View
Help
NAP Client Configuration (Local Comp
Enforcement Clients
User Interface Settings
Health Registration Settings
Enforcement Clients
Actions
Enforcement Clients
View
Refresh
Help
DHCP Quarantine Enforcement Client
Enable
Refresh
Properties
Help

Name	Status
DHCP Quarantine Enforcement Client	Disabled
IPsec Relying Party	Disabled
RD Gateway Quarantine Enforcement Client	Disabled
EAP Quarantine Enforcement Client	Enabled

DHCP Quarantine Enforcement Client

ID:	79617
Name:	DHCP Quarantine Enforcement Client
Description:	Provides DHCP based enforcement for NAP
Version:	1.0
Vendor:	Microsoft Corporation
Status:	Disabled

Tip – The EAP Quarantine Enforcement Client can be optionally enabled using the CLI by issuing the ***netsh nap client set enforcement ID = 79623 ADMIN = "ENABLE"*** command.

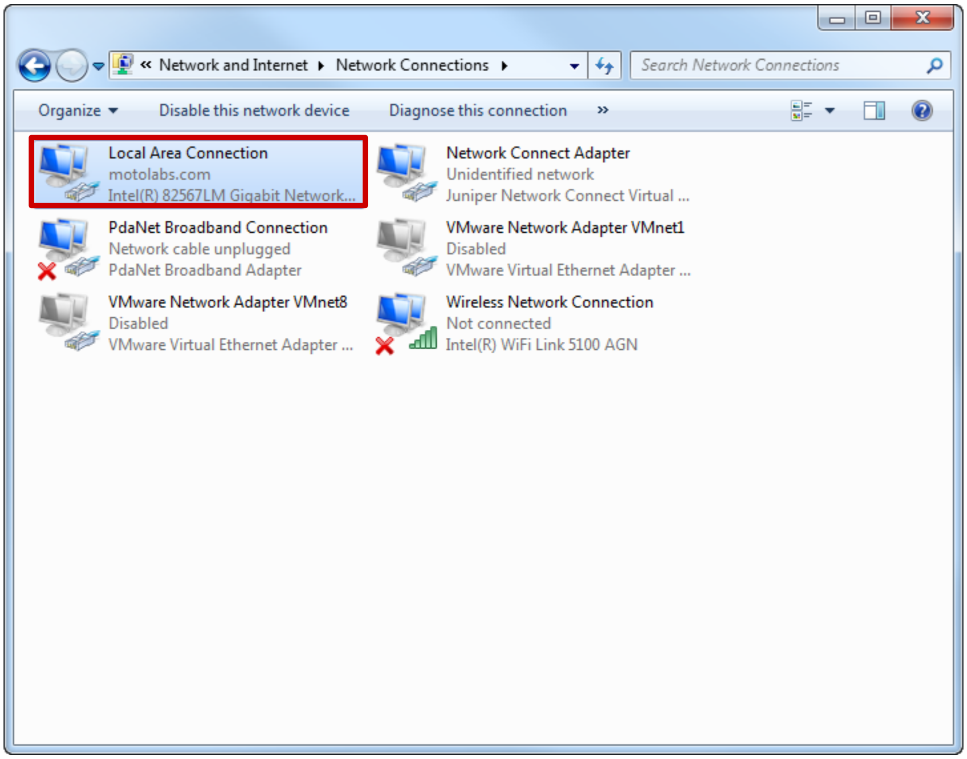
Tip – The EAP Quarantine Enforcement Client status can be optionally viewed using the CLI by issuing the ***netsh nap show configuration*** command.

2.6.4 Wired Authentication Configuration Steps

For this configuration step PEAP user authentication with NAP enforcement will be enabled on the Local Area Connection in Windows 7:

Note – The Windows 7 service ***Wired AutoConfig*** must be started before 802.1X can be enabled on a Local Area Connection.

1 In Windows 7 select *Control Panel > Network and Sharing Center > Change Adaptor Settings*. Right click on *Local Area Connection* then select *Properties*:


« Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize ▾
Disable this network device
Diagnose this connection
»

Local Area Connection
motolabs.com
Intel(R) 82567LM Gigabit Network...

Network Connect Adapter
Unidentified network
Juniper Network Connect Virtual ...

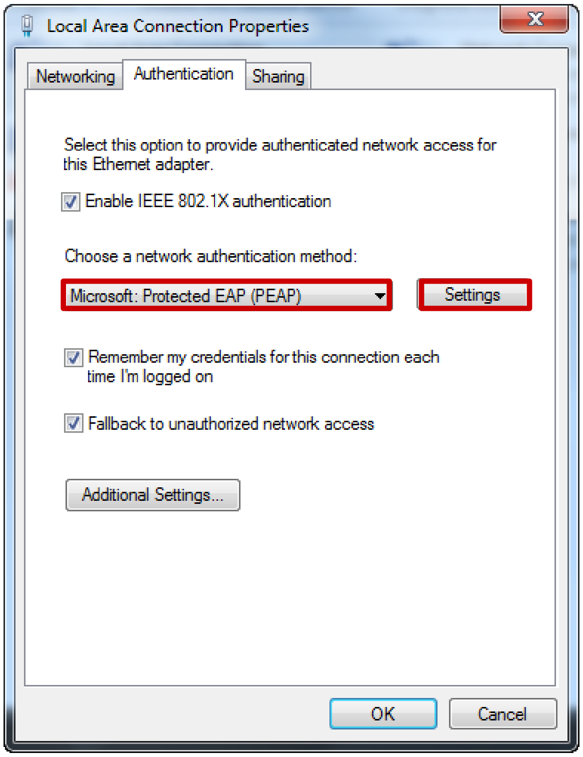
PdaNet Broadband Connection
Network cable unplugged
PdaNet Broadband Adapter

VMware Network Adapter VMnet1
Disabled
VMware Virtual Ethernet Adapter ...

VMware Network Adapter VMnet8
Disabled
VMware Virtual Ethernet Adapter ...

Wireless Network Connection
Not connected
Intel(R) WiFi Link 5100 AGN

2 Enable the option *Enable IEEE 802.1X authentication* then select the *network authentication method* type *Microsoft: Protected EAP (PEAP)*. Click *Settings*:



Local Area Connection Properties

Networking | Authentication | Sharing

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

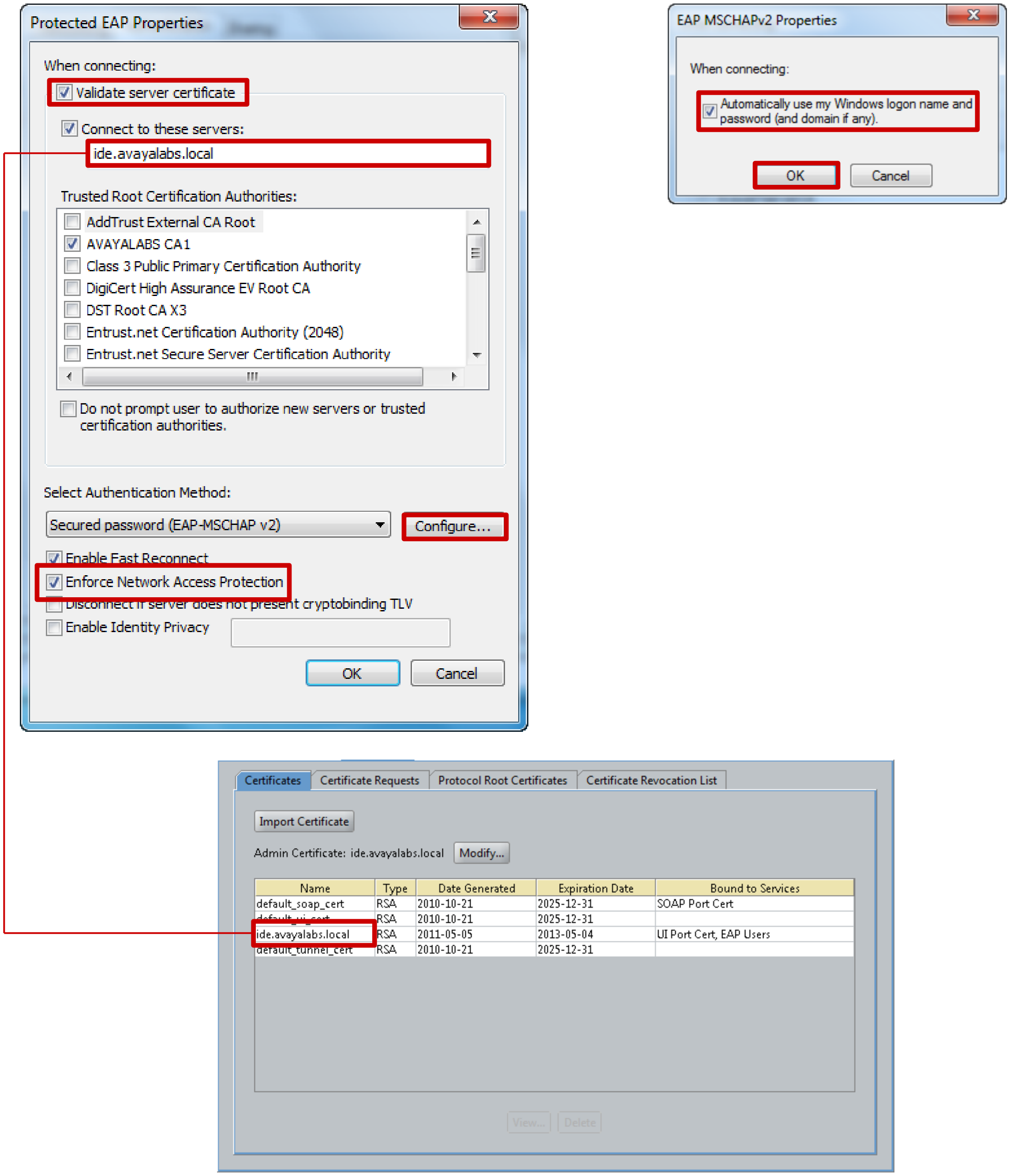
Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

3 **Enable the option *Validate Server Certificate*. Optionally enable *Connect to these servers* then enter the hostname of the Ignition Server as defined in the CN field of the signed server certificate installed on the Ignition Server. Enable *Enforce Network Access Protection*. Click *Configure* and enable the option *Automatically use my Windows logon name and password*. Click *OK* then *OK*:**



Protected EAP Properties

When connecting:

☑ Validate server certificate

☑ Connect to these servers:

ide.avayalabs.local

Trusted Root Certification Authorities:

☐ AddTrust External CA Root
☑ AVAYALABS CA1
☐ Class 3 Public Primary Certification Authority
☐ DigiCert High Assurance EV Root CA
☐ DST Root CA X3
☐ Entrust.net Certification Authority (2048)
☐ Entrust.net Secure Server Certification Authority

☐ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

☑ Enforce Network Access Protection

☐ Disconnect if server does not present cryptobinding TLV

☐ Enable Identity Privacy

EAP MSCHAPv2 Properties

When connecting:

☑ Automatically use my Windows logon name and password (and domain if any).

Admin Certificate: ide.avayalabs.local

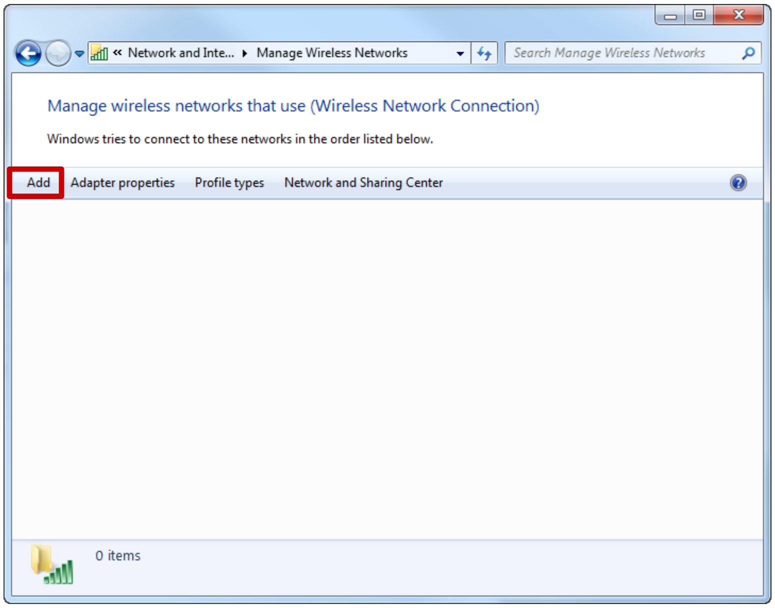
Name	Type	Date Generated	Expiration Date	Bound to Services
default_soap_cert	RSA	2010-10-21	2025-12-31	SOAP Port Cert
default_ui_cert	RSA	2010-10-21	2025-12-31	
ide.avayalabs.local	RSA	2011-05-05	2013-05-04	UI Port Cert, EAP Users
default_tunnel_cert	RSA	2010-10-21	2025-12-31	

2.6.5 Wireless Authentication Configuration Steps

For this configuration step a Wireless Network will be added to Windows 7 that will authenticate the Computer and Users on a WPA2 enabled Wireless LAN using PEAP while providing a single sign-on experience:

Note – The Windows 7 service ***WLAN AutoConfig*** must be started before 802.1X can be enabled on a Wireless interface.

1 In Windows 7 select *Control Panel > Network and Sharing Center > Manage Wireless Networks* then click *Add*:

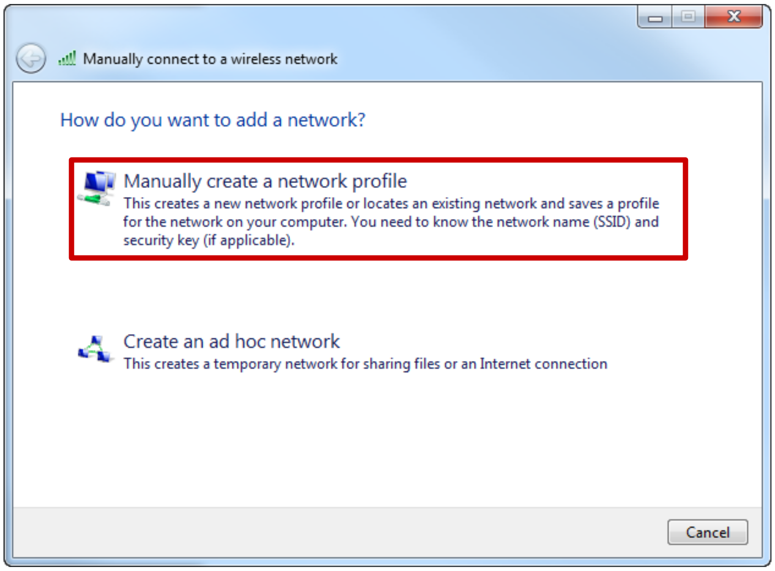

« Network and Inte... ▸ Manage Wireless Networks
Search Manage Wireless Networks
Add
Adapter properties
Profile types
Network and Sharing Center

Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

0 items

2 Select *Manually create a network profile*:

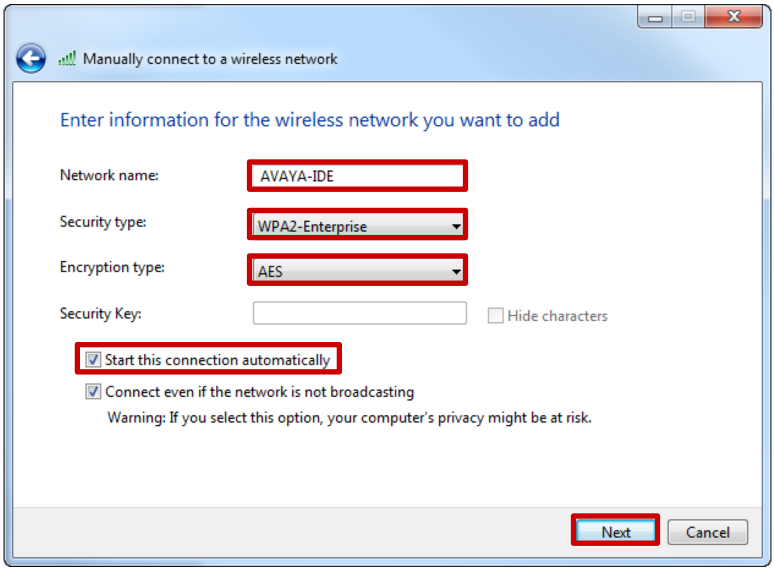


How do you want to add a network?

Manually create a network profile
This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).

Create an ad hoc network
This creates a temporary network for sharing files or an Internet connection

3 In the *Network name* field type the SSID name to connect to then set the *Security type* to *WPA2-Enterprise*. Set the *Encryption type* to *AES* then enable the option *Start this connection automatically*. Click *Next*:



Enter information for the wireless network you want to add

Network name: AVAYA-IDE

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

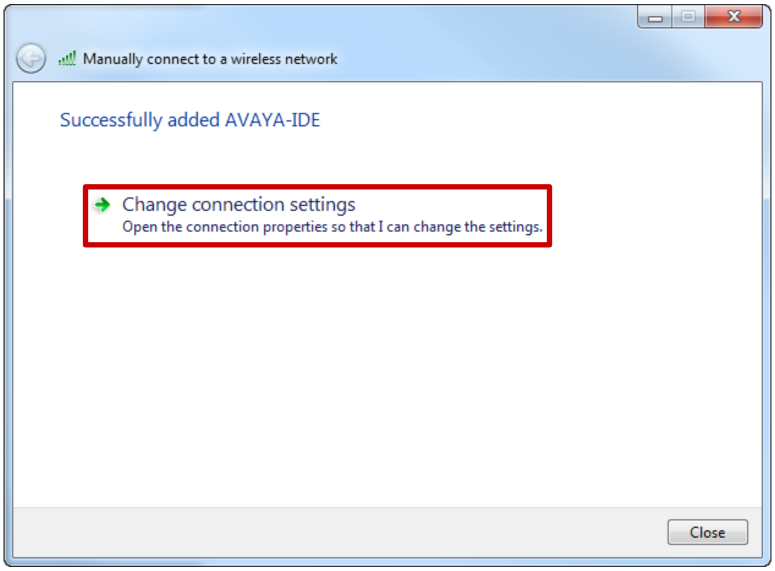
□ Hide characters

☑ Start this connection automatically

☑ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

4 Select *Change connection settings*:

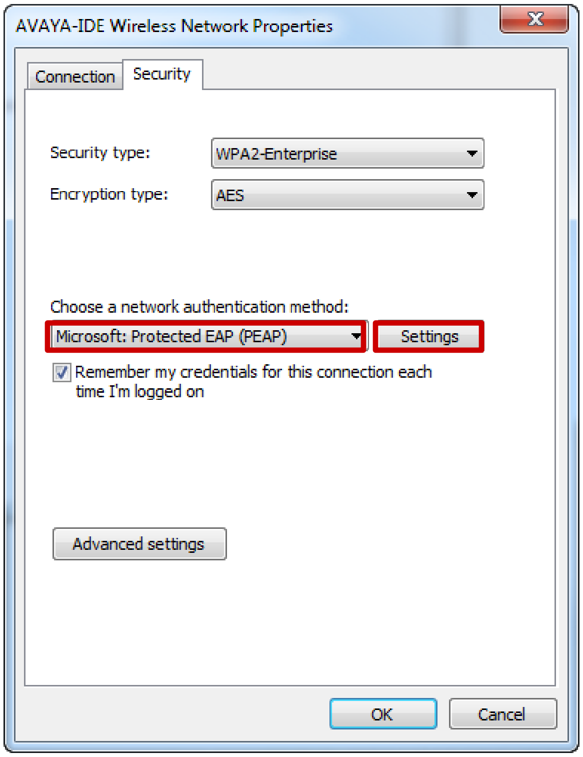


Successfully added AVAYA-IDE

Change connection settings

Open the connection properties so that I can change the settings.

5 Select the *network authentication method* type *Microsoft: Protected EAP (PEAP)* then click *Settings*:



AVAYA-IDE Wireless Network Properties

Connection | Security

Security type: WPA2-Enterprise

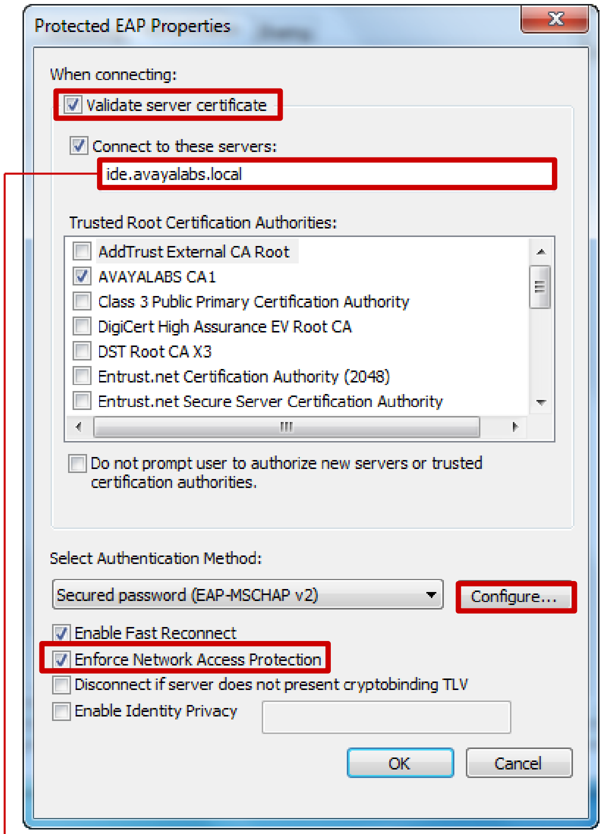
Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

6 Enable the option *Validate Server Certificate*. Optionally enable *Connect to these servers* then enter the hostname of the Ignition Server as defined in the CN field of the signed server certificate installed on the Ignition Server. Enable *Enforce Network Access Protection*. Click *Configure* and enable the option *Automatically use my Windows logon name and password*. Click *OK* then *OK*:



Protected EAP Properties

When connecting:

☑ Validate server certificate

☑ Connect to these servers:

ide.avayalabs.local

Trusted Root Certification Authorities:

- ☐ AddTrust External CA Root
- ☑ AVAYALABS CA1
- ☐ Class 3 Public Primary Certification Authority
- ☐ DigiCert High Assurance EV Root CA
- ☐ DST Root CA X3
- ☐ Entrust.net Certification Authority (2048)
- ☐ Entrust.net Secure Server Certification Authority

☐ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

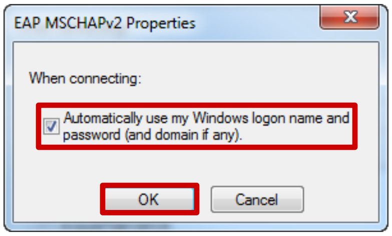
Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

☑ Enforce Network Access Protection

☐ Disconnect if server does not present cryptobinding TLV

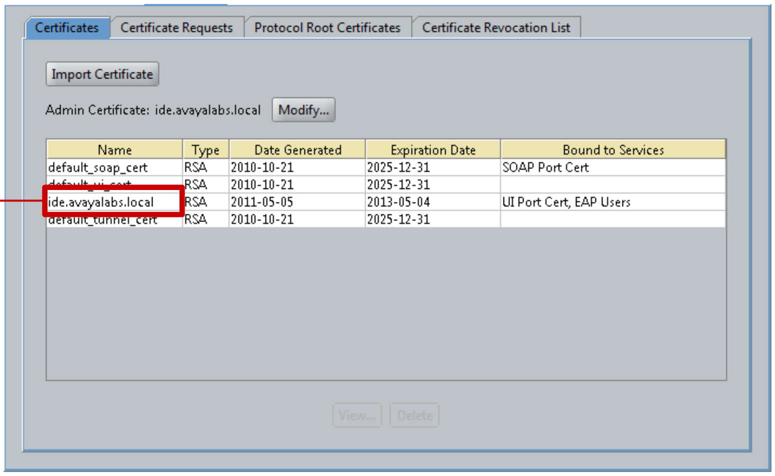
☐ Enable Identity Privacy



EAP MSCHAPv2 Properties

When connecting:

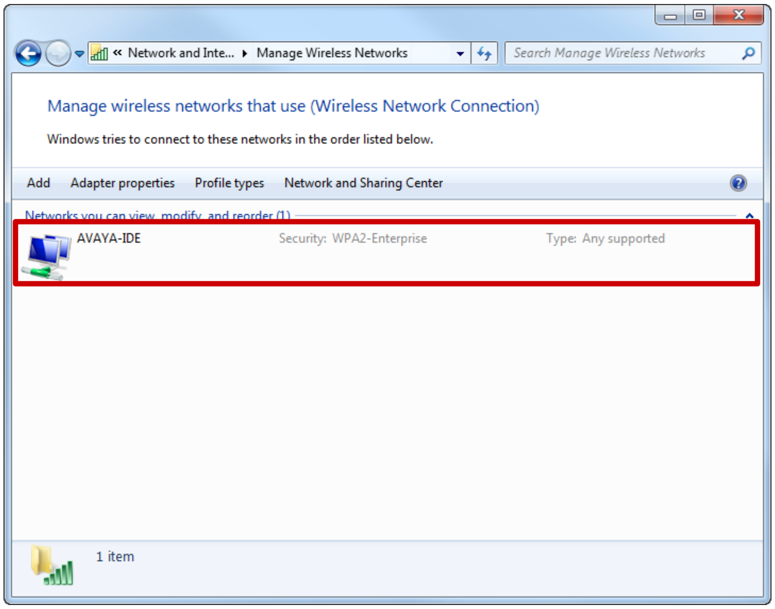
☑ Automatically use my Windows logon name and password (and domain if any).



Admin Certificate: ide.avayalabs.local

Name	Type	Date Generated	Expiration Date	Bound to Services
default_soap_cert	RSA	2010-10-21	2025-12-31	SOAP Port Cert
default_ui_cert	RSA	2010-10-21	2025-12-31	
ide.avayalabs.local	RSA	2011-05-05	2013-05-04	UI Port Cert, EAP Users
default_tunnel_cert	RSA	2010-10-21	2025-12-31	

7 A Wireless network profile has now been created in Windows 7:



« Network and Inte... ▸ Manage Wireless Networks
Search Manage Wireless Networks

Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

Add
Adapter properties
Profile types
Network and Sharing Center
Networks you can view, modify, and reorder (1)

AVAYA-IDE Security: WPA2-Enterprise Type: Any supported

1 item

3. Verification

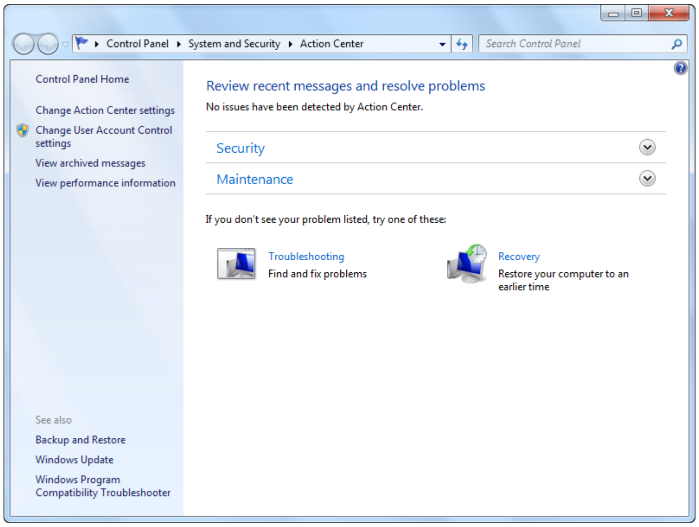
3.1 Avaya Ethernet Routing Switch

3.1.1 NAP Compliant Users

The following section highlights the steps required to validate EAPoL PEAP user authentication for Compliant Windows 7 Enterprise workstation:

1 Login to Windows 7 using a domain username and password which will initiate PEAP user authentication. In this example a domain user that is a member of the *Sales* group is used and the computer is fully compliant:

2 Open the Windows 7 *Action Center*. No issues will be displayed:


Control Panel ▸ System and Security ▸ Action Center
Search Control Panel
Control Panel Home
Change Action Center settings
Change User Account Control settings
View archived messages
View performance information
Security
Maintenance
Troubleshooting
Find and fix problems
Recovery
Restore your computer to an earlier time
See also
Backup and Restore
Windows Update
Windows Program Compatibility Troubleshooter

Review recent messages and resolve problems

No issues have been detected by Action Center.

If you don't see your problem listed, try one of these:

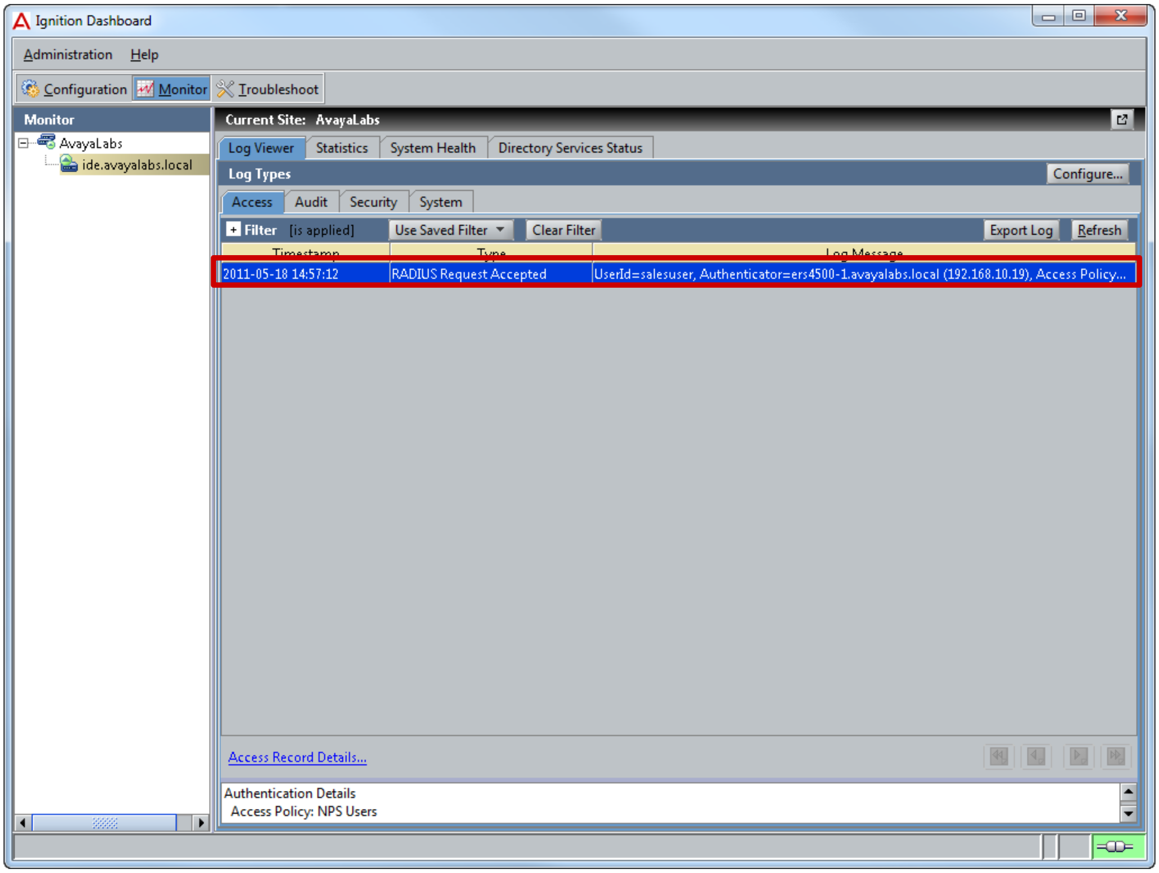
3 On the Avaya Ethernet Routing Switch view the EAPOL port status. The *Auth* status will display as *Yes* indicating the sales user has authenticated. In this example the Windows 7 workstation is connected to port *1/1*:

```
ERS4500# show eapol port 1/1

EAPOL Administrative State:  Enabled
Port-mirroring on EAP ports: Disabled
Unit/Port:  1/1
    Admin Status:  Auto
    Auth:  Yes
    Admin Dir:  Both
    ..
```

4 On the Avaya Ethernet Routing Switch view the dynamic VLAN assignment. In this example the sales user is *Compliant* and will be assigned to the *Sales* VLAN:

```
ERS4500# show vlan interface vids 1/1

Unit/Port VLAN VLAN Name        VLAN VLAN Name        VLAN VLAN Name
--------- ---- ---------------- ---- ---------------- ---- ----------------
1/1       11   Sales
--------- ---- ---------------- ---- ---------------- ---- ----------------
```

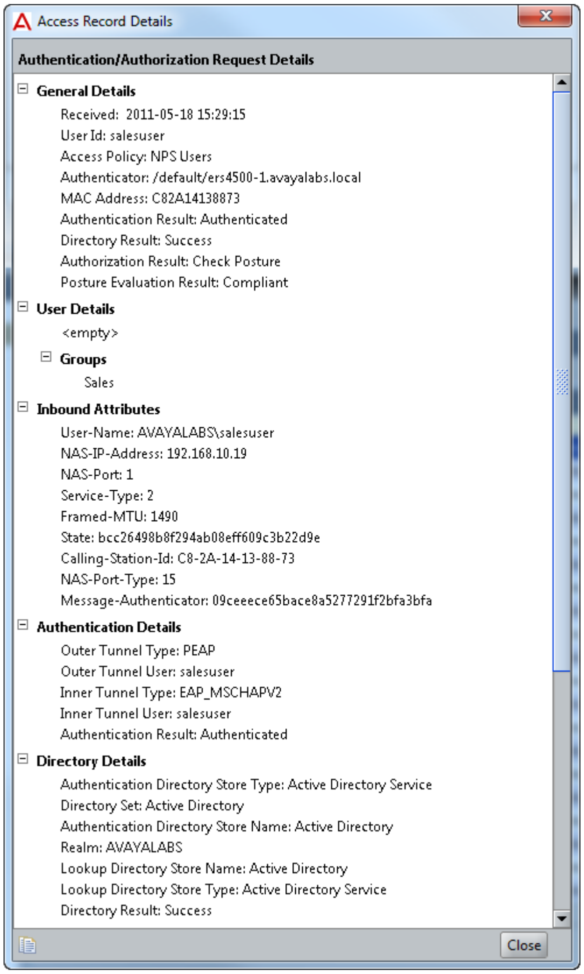
5 Using the *Ignition Dashboard* view the *Access Logs* by selecting *Monitor > Site-Name > Ignition-Server-Name > Log Viewer > Access*. A record showing a successful authentication and authorization for the sales user will be listed:



Timestamp	Type	Log Message
2011-05-18 14:57:12	RADIUS Request Accepted	UserId=salesuser, Authenticator=ers4500-1.avayalabs.local (192.168.10.19), Access Policy...

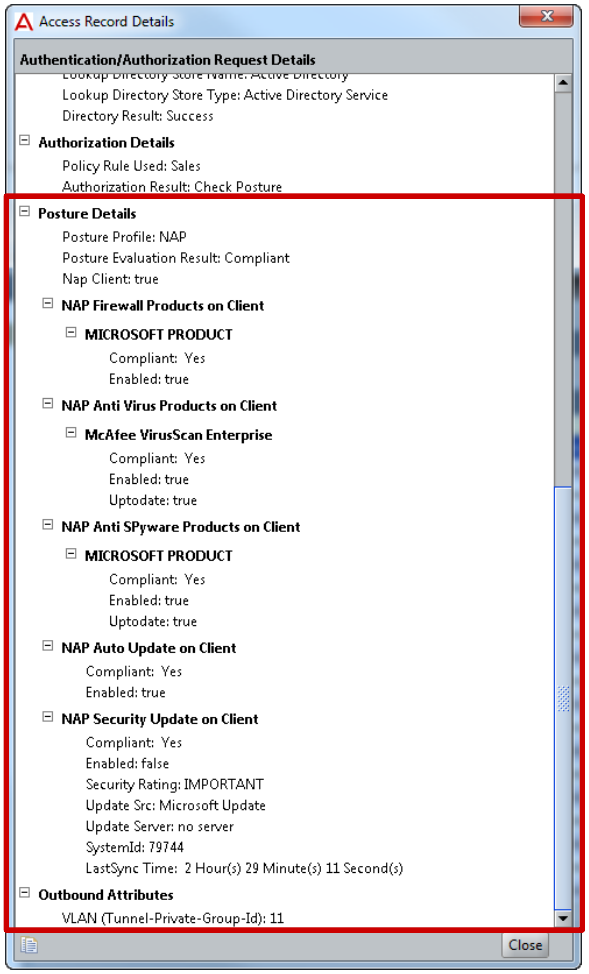
Authentication Details
Access Policy: NPS Users

6 Double-click on the computer authentication log entry to view the authentication and authorization details. The *Posture Details* section in the *Access Record* will highlight the posture evaluation results for the sales user and the assigned VLAN:


Access Record Details

Authentication/Authorization Request Details

```
⊟ General Details
     Received: 2011-05-18 15:29:15
     User Id: salesuser
     Access Policy: NPS Users
     Authenticator: /default/ers4500-1.avayalabs.local
     MAC Address: C82A14138873
     Authentication Result: Authenticated
     Directory Result: Success
     Authorization Result: Check Posture
     Posture Evaluation Result: Compliant
⊟ User Details
     <empty>
   ⊟ Groups
        Sales
⊟ Inbound Attributes
     User-Name: AVAYALABS\salesuser
     NAS-IP-Address: 192.168.10.19
     NAS-Port: 1
     Service-Type: 2
     Framed-MTU: 1490
     State: bcc26498b8f294ab08eff609c3b22d9e
     Calling-Station-Id: C8-2A-14-13-88-73
     NAS-Port-Type: 15
     Message-Authenticator: 09ceeece65bace8a5277291f2bfa3bfa
⊟ Authentication Details
     Outer Tunnel Type: PEAP
     Outer Tunnel User: salesuser
     Inner Tunnel Type: EAP_MSCHAPV2
     Inner Tunnel User: salesuser
     Authentication Result: Authenticated
⊟ Directory Details
     Authentication Directory Store Type: Active Directory Service
     Directory Set: Active Directory
     Authentication Directory Store Name: Active Directory
     Realm: AVAYALABS
     Lookup Directory Store Name: Active Directory
     Lookup Directory Store Type: Active Directory Service
     Directory Result: Success
```


Access Record Details

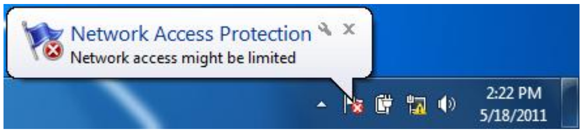
Authentication/Authorization Request Details

```
     Lookup Directory Store Name: Active Directory
     Lookup Directory Store Type: Active Directory Service
     Directory Result: Success
⊟ Authorization Details
     Policy Rule Used: Sales
     Authorization Result: Check Posture
⊟ Posture Details
     Posture Profile: NAP
     Posture Evaluation Result: Compliant
     Nap Client: true
   ⊟ NAP Firewall Products on Client
      ⊟ MICROSOFT PRODUCT
           Compliant:  Yes
           Enabled: true
   ⊟ NAP Anti Virus Products on Client
      ⊟ McAfee VirusScan Enterprise
           Compliant:  Yes
           Enabled: true
           Uptodate: true
   ⊟ NAP Anti SPyware Products on Client
      ⊟ MICROSOFT PRODUCT
           Compliant:  Yes
           Enabled: true
           Uptodate: true
   ⊟ NAP Auto Update on Client
        Compliant:  Yes
        Enabled: true
   ⊟ NAP Security Update on Client
        Compliant:  Yes
        Enabled: false
        Security Rating: IMPORTANT
        Update Src: Microsoft Update
        Update Server: no server
        SystemId: 79744
        LastSync Time:  2 Hour(s) 29 Minute(s) 11 Second(s)
⊟ Outbound Attributes
     VLAN (Tunnel-Private-Group-Id): 11
```

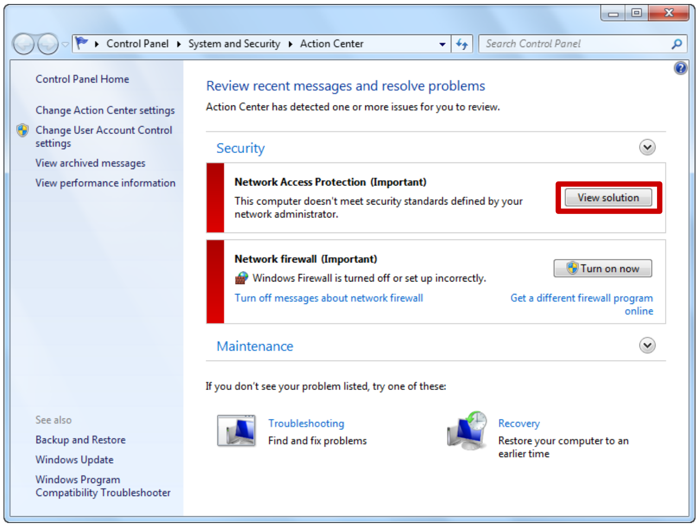
3.1.2 NAP Non-Compliant Users

The following section highlights the steps required to validate EAPoL PEAP user authentication for Non-Compliant Windows 7 Enterprise workstation:

1 Login to Windows 7 using a domain username and password which will initiate PEAP user authentication. In this example a domain user that is a member of the *Sales* group is used and the *Windows Firewall* and *Auto Remediation* have been *disabled*. A *Network Access Protection* dialog will be displayed in the task bar stating that *Network access might be limited*:


Network Access Protection
Network access might be limited

2 Open the Windows 7 *Action Center* then select *View Solution*:


Control Panel ▸ System and Security ▸ Action Center
Search Control Panel
Control Panel Home
Change Action Center settings
Change User Account Control settings
View archived messages
View performance information
See also
Backup and Restore
Windows Update
Windows Program Compatibility Troubleshooter

Review recent messages and resolve problems

Action Center has detected one or more issues for you to review.

Security

Network Access Protection (Important)

This computer doesn't meet security standards defined by your network administrator.

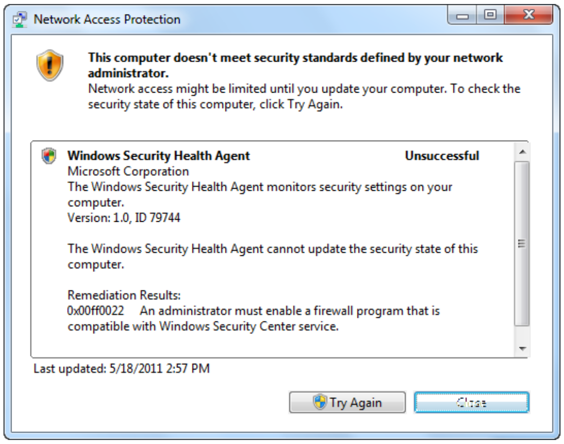
Network firewall (Important)

Windows Firewall is turned off or set up incorrectly.

Turn on now
Turn off messages about network firewall
Get a different firewall program online
Maintenance

If you don't see your problem listed, try one of these:

3 A Network Access Protection dialog window outlining why the computer has failed posture evaluation and how to remediate the issue will be displayed:



This computer doesn't meet security standards defined by your network administrator.
Network access might be limited until you update your computer. To check the security state of this computer, click Try Again.

Windows Security Health Agent **Unsuccessful**
Microsoft Corporation
The Windows Security Health Agent monitors security settings on your computer.
Version: 1.0, ID 79744

The Windows Security Health Agent cannot update the security state of this computer.

Remediation Results:
0x00ff0022 An administrator must enable a firewall program that is compatible with Windows Security Center service.

Last updated: 5/18/2011 2:57 PM

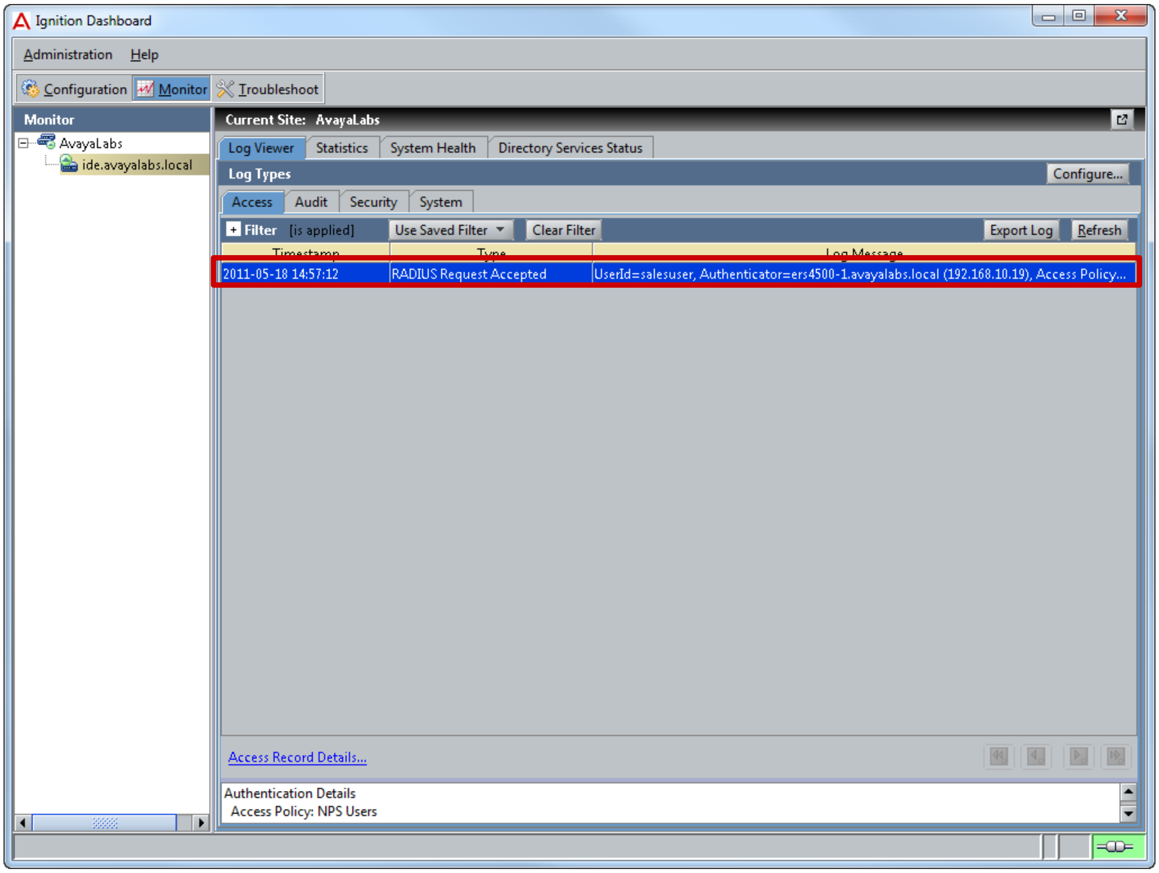
4 On the Avaya Ethernet Routing Switch view the EAPOL port status. The *Auth* status will display as *Yes* indicating the sales user has authenticated. In this example the Windows 7 workstation is connected to port *1/1*:

```
ERS4500# show eapol port 1/1

EAPOL Administrative State:  Enabled
Port-mirroring on EAP ports: Disabled
Unit/Port:  1/1
    Admin Status:  Auto
    Auth:  Yes
    Admin Dir:  Both
    ..
```

5 On the Avaya Ethernet Routing Switch view the dynamic VLAN assignment. In this example the sales user is *Non-Compliant* and will be assigned to the *Remediated* VLAN:

```
ERS4500# show vlan interface vids 1/1

Unit/Port VLAN VLAN Name         VLAN VLAN Name         VLAN VLAN Name
--------- ---- ----------------  ---- ----------------  ---- ----------------
1/1       14   Remediated
--------- ---- ----------------  ---- ----------------  ---- ----------------
```

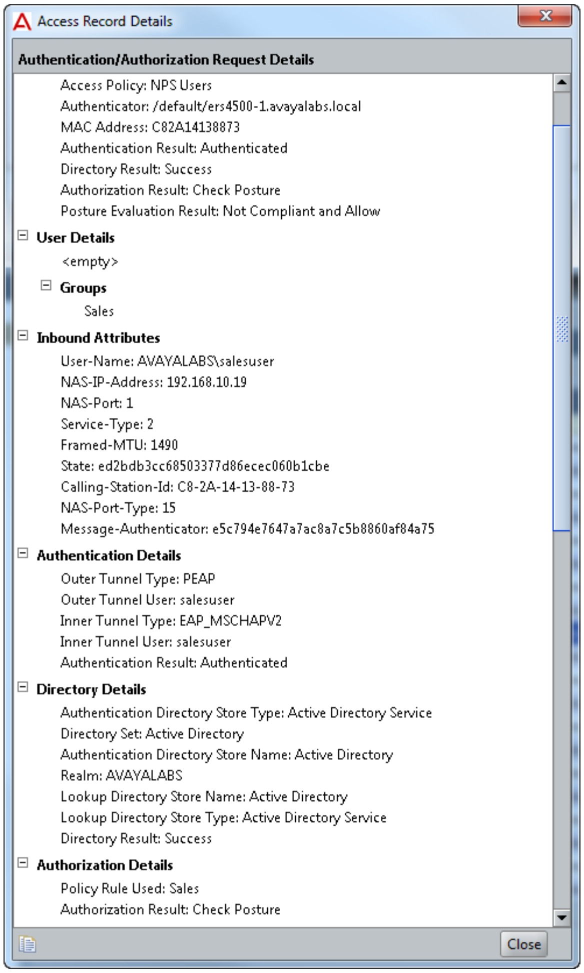
6 Using the *Ignition Dashboard* view the *Access Logs* by selecting *Monitor > Site-Name > Ignition-Server-Name > Log Viewer > Access.* A record showing a successful authentication and authorization for the sales user will be listed:



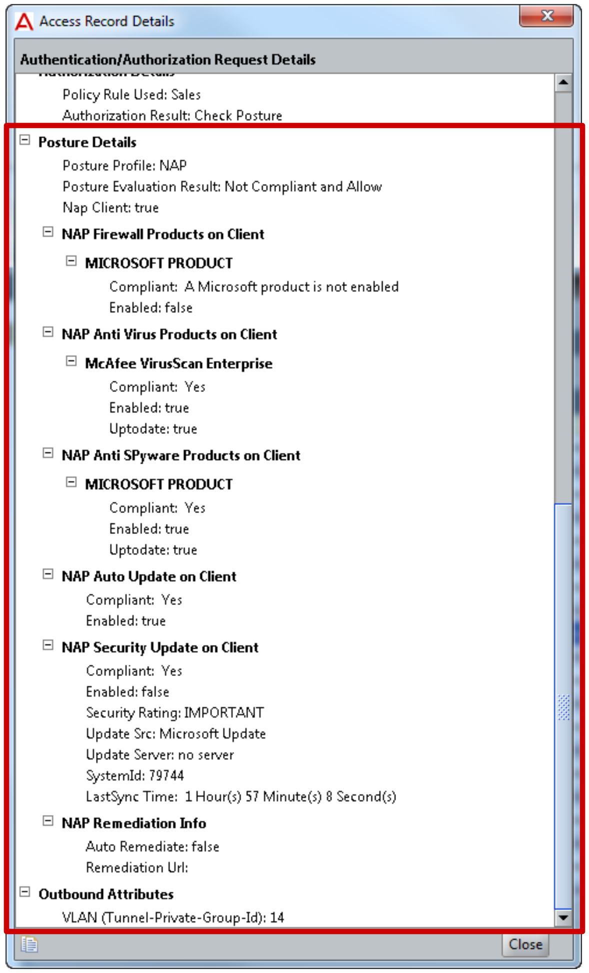
Timestamp	Type	Log Message
2011-05-18 14:57:12	RADIUS Request Accepted	UserId=salesuser, Authenticator=ers4500-1.avayalabs.local (192.168.10.19), Access Policy...

Authentication Details
Access Policy: NPS Users

5 Double-click on the computer authentication log entry to view the authentication and authorization details. The *Posture Details* section in the *Access Record* will highlight the posture evaluation results for the sales user, why posture evaluation failed and the assigned VLAN:



```
Access Record Details
Authentication/Authorization Request Details
    Access Policy: NPS Users
    Authenticator: /default/ers4500-1.avayalabs.local
    MAC Address: C82A14138873
    Authentication Result: Authenticated
    Directory Result: Success
    Authorization Result: Check Posture
    Posture Evaluation Result: Not Compliant and Allow
⊟ User Details
    <empty>
  ⊟ Groups
      Sales
⊟ Inbound Attributes
    User-Name: AVAYALABS\salesuser
    NAS-IP-Address: 192.168.10.19
    NAS-Port: 1
    Service-Type: 2
    Framed-MTU: 1490
    State: ed2bdb3cc68503377d86ecec060b1cbe
    Calling-Station-Id: C8-2A-14-13-88-73
    NAS-Port-Type: 15
    Message-Authenticator: e5c794e7647a7ac8a7c5b8860af84a75
⊟ Authentication Details
    Outer Tunnel Type: PEAP
    Outer Tunnel User: salesuser
    Inner Tunnel Type: EAP_MSCHAPV2
    Inner Tunnel User: salesuser
    Authentication Result: Authenticated
⊟ Directory Details
    Authentication Directory Store Type: Active Directory Service
    Directory Set: Active Directory
    Authentication Directory Store Name: Active Directory
    Realm: AVAYALABS
    Lookup Directory Store Name: Active Directory
    Lookup Directory Store Type: Active Directory Service
    Directory Result: Success
⊟ Authorization Details
    Policy Rule Used: Sales
    Authorization Result: Check Posture
                                                        Close
```



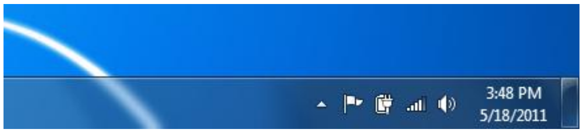
```
Access Record Details
Authentication/Authorization Request Details
    Policy Rule Used: Sales
    Authorization Result: Check Posture
⊟ Posture Details
    Posture Profile: NAP
    Posture Evaluation Result: Not Compliant and Allow
    Nap Client: true
  ⊟ NAP Firewall Products on Client
    ⊟ MICROSOFT PRODUCT
        Compliant:  A Microsoft product is not enabled
        Enabled: false
  ⊟ NAP Anti Virus Products on Client
    ⊟ McAfee VirusScan Enterprise
        Compliant:  Yes
        Enabled: true
        Uptodate: true
  ⊟ NAP Anti SPyware Products on Client
    ⊟ MICROSOFT PRODUCT
        Compliant:  Yes
        Enabled: true
        Uptodate: true
  ⊟ NAP Auto Update on Client
      Compliant:  Yes
      Enabled: true
  ⊟ NAP Security Update on Client
      Compliant:  Yes
      Enabled: false
      Security Rating: IMPORTANT
      Update Src: Microsoft Update
      Update Server: no server
      SystemId: 79744
      LastSync Time:  1 Hour(s) 57 Minute(s) 8 Second(s)
  ⊟ NAP Remediation Info
      Auto Remediate: false
      Remediation Url:
⊟ Outbound Attributes
    VLAN (Tunnel-Private-Group-Id): 14
                                                        Close
```

3.2 Wireless LAN 8100

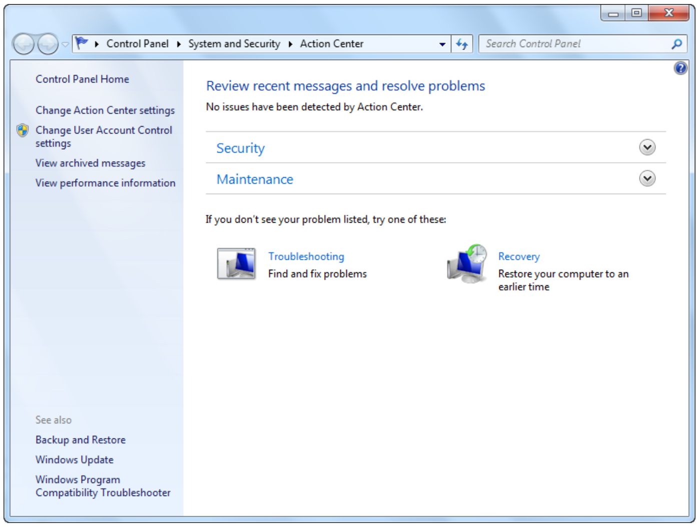
3.2.1 NAP Compliant Users

The following section highlights the steps required to validate Wireless PEAP user authentication for Compliant Windows 7 Enterprise workstation:

1 Login to Windows 7 using a domain username and password which will initiate wireless PEAP user authentication. In this example a domain user that is a member of the *Sales* group is used and the computer is fully compliant:



2 Open the Windows 7 *Action Center*. No issues will be displayed:



Control Panel Home

Change Action Center settings

Change User Account Control settings

View archived messages

View performance information

Review recent messages and resolve problems

No issues have been detected by Action Center.

Security

Maintenance

If you don't see your problem listed, try one of these:

Troubleshooting
Find and fix problems

Recovery
Restore your computer to an earlier time

See also

Backup and Restore

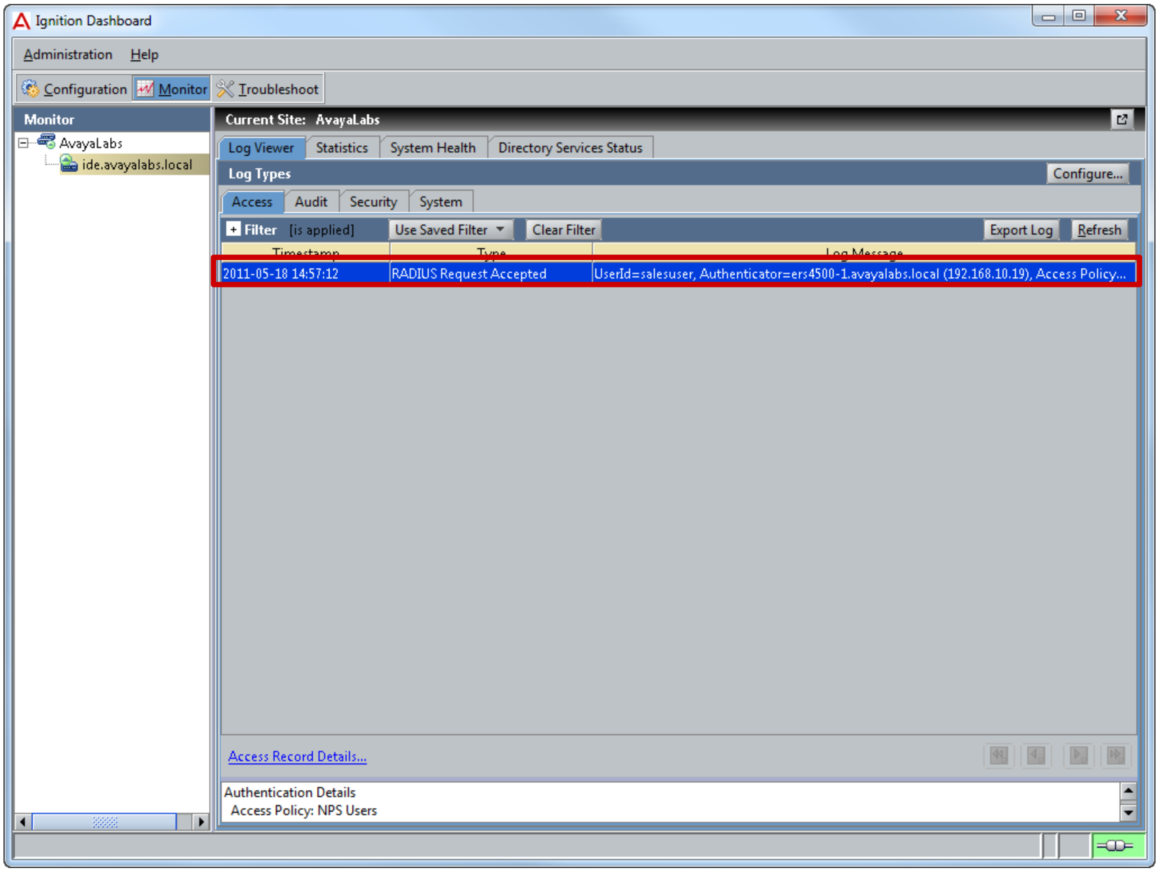
Windows Update

Windows Program Compatibility Troubleshooter

3 On the Avaya Ethernet Routing Switch view the dynamic VLAN assignment. In this example the sales user is *Compliant* and will be assigned to the *Sales* Mobility VLAN:

```
WC8180# show wireless client status

Total number of clients: 1


-------------------------------------------------------------------------------
     Client           Client         Associated      Mobility        Status
  MAC Address       IP Address       Controller        VLAN
----------------- --------------- --------------- --------------- -------------
E0:F8:47:0F:E0:14 192.168.10.100  192.168.10.30   Sales           Authenticated
-------------------------------------------------------------------------------
```

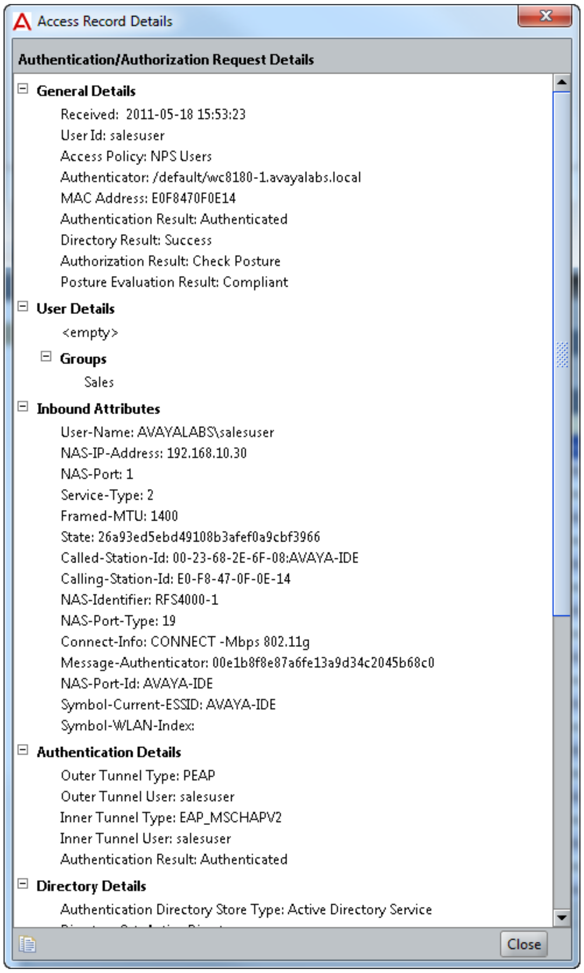
4 Using the *Ignition Dashboard* view the *Access Logs* by selecting *Monitor > Site-Name > Ignition-Server-Name > Log Viewer > Access*. A record showing a successful authentication and authorization for the sales user will be listed:



Timestamp	Type	Log Message
2011-05-18 14:57:12	RADIUS Request Accepted	UserId=salesuser, Authenticator=ers4500-1.avayalabs.local (192.168.10.19), Access Policy...

Authentication Details
Access Policy: NPS Users

5 Double-click on the computer authentication log entry to view the authentication and authorization details. The *Posture Details* section in the *Access Record* will highlight the posture evaluation results for the sales user and the assigned VLAN:



Access Record Details

Authentication/Authorization Request Details

General Details

Received: 2011-05-18 15:53:23
User Id: salesuser
Access Policy: NPS Users
Authenticator: /default/wc8180-1.avayalabs.local
MAC Address: E0F8470F0E14
Authentication Result: Authenticated
Directory Result: Success
Authorization Result: Check Posture
Posture Evaluation Result: Compliant

User Details

<empty>

Groups

Sales

Inbound Attributes

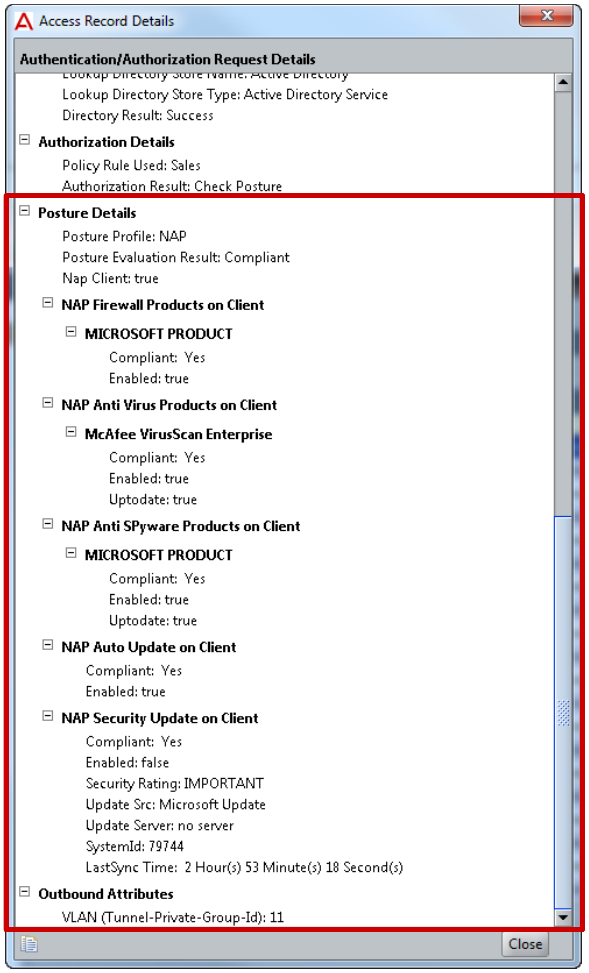
User-Name: AVAYALABS\salesuser
NAS-IP-Address: 192.168.10.30
NAS-Port: 1
Service-Type: 2
Framed-MTU: 1400
State: 26a93ed5ebd49108b3afef0a9cbf3966
Called-Station-Id: 00-23-68-2E-6F-08:AVAYA-IDE
Calling-Station-Id: E0-F8-47-0F-0E-14
NAS-Identifier: RFS4000-1
NAS-Port-Type: 19
Connect-Info: CONNECT -Mbps 802.11g
Message-Authenticator: 00e1b8f8e87a6fe13a9d34c2045b68c0
NAS-Port-Id: AVAYA-IDE
Symbol-Current-ESSID: AVAYA-IDE
Symbol-WLAN-Index:

Authentication Details

Outer Tunnel Type: PEAP
Outer Tunnel User: salesuser
Inner Tunnel Type: EAP_MSCHAPV2
Inner Tunnel User: salesuser
Authentication Result: Authenticated

Directory Details

Authentication Directory Store Type: Active Directory Service



Access Record Details

Authentication/Authorization Request Details

Lookup Directory Store Name: Active Directory
Lookup Directory Store Type: Active Directory Service
Directory Result: Success

Authorization Details

Policy Rule Used: Sales
Authorization Result: Check Posture

Posture Details

Posture Profile: NAP
Posture Evaluation Result: Compliant
Nap Client: true

NAP Firewall Products on Client

MICROSOFT PRODUCT

Compliant: Yes
Enabled: true

NAP Anti Virus Products on Client

McAfee VirusScan Enterprise

Compliant: Yes
Enabled: true
Uptodate: true

NAP Anti SPyware Products on Client

MICROSOFT PRODUCT

Compliant: Yes
Enabled: true
Uptodate: true

NAP Auto Update on Client

Compliant: Yes
Enabled: true

NAP Security Update on Client

Compliant: Yes
Enabled: false
Security Rating: IMPORTANT
Update Src: Microsoft Update
Update Server: no server
SystemId: 79744
LastSync Time: 2 Hour(s) 53 Minute(s) 18 Second(s)

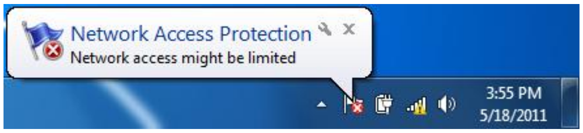
Outbound Attributes

VLAN (Tunnel-Private-Group-Id): 11

3.2.2 NAP Non-Compliant Users

The following section highlights the steps required to validate Wireless PEAP user authentication for Non-Compliant Windows 7 Enterprise workstation:

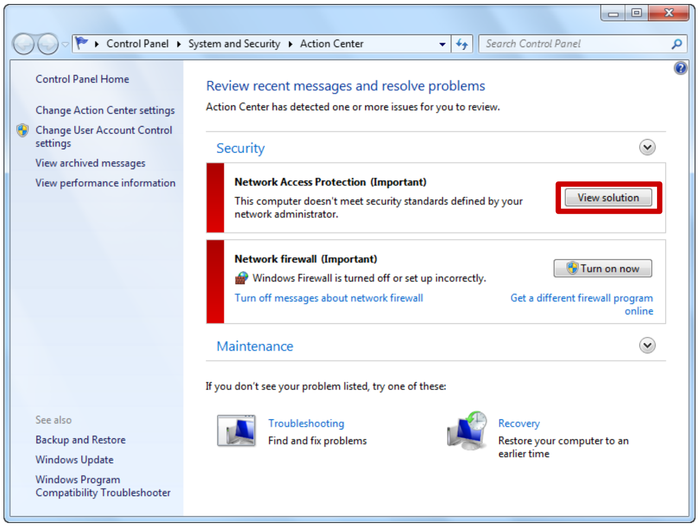
1 Login to Windows 7 using a domain username and password which will initiate wireless PEAP user authentication. In this example a domain user that is a member of the *Sales* group is used and the *Windows Firewall* and *Auto Remediation* have been *disabled*. A *Network Access Protection* dialog will be displayed in the task bar stating that *Network access might be limited*:



Network Access Protection

Network access might be limited

2 Open the Windows 7 *Action Center* then select *View Solution*:



Control Panel ▸ System and Security ▸ Action Center
Search Control Panel
Control Panel Home
Change Action Center settings
Change User Account Control settings
View archived messages
View performance information
See also
Backup and Restore
Windows Update
Windows Program Compatibility Troubleshooter

Review recent messages and resolve problems

Action Center has detected one or more issues for you to review.

Security

Network Access Protection (Important)

This computer doesn't meet security standards defined by your network administrator.

Network firewall (Important)

Windows Firewall is turned off or set up incorrectly.

Turn on now
Turn off messages about network firewall
Get a different firewall program online

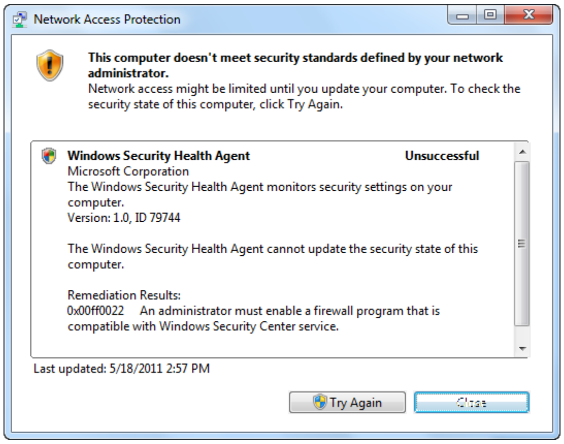
Maintenance

If you don't see your problem listed, try one of these:

Troubleshooting
Find and fix problems

Recovery
Restore your computer to an earlier time

3 A Network Access Protection dialog window outlining why the computer has failed posture evaluation and how to remediate the issue will be displayed:



Network Access Protection

This computer doesn't meet security standards defined by your network administrator.
Network access might be limited until you update your computer. To check the security state of this computer, click Try Again.

Windows Security Health Agent **Unsuccessful**
Microsoft Corporation
The Windows Security Health Agent monitors security settings on your computer.
Version: 1.0, ID 79744

The Windows Security Health Agent cannot update the security state of this computer.

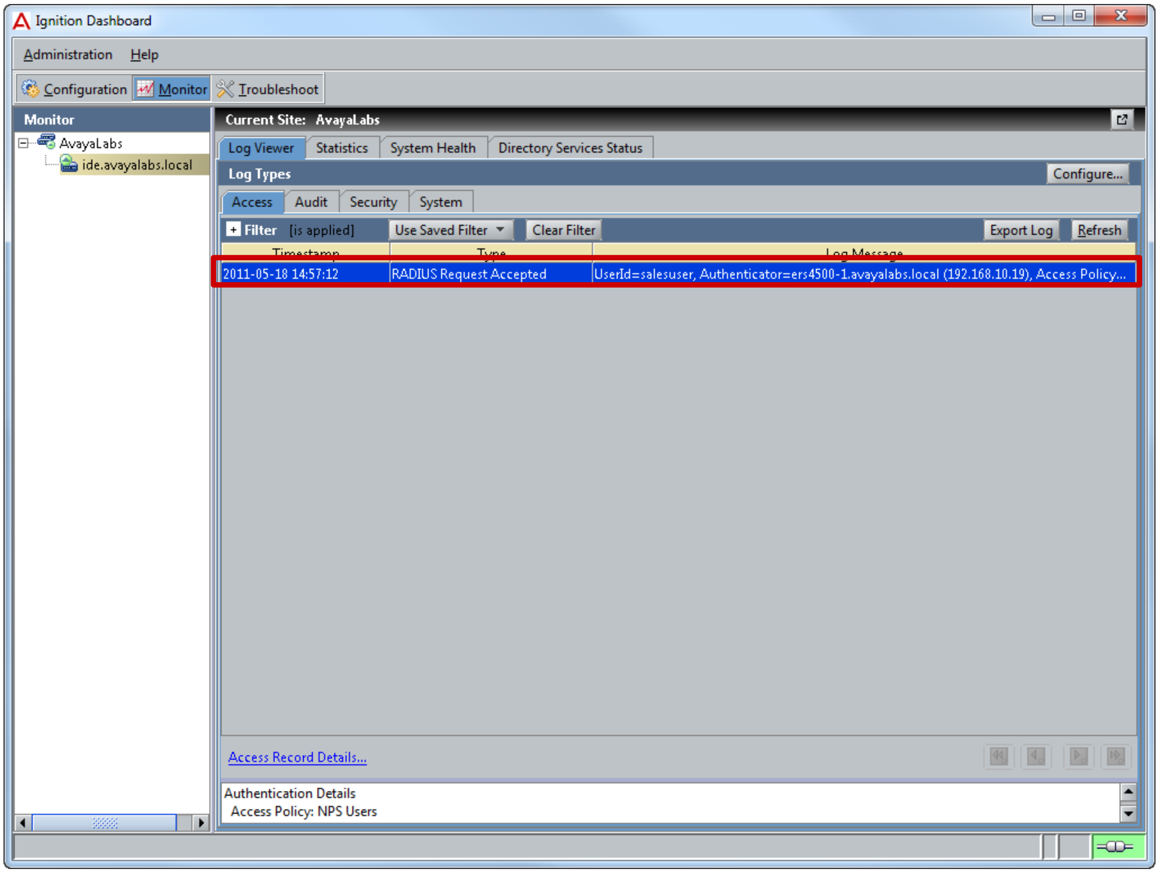
Remediation Results:
0x00ff0022 An administrator must enable a firewall program that is compatible with Windows Security Center service.

Last updated: 5/18/2011 2:57 PM

4 On the Avaya Ethernet Routing Switch view the dynamic VLAN assignment. In this example the sales user is *Non-Compliant* and will be assigned to the *Remediated* Mobility VLAN:

```
WC8180# show wireless client status

Total number of clients: 1


--------------------------------------------------------------------------------
     Client            Client        Associated      Mobility        Status
  MAC Address        IP Address      Controller        VLAN
----------------- --------------- --------------- --------------- -------------
E0:F8:47:0F:E0:14 192.168.14.100  192.168.10.30  Remediated      Authenticated
--------------------------------------------------------------------------------
```

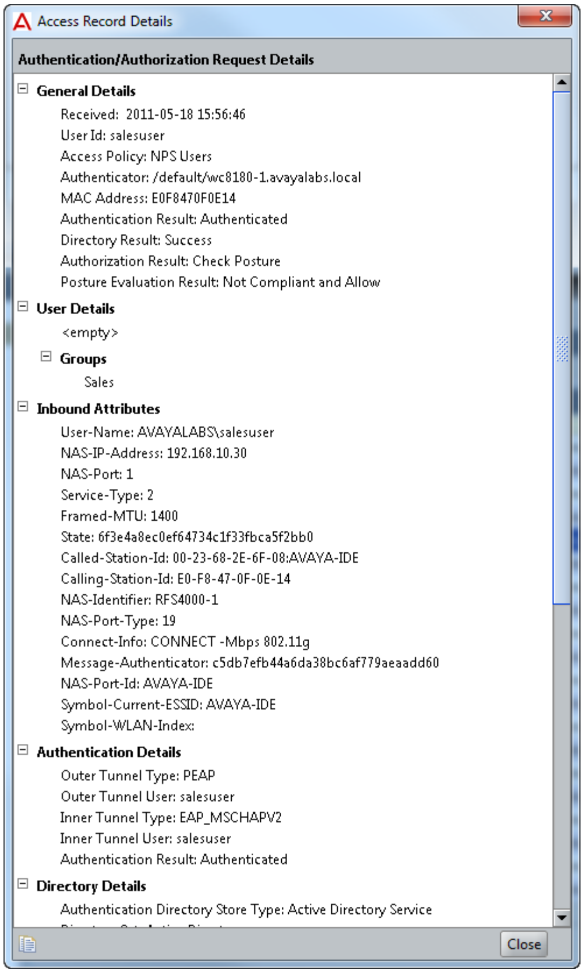
5 Using the *Ignition Dashboard* view the *Access Logs* by selecting *Monitor > Site-Name > Ignition-Server-Name > Log Viewer > Access*. A record showing a successful authentication and authorization for the sales user will be listed:



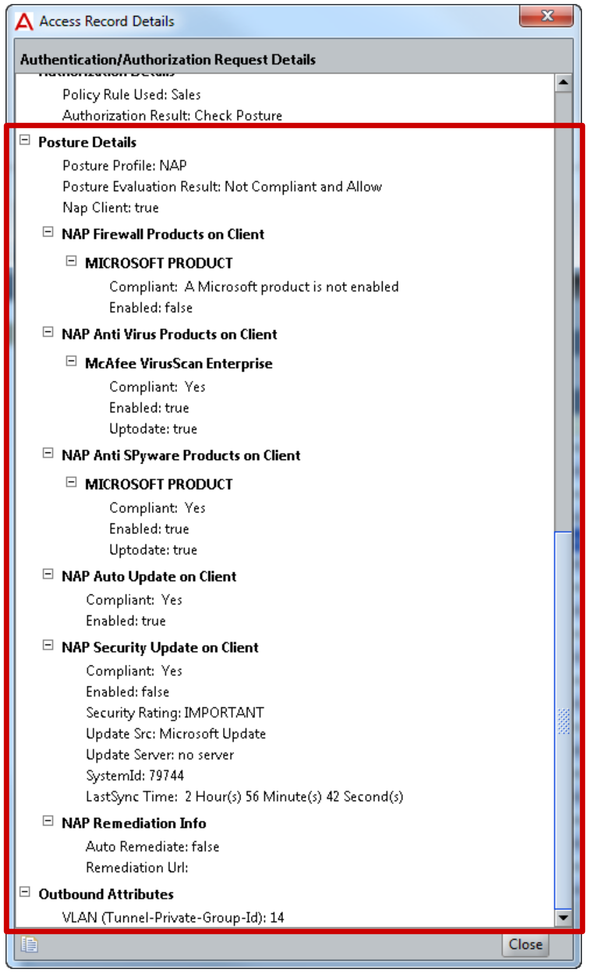
Timestamp	Type	Log Message
2011-05-18 14:57:12	RADIUS Request Accepted	UserId=salesuser, Authenticator=ers4500-1.avayalabs.local (192.168.10.19), Access Policy...

Authentication Details
Access Policy: NPS Users

5 Double-click on the computer authentication log entry to view the authentication and authorization details. The *Posture Details* section in the *Access Record* will highlight the posture evaluation results for the sales user, why posture evaluation failed and the assigned VLAN:



```
Authentication/Authorization Request Details
⊟ General Details
      Received:  2011-05-18 15:56:46
      User Id: salesuser
      Access Policy: NPS Users
      Authenticator: /default/wc8180-1.avayalabs.local
      MAC Address: E0F8470F0E14
      Authentication Result: Authenticated
      Directory Result: Success
      Authorization Result: Check Posture
      Posture Evaluation Result: Not Compliant and Allow
⊟ User Details
      <empty>
  ⊟ Groups
        Sales
⊟ Inbound Attributes
      User-Name: AVAYALABS\salesuser
      NAS-IP-Address: 192.168.10.30
      NAS-Port: 1
      Service-Type: 2
      Framed-MTU: 1400
      State: 6f3e4a8ec0ef64734c1f33fbca5f2bb0
      Called-Station-Id: 00-23-68-2E-6F-08:AVAYA-IDE
      Calling-Station-Id: E0-F8-47-0F-0E-14
      NAS-Identifier: RFS4000-1
      NAS-Port-Type: 19
      Connect-Info: CONNECT -Mbps 802.11g
      Message-Authenticator: c5db7efb44a6da38bc6af779aeaadd60
      NAS-Port-Id: AVAYA-IDE
      Symbol-Current-ESSID: AVAYA-IDE
      Symbol-WLAN-Index:
⊟ Authentication Details
      Outer Tunnel Type: PEAP
      Outer Tunnel User: salesuser
      Inner Tunnel Type: EAP_MSCHAPV2
      Inner Tunnel User: salesuser
      Authentication Result: Authenticated
⊟ Directory Details
      Authentication Directory Store Type: Active Directory Service
```



```
Authentication/Authorization Request Details
      Policy Rule Used: Sales
      Authorization Result: Check Posture
⊟ Posture Details
      Posture Profile: NAP
      Posture Evaluation Result: Not Compliant and Allow
      Nap Client: true
  ⊟ NAP Firewall Products on Client
    ⊟ MICROSOFT PRODUCT
          Compliant:  A Microsoft product is not enabled
          Enabled: false
  ⊟ NAP Anti Virus Products on Client
    ⊟ McAfee VirusScan Enterprise
          Compliant:  Yes
          Enabled: true
          Uptodate: true
  ⊟ NAP Anti SPyware Products on Client
    ⊟ MICROSOFT PRODUCT
          Compliant:  Yes
          Enabled: true
          Uptodate: true
  ⊟ NAP Auto Update on Client
        Compliant:  Yes
        Enabled: true
  ⊟ NAP Security Update on Client
        Compliant:  Yes
        Enabled: false
        Security Rating: IMPORTANT
        Update Src: Microsoft Update
        Update Server: no server
        SystemId: 79744
        LastSync Time:  2 Hour(s) 56 Minute(s) 42 Second(s)
  ⊟ NAP Remediation Info
        Auto Remediate: false
        Remediation Url:
⊟ Outbound Attributes
      VLAN (Tunnel-Private-Group-Id): 14
```

4. Troubleshooting

The following section highlights some common issues and resolutions when deploying Active Directory computer and user authentication:

4.1 Authentication

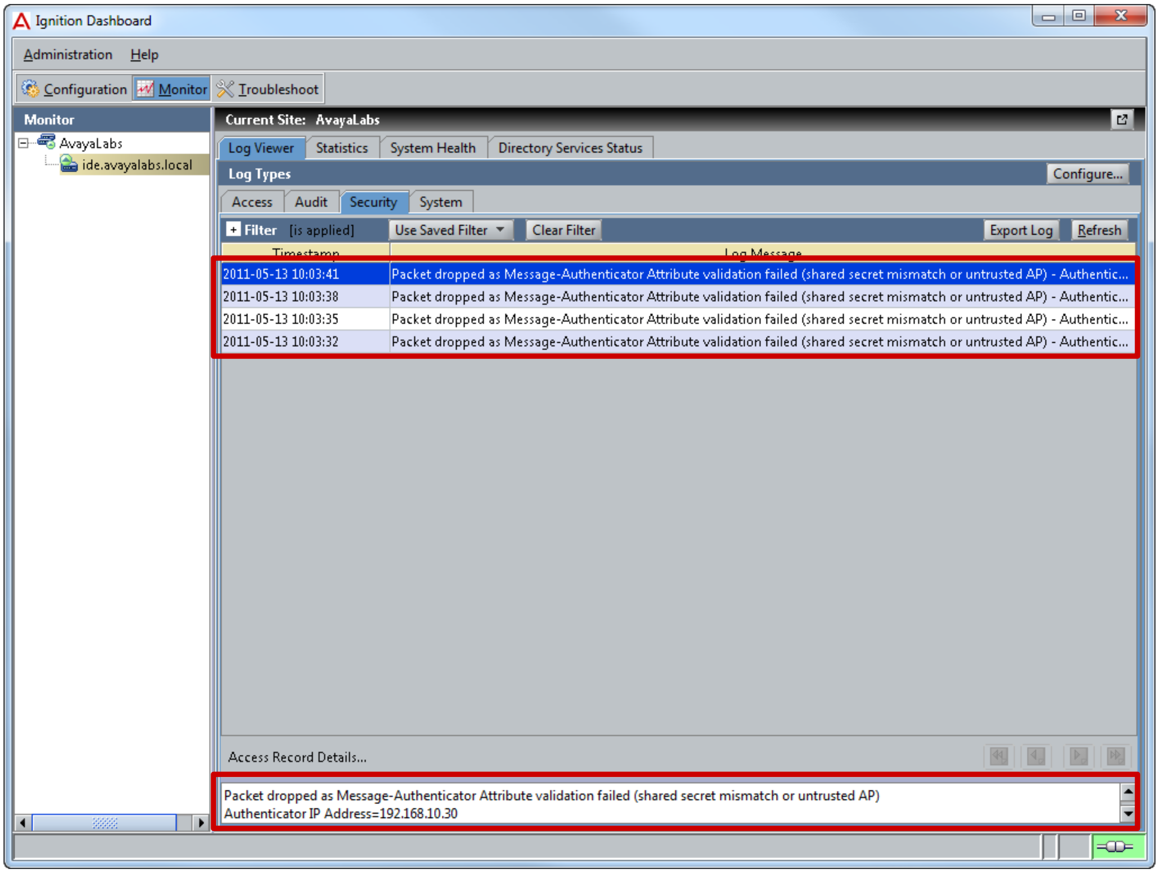
4.1.1 Authenticator Trust

Problem Description:

One of the most common causes of failed authentication attempts is a mismatched RADIUS shared secret, authenticator IP address mismatch or no authenticator entry. When an authentication request is received by the Ignition Server, the Ignition Server will verify that the authenticator is trusted and the RADIUS shared secret matches.

If an Authenticator entry cannot be located for the source IP address that the RADIUS authentication request was received from or the RADIUS shared secret is mismatched, the Ignition Server will drop the authentication request.

Using the Ignition Dashboard by select ***Monitor > Site-Name > Ignition-Server-Name > Log Viewer > Security***. A ***Packet dropped as Message-Authenticator Attribute validation failed*** log entry will be displayed:



Timestamp	Log Message
2011-05-13 10:03:41	Packet dropped as Message-Authenticator Attribute validation failed (shared secret mismatch or untrusted AP) - Authentic...
2011-05-13 10:03:38	Packet dropped as Message-Authenticator Attribute validation failed (shared secret mismatch or untrusted AP) - Authentic...
2011-05-13 10:03:35	Packet dropped as Message-Authenticator Attribute validation failed (shared secret mismatch or untrusted AP) - Authentic...
2011-05-13 10:03:32	Packet dropped as Message-Authenticator Attribute validation failed (shared secret mismatch or untrusted AP) - Authentic...

```
Packet dropped as Message-Authenticator Attribute validation failed (shared secret mismatch or untrusted AP)
Authenticator IP Address=192.168.10.30
```

Resolution:

1. Using the Ignition Dashboard select ***Configuration > Site-Name > Site-Configuration > Authenticators > default***. Verify the Ignition Server has an Authenticator entry for the Avaya Wireless LAN Controller 8180 or Avaya Ethernet Routing Switch(es).

2. If an Authenticator entry is present, verify the ***IP Address*** for the Authenticator record is correct:

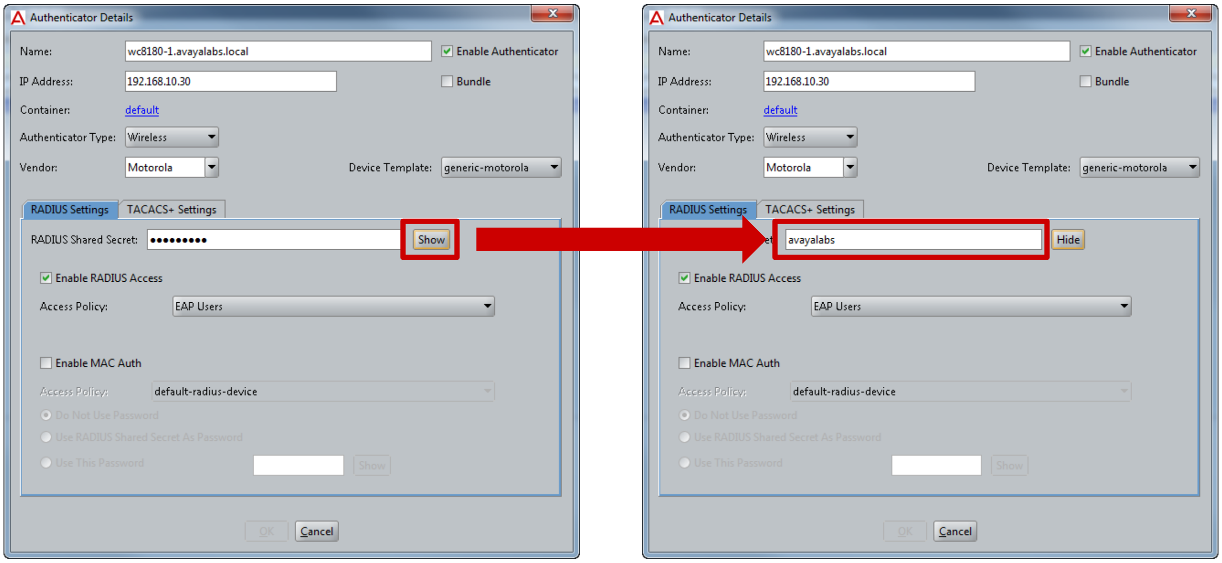
    a. The Avaya Wireless LAN Controller 8180 uses the ***Interface-IP*** address to originate RADIUS authentication and accounting requests.

    b. An individual Avaya Ethernet Routing Switch uses the ***Switch Management*** IP address to originate RADIUS authentication and accounting requests.

    c. A stack of Avaya Ethernet Routing Switches uses the ***Stack Management*** IP address to originate RADIUS authentication and accounting requests.

3. If the Authenticator entry is present and the IP Address is correct, reset the RADIUS shared secret on the Wireless LAN Controller 8180 or Ethernet Routing Switch(es) to match the RADIUS Shared Secret defined in the Authenticator record.

    TIP – You can view the RADIUS Shared Secret within the Authenticator Details window by selecting ***Show*** next to the defined ***RADIUS Shared Secret***:



Authenticator Details

Name: wc8180-1.avayalabs.local ☑ Enable Authenticator

IP Address: 192.168.10.30 □ Bundle

Container: default

Authenticator Type: Wireless

Vendor: Motorola Device Template: generic-motorola

RADIUS Settings | TACACS+ Settings

RADIUS Shared Secret: ••••••••• Show

☑ Enable RADIUS Access

Access Policy: EAP Users

□ Enable MAC Auth

Access Policy: default-radius-device

○ Do Not Use Password

○ Use RADIUS Shared Secret As Password

○ Use This Password Show

OK Cancel

Authenticator Details

Name: wc8180-1.avayalabs.local ☑ Enable Authenticator

IP Address: 192.168.10.30 □ Bundle

Container: default

Authenticator Type: Wireless

Vendor: Motorola Device Template: generic-motorola

RADIUS Settings | TACACS+ Settings

avayalabs Hide

☑ Enable RADIUS Access

Access Policy: EAP Users

□ Enable MAC Auth

Access Policy: default-radius-device

○ Do Not Use Password

○ Use RADIUS Shared Secret As Password

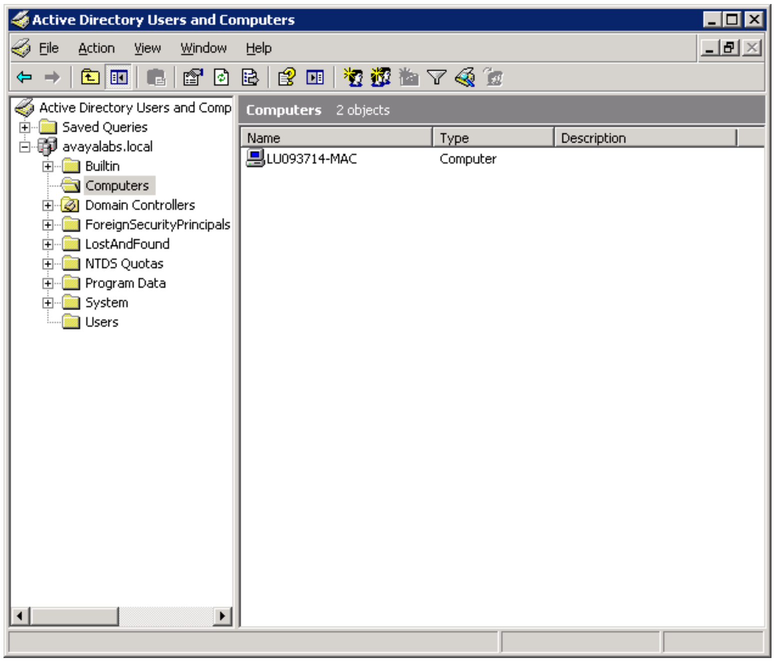
○ Use This Password Show

OK Cancel

4.1.2 NTLM Authentication

Problem Description:

PEAP uses MSCHAPv2 as an inner authentication protocol which is not natively supported by LDAP. To overcome this limitation the Ignition Server employs NTLM authentication and creates a computer object in the ***Computers*** container in the Active Directory tree. If the computer object is not present, MSCHAPv2 authentication will not be possible and authentication will fail.

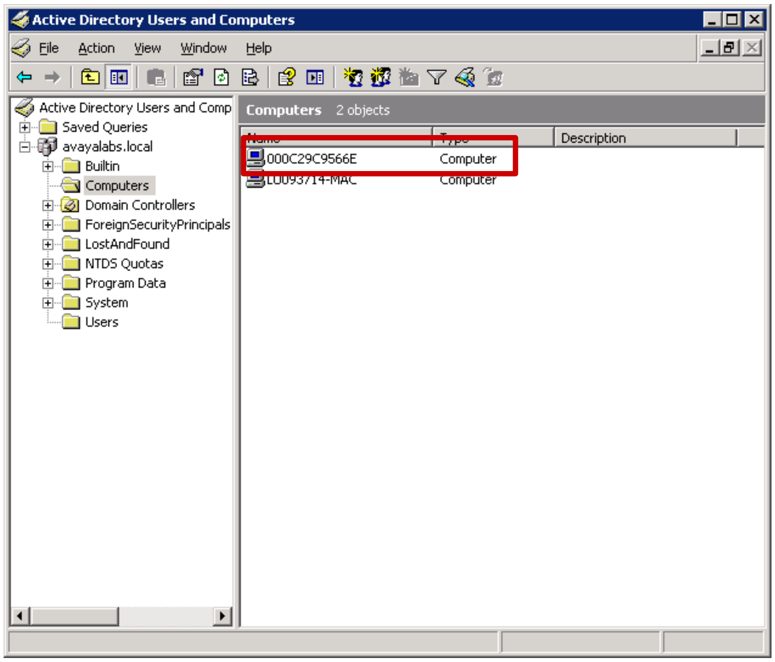


Name	Type	Description
LU093714-MAC	Computer	

Resolution:

If MSCHAPv2 authentication is failing:

1. Check the ***Computers*** container in Active Directory and look for the Ignition Server computer object. The Name will either be the MAC address of the Ignition Server or the resolvable hostname.
2. If the computer object is missing, assign the Ignition Server bind user account with the necessary permissions required to allow it to ***Create Computer Objects*** in the domain (http://technet.microsoft.com/en-us/library/cc754478.aspx). Alternatively assign the account to the Domain Admins group.
3. Initiate an MSCHAPv2 authentication request. If the Ignition Server bind user account has the necessary permissions it will create a computer object I the Computers container.



- Active Directory Users and Comp
  - Saved Queries
  - avayalabs.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - LostAndFound
    - NTDS Quotas
    - Program Data
    - System
    - Users

Computers 2 objects

Name	Type	Description
000C29C9566E	Computer	
LL0093714-MAC	Computer	

4.1.3 EAPOL Quiet Period

Each Ethernet port on an Avaya Ethernet Routing Switch supports various EAPOL timers. Most EAPOL deployments can utilize the default timer values; however there may be some instances where certain timers need to be modified to address authentication performance issues.

Problem Description:

When an EAPOL authentication attempt fails, the Avaya Ethernet Routing Switch will wait for the ***Quiet Period*** before a new authentication attempt is accepted. While the Ethernet host may attempt to re-authenticate, the Avaya Ethernet Routing Switch will not accept the new authentication until the ***Quiet Period*** expires which can impact the Windows workstations ability to access the network. For example a user on a Windows host that fails computer authentication will have to wait 60 seconds before user authentication can occur and access to the network is permitted.

Parameter	Default Value	Description
Quiet Period	**60 (s)**	Time interval between an authentication failure and the start of a new authentication attempt.

Resolution:

1. If users are experiencing long authentication times due to initial authentication failures, consider reducing the ***Quiet Period*** to***10*** seconds (or lower) to minimize the impact on the user and provide a transparent logon experience.

4.1.4 EAPOL Re-Authentication

Problem Description:

When re-authentication is enabled on an EAPOL port, the Avaya Ethernet Routing Switch will initiate re-authentication when the re-authentication period expires. Re-authentication is a useful feature as it provides a mechanism to disconnect users when their Active Directory accounts are disabled or if time and date authorization attributes are applied to users. Without re-authentication, users with expired or disabled credentials will remain connected to the network and time and date authorization restrictions will never be applied to users.

Parameter	Default Value	Description
Re-Authentication Period	**3600 (s)**	Time interval between successive re-authentications.

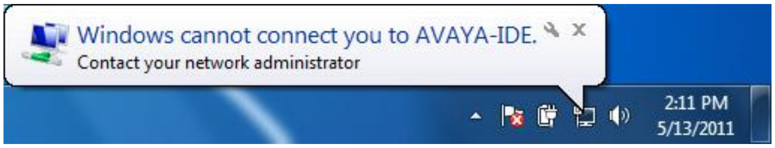
Resolution:

1. If users are remaining authenticated after their Active Directory accounts are disabled or time and date permissions expire, enabled re-authentication on the EAPOL ports.
2. When implementing time and date authorization policies are being deployed, consider reducing the ***Re-Authentication Period*** to ***15*** minutes. This will ensure users are disconnected within reason while balancing the increase in authentication requests.

4.2 CA Root Certificates

Problem Description:

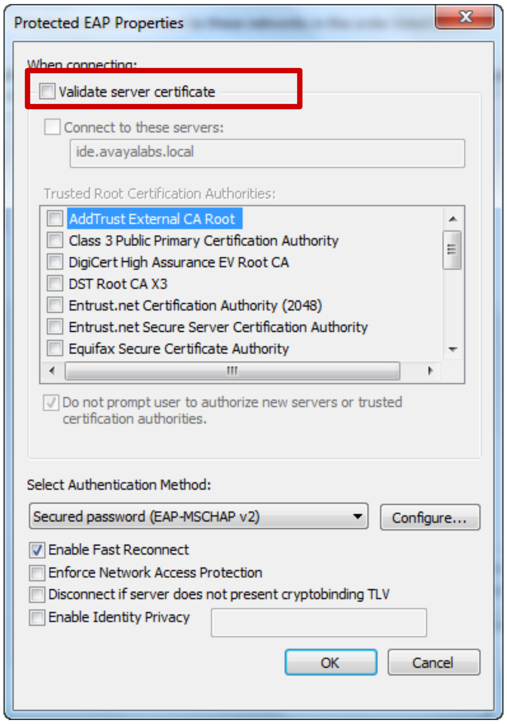
By default during PEAP authentication a Windows workstations will attempt to validate the signed server certificate installed on the RADIUS authentication server using the corresponding CA root certificate installed in the users or computers ***Trusted Root Certificate Authorities*** store. If no CA root certificate is found, the TLS session will not be trusted and PEAP authentication will fail.



Windows cannot connect you to AVAYA-IDE.
Contact your network administrator

Resolution:

1. Temporarily uncheck the ***Protected EAP Properties*** option ***Validate server certificate***. If the user's credentials are valid this will allow the user to authenticate and connect to the network.
2. Install the appropriate CA root certificate following the procedure outlined in ***Section 2.6.1***. If the machine is a member of the domain you may also use the MMC certificate snap-in to renew the certificate.
3. Once the CA root certificate has been installed, re-enable the ***Protected EAP Properties*** option ***Validate server certificate***.

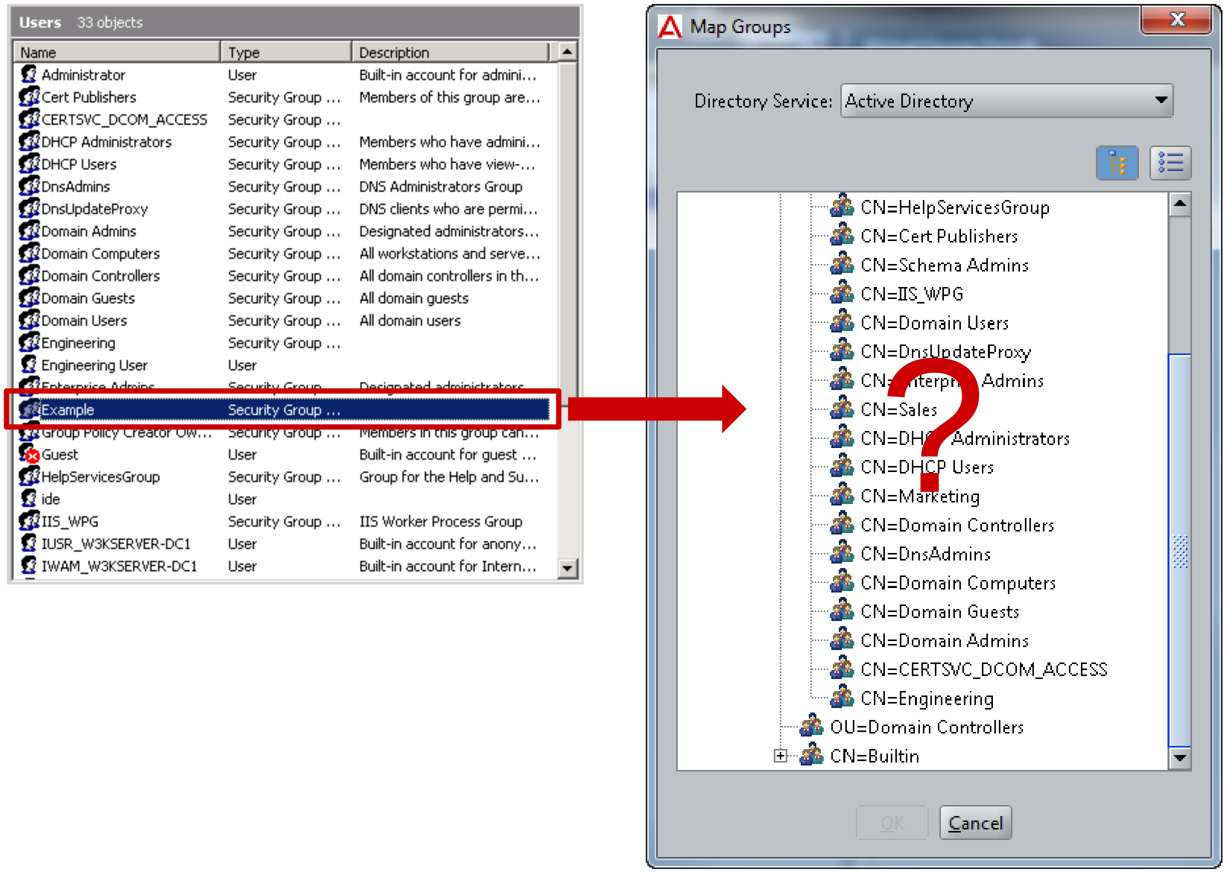


Protected EAP Properties
When connecting:
☐ Validate server certificate
☐ Connect to these servers:
ide.avayalabs.local
Trusted Root Certification Authorities:
☐ AddTrust External CA Root
☐ Class 3 Public Primary Certification Authority
☐ DigiCert High Assurance EV Root CA
☐ DST Root CA X3
☐ Entrust.net Certification Authority (2048)
☐ Entrust.net Secure Server Certification Authority
☐ Equifax Secure Certificate Authority
☑ Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
☑ Enable Fast Reconnect
☐ Enforce Network Access Protection
☐ Disconnect if server does not present cryptobinding TLV
☐ Enable Identity Privacy
OK
Cancel

4.3 Active Directory Cache

Problem Description:

The Ignition Server maintains a cache for each Directory Services groups and attributes. When a new group is added to Active Directory it might take some time for the Active Directory cache to be updated on the Ignition Server which may result in new groups not being visible when attempting to map a Virtual Group to an Active Directory group.



Users 33 objects

Name	Type	Description
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Members of this group are...
CERTSVC_DCOM_ACCESS	Security Group ...	
DHCP Administrators	Security Group ...	Members who have admini...
DHCP Users	Security Group ...	Members who have view-...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Engineering	Security Group ...	
Engineering User	User	
Enterprise Admins	Security Group	Designated administrators
Example	Security Group ...	
Group Policy Creator Ow...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServicesGroup	Security Group ...	Group for the Help and Su...
ide	User	
IIS_WPG	Security Group ...	IIS Worker Process Group
IUSR_W3KSERVER-DC1	User	Built-in account for anony...
IWAM_W3KSERVER-DC1	User	Built-in account for Intern...

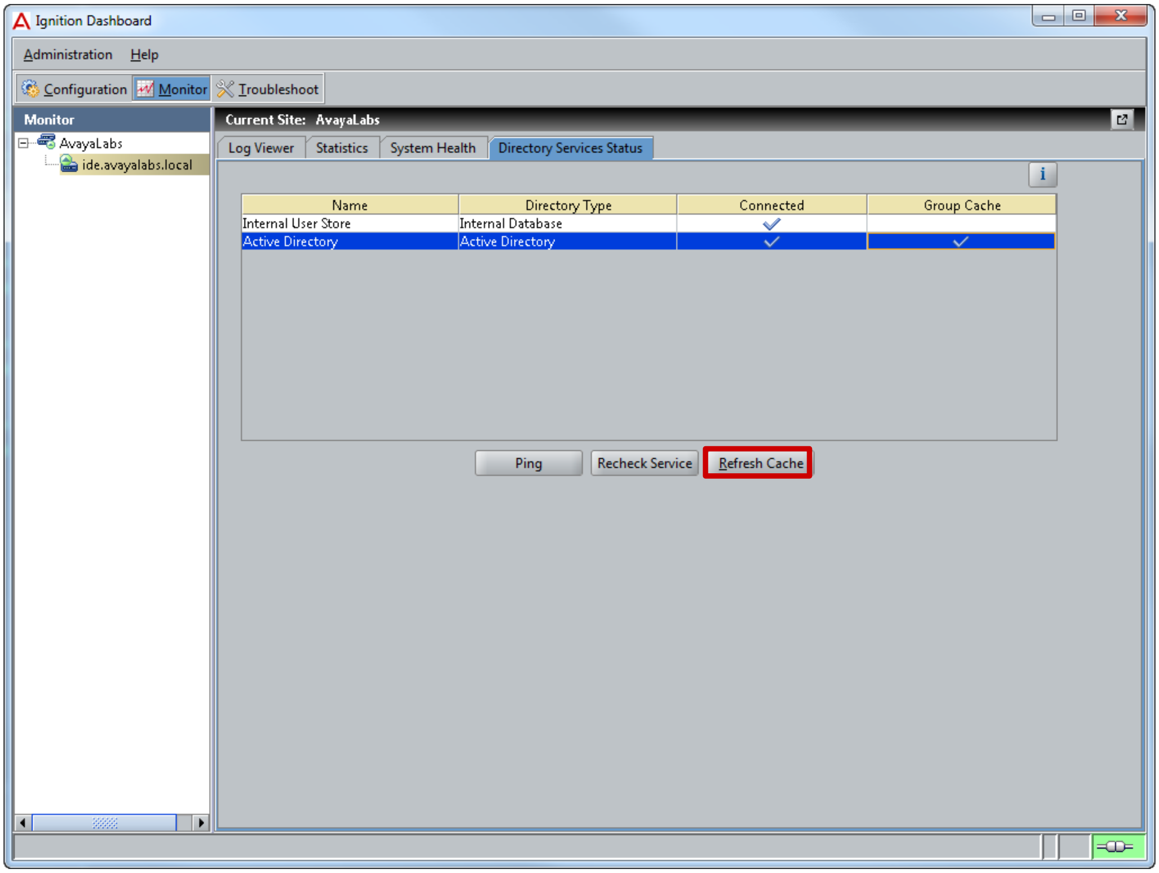
Map Groups

Directory Service: Active Directory

- CN=HelpServicesGroup
- CN=Cert Publishers
- CN=Schema Admins
- CN=IIS_WPG
- CN=Domain Users
- CN=DnsUpdateProxy
- CN=Enterprise Admins
- CN=Sales
- CN=DHCP Administrators
- CN=DHCP Users
- CN=Marketing
- CN=Domain Controllers
- CN=DnsAdmins
- CN=Domain Computers
- CN=Domain Guests
- CN=Domain Admins
- CN=CERTSVC_DCOM_ACCESS
- CN=Engineering
- OU=Domain Controllers
- CN=Builtin

Resolution:

If an Active Directory group is not visible on the Ignition Server, you can force an Active Directory cache using the Ignition Dashboard by selecting ***Monitor > Ignition-Server-Name > Directory Services Status > Refresh Cache***.



Current Site: AvayaLabs

Name	Directory Type	Connected	Group Cache
Internal User Store	Internal Database	✓	
Active Directory	Active Directory	✓	✓

5. Reference Documentation

Publication Number	Document Title
NN47280-500	Avaya Identity Engines Ignition Server Configuration Guide
NN47205-505	Avaya Ethernet Routing Switch 4500 Series Configuration – Security
NN47251-500	Avaya WLAN 8100 Configuration – WC8180 (CLI)