>BUSINESS MADE **SIMPLE**

NORTEL

Nortel Secure Network Access 2.0
Engineering

> Nortel Secure Network Access 2.0 802.1X Authentication with Nortel Health Agent and Microsoft Network Access Protection Endpoint Inspection Technical Configuration Guide

Enterprise Business Solutions
Document Date: August 5, 2008
Document Number: NN48500-567
Document Version: 2.0

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at www.nortel.com.

Abstract

This document provides an overview on how to configure the Nortel Secure Network Access Switch to authenticate and provide inspection of Microsoft Windows XP and Vista workstations running the Microsoft EAP Quarantine Enforcement and Nortel Health Agent Clients.

Revision Control

No	Date	Version	Revised by	Remarks
1	07/09/2008	1.0	EBS	Initial draft and first release internally. Approved by PLM
2	08/05/2008	2/0	EBS	PLM approved for external release.

Table of Contents:

Figures:

Tables:

Document Updates:

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 Nortel devices are displayed in a Lucinda Console font:

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

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

1. Overview:

This document provides an overview on how to configure the Nortel Secure Network Access Switch to authenticate and provide end-point inspection of wired Microsoft Windows XP and Vista workstations running the Microsoft EAP Quarantine Enforcement Client and Nortel Health Agent Client.

Microsoft Network Access Protection (NAP) delivers a new set of operating system components that provide a platform for protected access to private networks. The NAP platform provides an integrated way of detecting the state of a network client that is attempting to connect to a network and restricting the access of the network client until the policy requirements for connecting to the network have been met.

The NSNA/NAP interoperability architecture allows customers to deploy both the NSNA solution and the Network Access Protection (NAP) concurrently. These components interoperate, allowing customers to enforce security policies for network access using both NSNA and NAP. This architecture allows deployment of NAP clients with or without a Windows 2008 Server based Network Policy Server (NPS) present on the network. If the Microsoft NPS server is present, it will be consulted and its response will be used in a configurable way to augment the access decision made by the SNAS. If a Microsoft NPS server is not in place, the Secure Network Access Switch can communicate with the NAP client components.

This configuration guide describes a solution that does not use or require a Windows 2008 Server with NPS. Integrating Windows 2008 Server with NPS can be performed by specifying a "Remote Policy Server" in the NAP settings on the Secure Network Access Switch.

1.1 NHA / NAP 802.1X Enforcement Overview:

This section provides a brief overview of how 802.1X enforcement functions on the Nortel Secure Network Access Switch with the Microsoft Network Access Protection and Nortel Health Agent Clients.

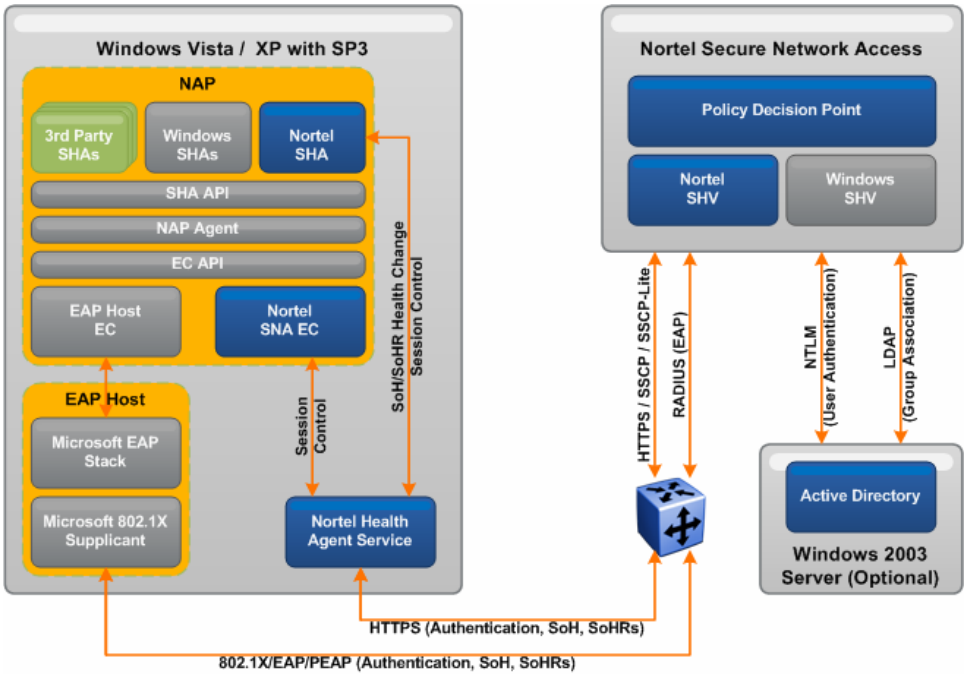


Figure 1.1 – NHA / NAP 802.1X Enforcement Framework

1.1.1 Authentication Process:

1. The Windows XP / Vista workstation initiates 802.1X authentication.
2. Using Protected EAP the workstation sends its user and/or computer authentication credentials to the Nortel Secure Network Access Switch providing RADIUS services for the Nortel Ethernet Switch. The credentials are either authenticated locally or using NTLM against authenticated against Active Directory.
3. If the authentication credentials are not valid, the 802.1X connection attempt is terminated.
4. If the authentication credentials are valid, the Network Policy Server on the Nortel Secure Network Access Switch requests the health state from the Windows XP / Vista workstation.
5. The Windows XP / Vista workstation sends the Network Access Protection and Nortel Health Agent health state information to the Nortel Secure Network Access Switch.
6. The Nortel Secure Network Access Switch evaluates the health state information of the Windows XP / Vista workstation, determines whether the workstation is compliant, and forwards a RADIUS Access Accept with the appropriate VLAN information to the Nortel Ethernet Switch.
   a. If the workstation is non-compliant, the Nortel Secure Network Access Switch forwards RADIUS return attributes to the Nortel Ethernet Switch which places the workstation in a remediated Yellow VLAN.

      Optionally the Network Policy Server may re-provision the workstation with the required updates to be compliant with health policy. If successful the workstation restarts 802.1X authentication and sends its updated health state information to the Network Policy Server. The Nortel Secure Network Access Switch forwards RADIUS return attributes to the Nortel Ethernet Switch which places the workstation in an un-restricted Green VLAN.
   b. If the Windows XP / Vista workstation is compliant, the Nortel Secure Network Access Switch forwards RADIUS return attributes to the Nortel Ethernet Switch which places the workstation in an un-restricted Green VLAN.

1.1.2 Health Agent States:

As shown in figure 1.1.2.1 the Microsoft EAP Quarantine Enforcement Client can be in two states depending on the workstation's compliance state compared to the policy defined on the Network Policy Server.

Taskbar Icon	Client State Description
	Policy checks have been performed and the Microsoft EAP Quarantine Enforcement Client is in a non-compliant state. In this state the workstation will be placed into a Yellow remediated VLAN.
	Policy checks have been performed and the Microsoft EAP Quarantine Enforcement Client is in a compliant state. Assuming the Nortel Health Agent policies are compliant the workstation will be placed into an unrestricted Green VLAN.

Figure 1.1.2.1 – Microsoft NAP Agent States

As shown in figure 1.1.2.2 the Nortel Health Agent may be in one of three states depending on the workstations compliance state compared to the Nortel Health Policy assigned to the group.

Taskbar Icon	Client State Description
	No policy checks have been performed and the Nortel Health Agent is idle state.
	Policy checks have been performed and the Nortel Health Agent is in non-compliant state. In this state the workstation will be placed into a Yellow remediated VLAN.
	Policy checks have been performed and the Nortel Health Agent is in compliant state. Assuming the Microsoft policies are compliant the workstation will be placed into an unrestricted Green VLAN.

Figure 1.1.2.2 – Nortel Health Agent States

1.1.3 VLAN States:

The Nortel Secure Network Access Switch uses standard IETF RADIUS return attributes upon successful PEAP authentication to place workstations into the appropriate VLAN based on Microsoft Network Access Protection and Nortel Health Agent compliance states.

During configuration Green and Yellow VLAN Names and IDs are created on the Nortel Secure Network Access Switch. These VLANs are then combined with Filters in an Extended Profile to define the VLAN membership based on NAP and NHA policy compliance state. Table 1.1.3 shows the standard RADIUS return attributes forwarded by the Nortel Secure Network Access Switch to the Nortel Ethernet Switch to assign the VLANs:

Attribute Name	Vendor-ID	Attribute-ID	Value
Tunnel-Type	0	64	13 – (Virtual LANs)
Tunnel-Medium-Type	0	65	6 – (802)
Tunnel-Private-Group-ID	0	81	Numeric VLAN-ID assigned to the port based on compliance state

Table 1.1.3 – Standard RADIUS Return Attributes

A workstation with the Microsoft Network Access Protection and Nortel Health Agent clients may be in one of three VLAN states depending on authentication status and policy compliance state:

- Pre-Authentication – Windows XP / Vista workstations that have not performed PEAP user or computer authentication will be in an isolated state and not assigned a VLAN. The only communication that may occur between the workstation and Switch is EAP authentication and no other traffic will be passed.
- Non-Compliant – Windows XP / Vista workstations that have performed PEAP user and/or computer authentication but fail policy checks will be placed into a remediated Yellow VLAN. The remediated VLAN is intended to provide restricted access to the network to allow the workstation to obtain the required updates to become compliant. Once compliant the workstation is transitioned to the un-restricted Green VLAN.
- Compliant – Windows XP / Vista workstations that have performed PEAP user and/or computer authentication and pass policy checks will be placed into an unrestricted Green VLAN with full access to the network. If the workstations compliance state changes the workstation is transitioned to the remediated Yellow VLAN.

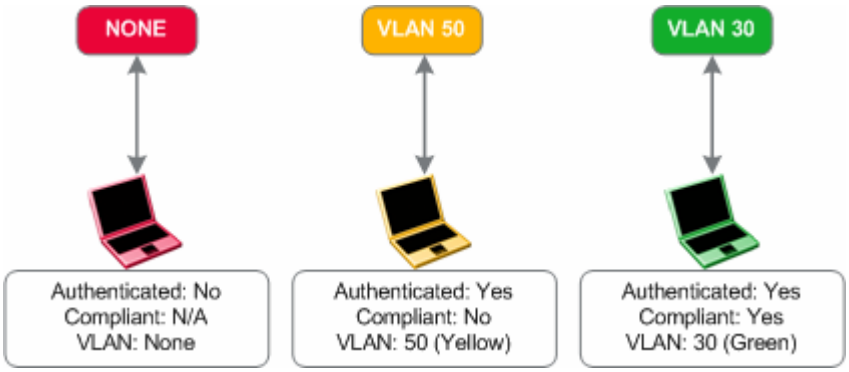


Figure 1.1.3 – VLAN States

1.2 Topology:

Figure 1.2 shows the topology that will be used in this configuration guide using the following Nortel and Microsoft platforms:

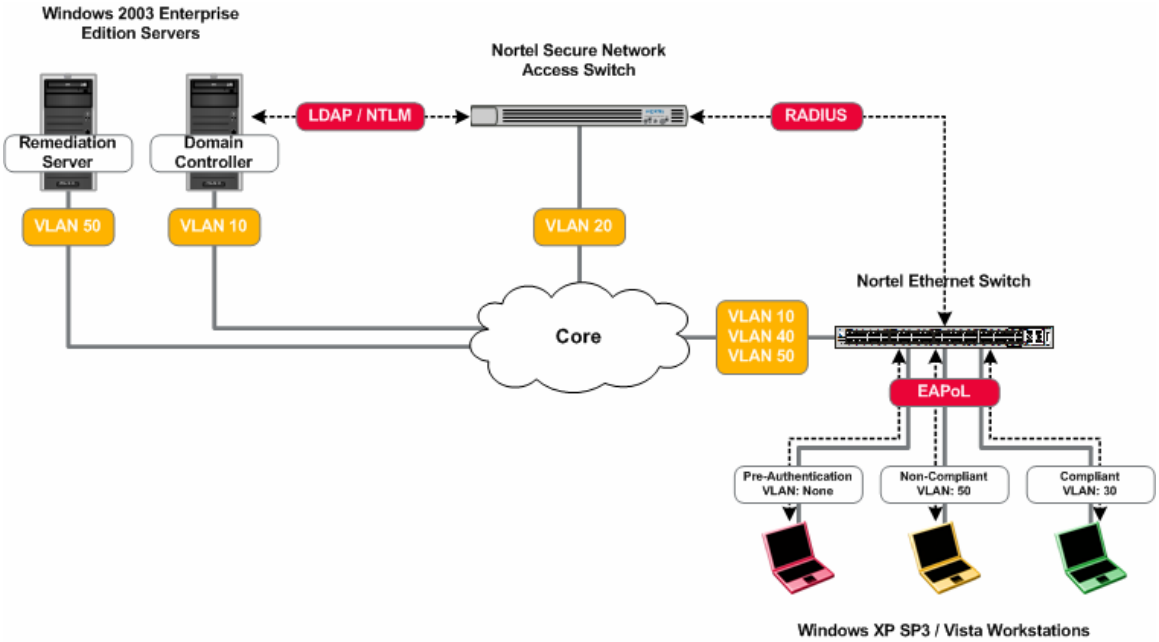


Figure 1.2 – Topology

- The Nortel Secure Network Access Switch will be configured to support PEAP Authentication from the Windows XP and Vista workstations and authenticate the users against Active Directory using NTLM. Additionally the Nortel Secure Network Access Switch will be configured to provide NAP / NHA compliance verification and assign the users to unrestricted (Green) or restricted (Yellow) VLAN based on the workstations compliance state.
- The Nortel Ethernet Routing Switch will be configured to support EAPOL clients and forward RADIUS authentication requests to the Nortel Secure Network Access Switch. Additionally the Green and Yellow VLANs will be created on the switch which will be dynamically assigned to EAPOL NAP users based on compliance state using standard IETF RADIUS return attributes from the Nortel Secure Network Access Switch.
- The Microsoft Windows 2003 Server will be configured with the appropriate Active Directory User and Group objects to support user authentication and group associations. During authentication the Nortel Secure Network Access Switch will perform NTLM user authentication against Active Directory and using LDAP lookup will determine the user's group membership which will determine the VLAN outcome based on compliance state.
- The Microsoft Windows Workstations will be configured to perform Single Sign-On PEAP authentication to the Nortel Ethernet Switch as well as exchange NAP compliance state with the Nortel Secure Network Access Switch. Based on NAP / NHA compliance state the workstation will either be placed in a remediated VLAN (Yellow) or unrestricted VLAN (Green).

This document provides configuration details for Nortel and Microsoft components shown in figure 1.2 but does not address installation of the core Windows operating systems or services such as Active Directory, DHCP, DNS or Certificate Services. These topics are out of the scope of this document and the reader should reference the appropriate vendor documentation.

1.3 Pre-Requisites:

This document makes the following assumptions in regards to the Network Infrastructure, Windows 2003 server, Windows XP workstation and Windows Vista workstations:

1. A Windows 2003 Advanced or Enterprise Server is installed with the following:
    a. Latest service pack and updates installed
    b. The following services have been installed:
        i. Active Directory (Domain Controller).
        ii. Certificate Services (Enterprise Root CA).
        iii. Domain Name Services (DNS).
        iv. Dynamic Host Configuration Protocol (DHCP).
        v. Internet Information Services (IIS).
    c. A server certificate with public key has been issued from the Enterprise Root CA and has been exported as a PKCS#12 file.
    d. A CA root certificate has been issued from the Enterprise Root CA and has been exported to a file.
    e. The server can ping the Nortel Secure Network Access Switch.
2. Windows XP / Vista Workstations with the following:
    a. Latest service pack and updates installed.
    b. The workstation is a member of the Domain.
    c. A CA Root certificate issued from the Enterprise Root CA is installed.
    d. The Nortel Health Agent with appropriate Java Runtime Engine is installed and operational on the Workstation.
3. A core routing switch is in place and has been configured to provide inter-VLAN routing and DHCP forwarding services.

2. Configuration:

2.1 Nortel Secure Network Access Switch:

This section provides configuration steps required to configure a Nortel Secure Network Access Switch to support Microsoft Network Access Protection EAP clients. For this section the following configuration steps will be performed:

1. Base Configuration (Section 2.1.1)
2. VLANs (Section 2.1.2)
3. Certificates (Section 2.1.3)
4. Authentication Servers (Section 2.1.4)
5. Filters (Section 2.1.5)
6. Groups (Section 2.1.6)
7. Extended Profiles (Section 2.1.7)
8. RADIUS Server (Section 2.1.8)
9. Network Access Protection (Section 2.1.9)
10. Nortel Health Agent Policy (Section 2.1.10)

2.1.1 Base Configuration:

The following baseline configuration will performed on the Secure Network Access Switch:

- IP Addressing – The Interface, Management and Virtual IP Addresses will be defined.
- DNS – DNS Server IP Address and Domain Name will be defined.
- Time – The Timezone and NTP Server IP Address will be defined.
- Management – The administrator password will be defined.
- The Browser Based Interface (BBI) enabled.

A baseline configuration may be established on the Secure Network Access Switch with a console connection using the following procedure:

1 Define the NSNAS base host configuration by issuing the following command on the NSNAS Setup Menu:

```
------------------------------------------------------------
[Setup Menu]
      join       - Join an existing cluster
      new        - Initialize host as a new installation
      boot       - Boot menu
      info       - Information menu
      exit       - Exit  [global command, always available]
>> Setup# new
```

2	Define the following parameters:
Interface IP: ***192.168.20.10***	The real IP address (RIP) assigned to the NSNAS.
Network Mask: ***255.255.255.0***	The network mask assigned to the NSNAS. In this example the NSNAS is deployed in an isolated VLAN but a smaller subnet with fewer host addresses could be utilized to save address space.
VLAN Tag: ***0***	Defines the 802.1Q tag used for the physical Ethernet interface. A value of 0 disables 802.1Q tagging.
Two Armed Configuration: ***no***	This example utilizes a one-armed configuration.
Default Gateway: ***192.168.20.1***	The default gateway on the core used by the NSNAS.
Management IP: ***192.168.20.11***	Defines the management IP address for the NSNAS.
DNS Server: ***192.168.10.5***	The IP address of the Windows 2003 Enterprise Server providing DNS services.
Generate SSH Host Keys: ***yes***	Generates a new SSH host keys used for SSH management and communication with SREM.
Enter a password for the "admin" user: ***admin-password***	Enter and confirm the password assigned to the admin user account. The admin user has full access to the NSNAS.
Run NSNAS quick configuration wizard?: ***yes***	Invokes a wizard which creates basic parameters that we will use to provide 802.1X authentication.
NSNAS Portal Virtual IP address: ***192.168.20.12***	The virtual IP address on the NSNAS used to provide DHCP, DNS and HTTP/HTTPS services to guest users.
NSNAS Domain name: ***eselab.com***	The DNS domain name for the system. For this example the domain name is eselab.com.
Create http to https redirect server: ***yes***	Allows the NSNAS to capture users HTTP sessions and re-direct the browser to the HTTPS portal login page for authentication.
Create default tunnel guard user: ***no***	Local user accounts will not be used in this example.
Create default system account: ***no***	Local host authentication will not be used in this example.

Would you like to enable the Nortel TunnelGuard Desktop Agent? ***Yes***	The TunnelGuard desktop agent will not be required for this example but will be enabled.
Enable secure web based configuration management: ***yes***	The browser based interface (BBI) will be enabled to perform the remaining configuration on the NSNAS.

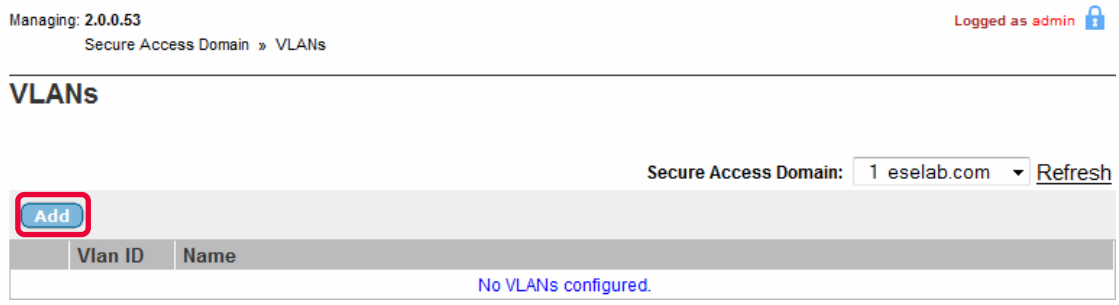
2.1.2 VLANs:

Two VLANs will be defined on the Nortel Secure Network Access Switch that will determine the NAP client VLAN membership based on compliance state. The VLAN membership will be forwarded to the Nortel Ethernet Switch using standard IETF RADIUS return attributes during EAPoL authentication upon successful Active Directory user authentication:

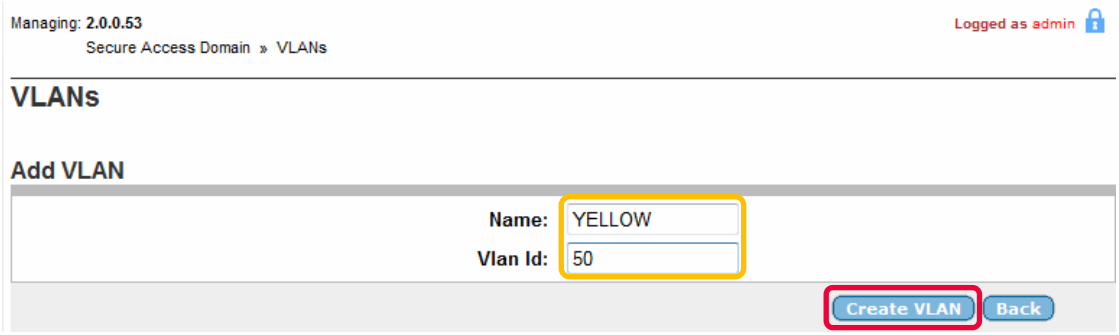
VLAN ID	VLAN Name	Purpose
30	GREEN	Will be assigned to compliant devices and will provide unrestricted access to the network.
50	YELLOW	Will be assigned to non-compliant devices and will provide remediated restricted access to the network.

VLANs may be defined and installed on the Secure Network Access Switch using the Browser Based Interface with the following procedure:

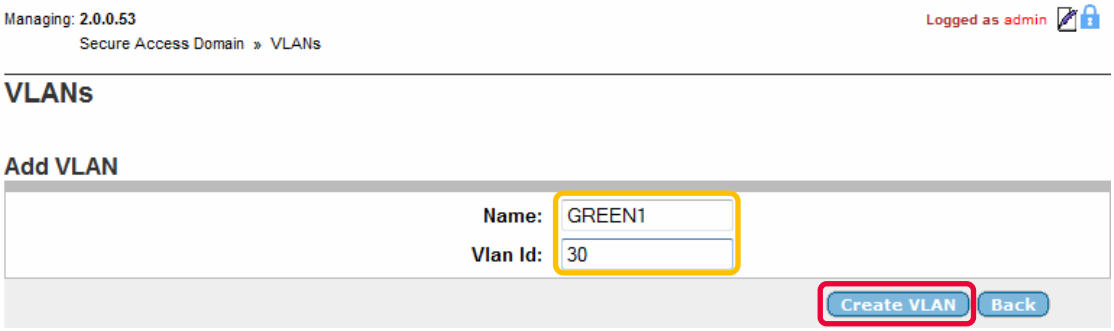
1 Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *VLANs* and then *Add*.



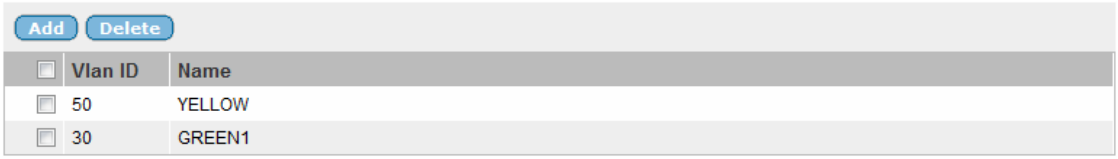
2 Enter the name *YELLOW* and specify the VLAN Id *50*. Click *Create VLAN*.



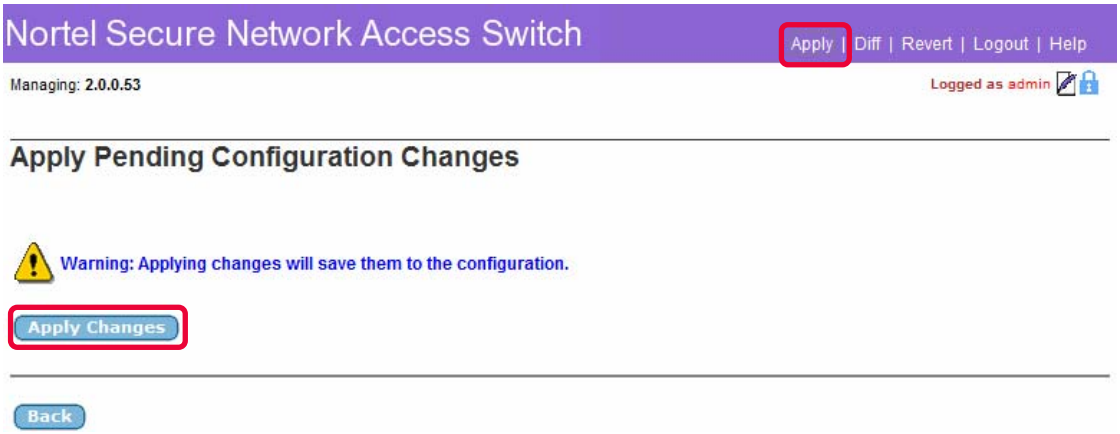
3 Click *Add*. Enter the name *GREEN* and specify the VLAN Id *30*. Click *Create VLAN*.



4 The Yellow and Green VLANs will now be defined on the Nortel Secure Network Access Switch.



5 Apply and save the changes by clicking *Apply* and then *Apply Changes*.



2.1.3 Certificates:

A Server and CA Root Certificate issued from Windows 2003 Certificate Services will be installed on the Secure Network Access Switch to support PEAP authentication:

- Server Certificate – Issued from an Enterprise or Public Certification Authority and is used to secure client credentials during PEAP authentication.
- CA Root Certificate – Issued from an Enterprise or Public Certification Authority and is installed on the SNAS and Windows Workstations to verify the validity of all certificates issued from the Certification Authority.

In this example the server and CA root certificates were issued from Microsoft Certificate Services using the Web Enrolment tool and exported to a PKCS#12 file. The Server Certificate was issued with the Common Name (CN) nsnas-vip.eselab.com which resolves to the Virtual IP Address on the Secure Network Access Switch.

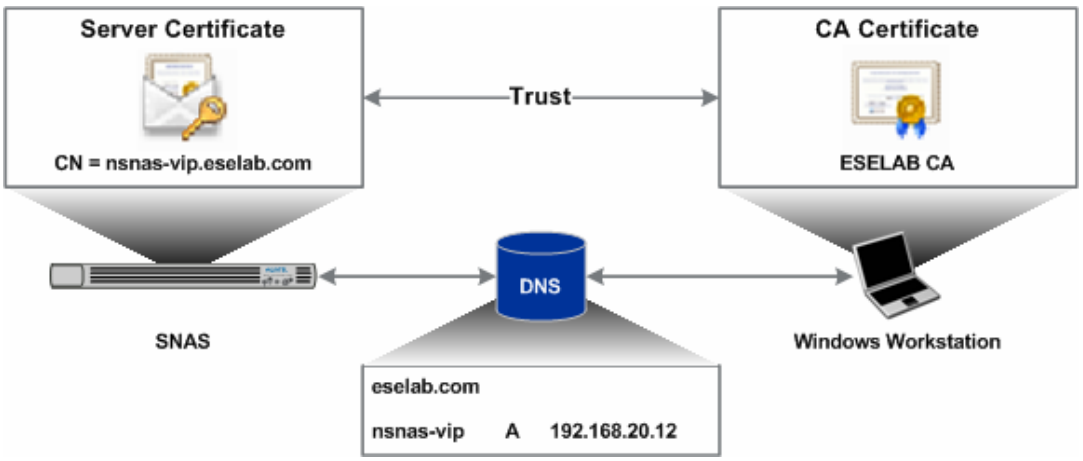
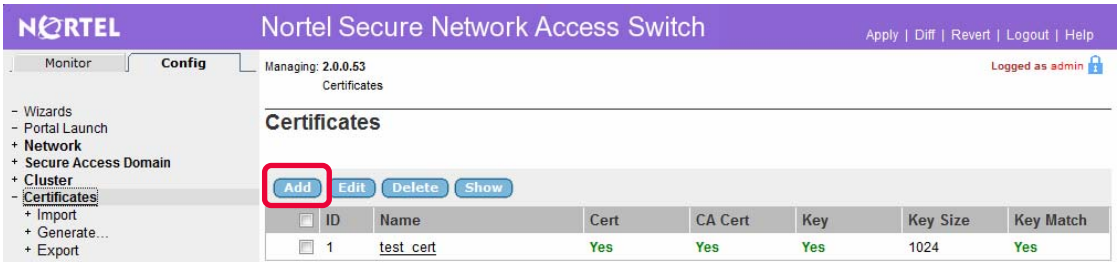


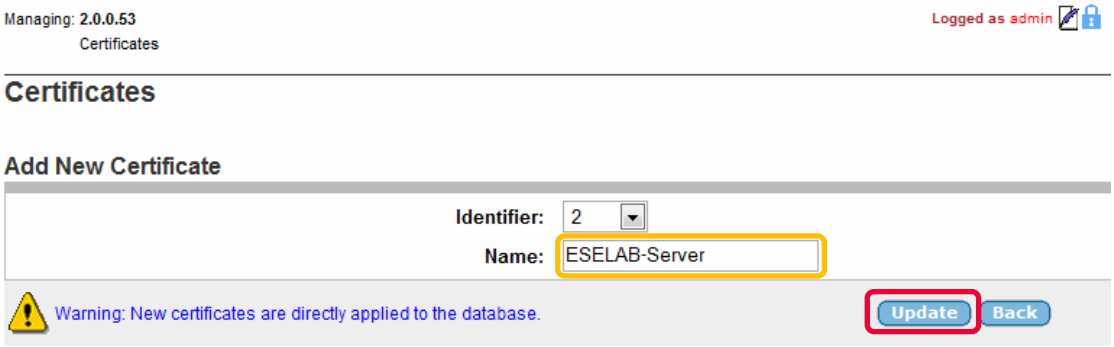
Figure 2.1.3 – Server Certificate

Certificates may be defined and installed on the Secure Network Access Switch using the Browser Based Interface with the following procedure:

1 Using the Browser Based Interface (BBI) navigation tree click *Certificates* and then *Add*.

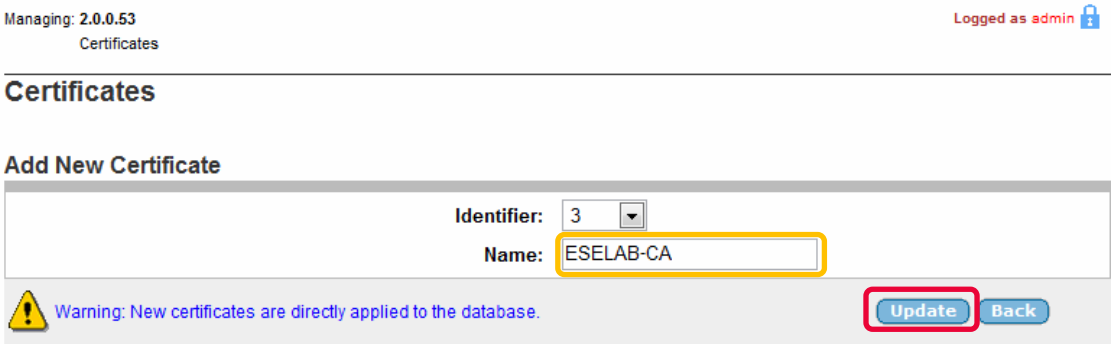


2 Specify a unique name for the server certificate and then click *Update*.

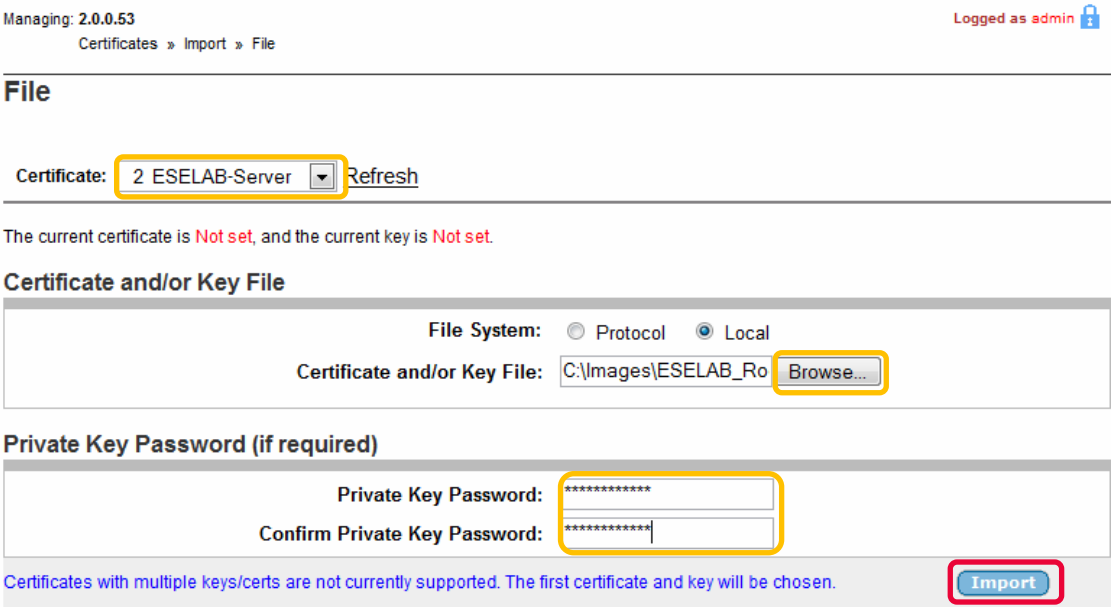


3 Click *Add* and specify unique a name for the CA root certificate and then click

Update.

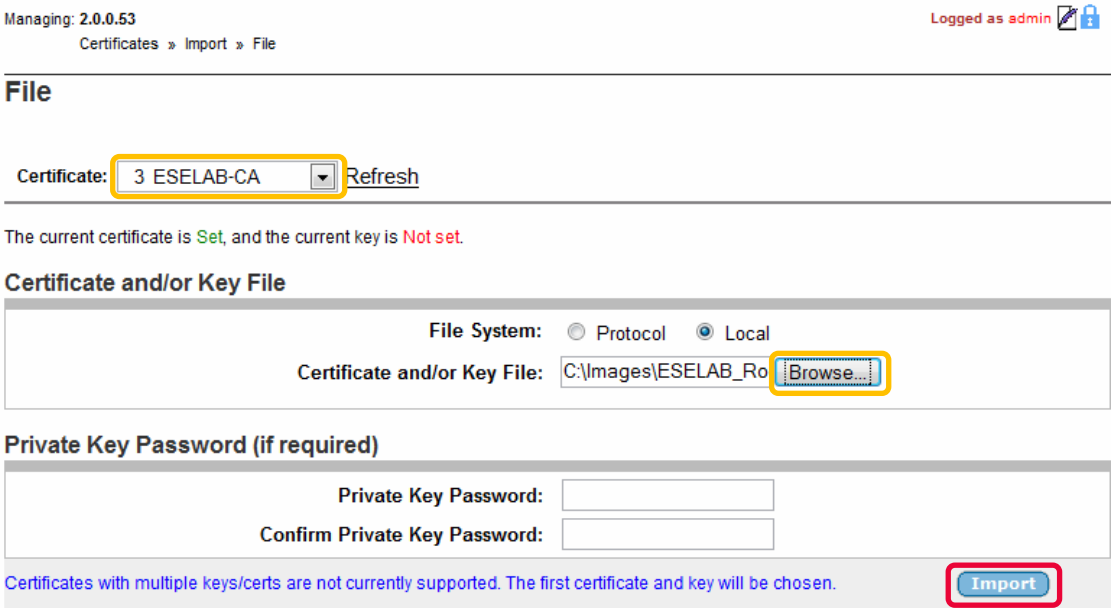


4 **Using the navigation tree click *Certificates*, *Import* and then *File*. In the *Certificate* pull-down menu select the server certificate name created in step 2. Click Browse and locate the PKCS#12 server certificate issued from the Certificate Authority. Enter and verify the *Private Key Password* then click *Import*.**



5 **Using the navigation tree click *Certificates*, *Import* and then *File*. In the *Certificate* pull-down menu select the CA root certificate name created in step 3. Click Browse**

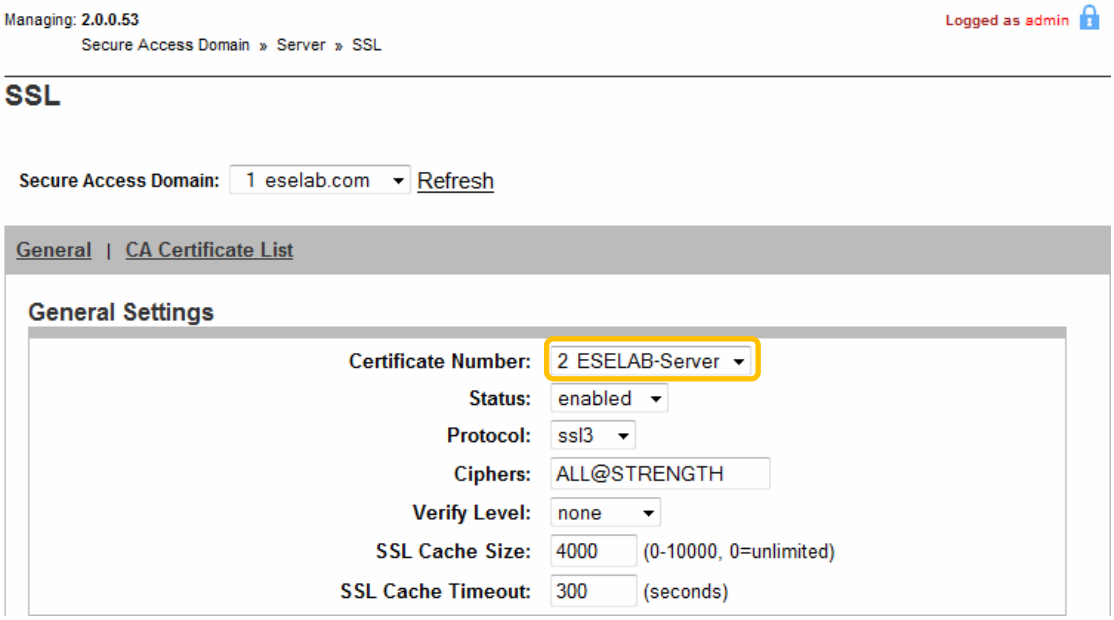
and locate the CA certificate issued from the Certificate Authority then click *Import*. Note that the CA root certificate does not require a *Private Key Password*.



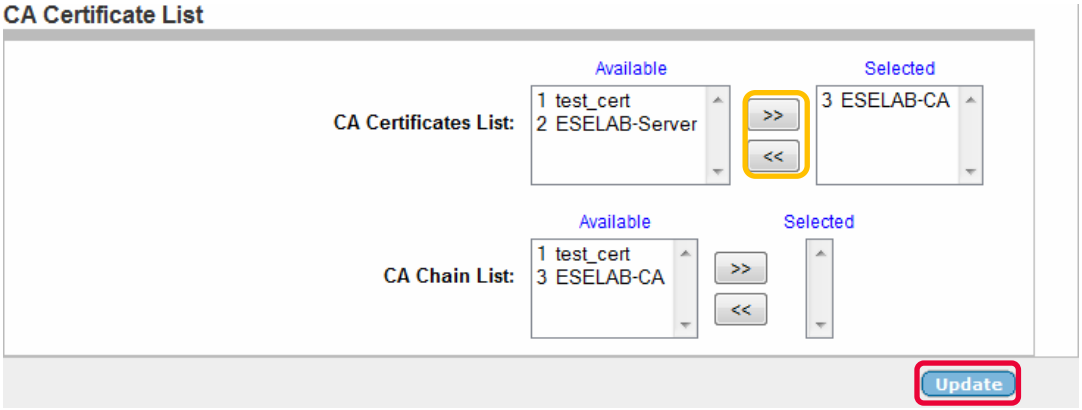
6 The server and CA root certificates will now be installed on the Secure Network Access Switch.

ID	Name	Cert	CA Cert	Key	Key Size	Key Match
1	test_cert	Yes	Yes	Yes	1024	Yes
2	ESELAB-Server	Yes	No	Yes	1024	Yes
3	ESELAB-CA	Yes	Yes	No		

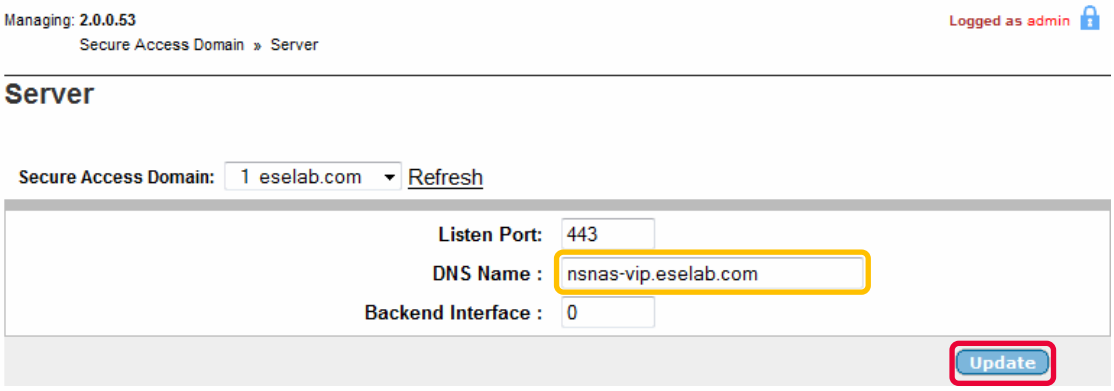
7 Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *Server* and then *SSL*. Click on the *Certificate Number* pull-down menu and select the Server Certificate name installed in the previous steps.



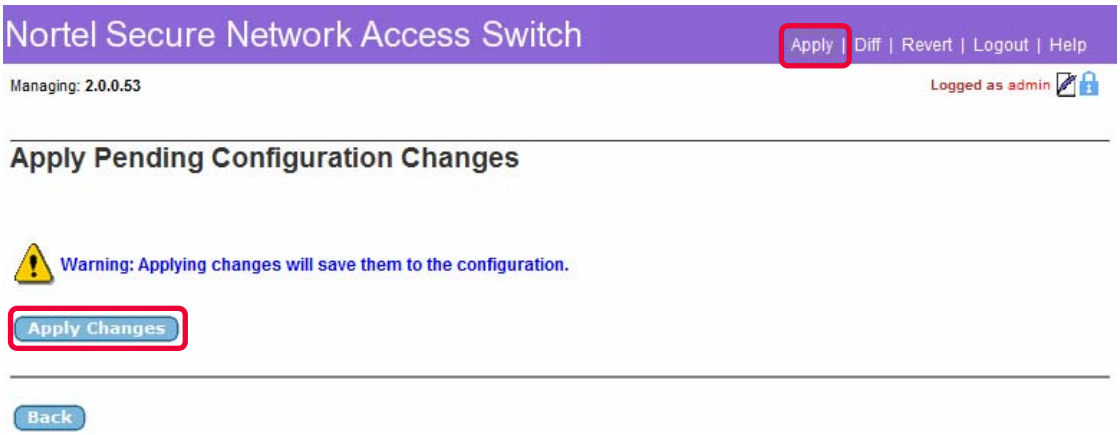
8 **In the *CA Certificate List* remove the default CA certificate named *test_cert* and add the CA Certificate installed in the previous steps. Click *Update*.**



9 **Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain* then *Server*. In the *DNS Name* field enter the fully qualified name of the host as specified in the Common Name field in the Server Certificate. Click *Update*.**



10 Apply and save the changes by clicking *Apply* and then *Apply Changes*.



2.1.4 Authentication Servers:

An LDAP and NTLM server will be created on the Secure Network Access Switch to authenticate RADIUS access requests against Active Directory. The NTLM server will be used for user authentication and LDAP server used for group association:

- An LDAP authentication server entry will be created which will be used for Active Directory group association.
- An NTLM authentication server entry will be created which will be used for Active Directory user authentication.
- The NTLM authentication server will be added to the authentication order.

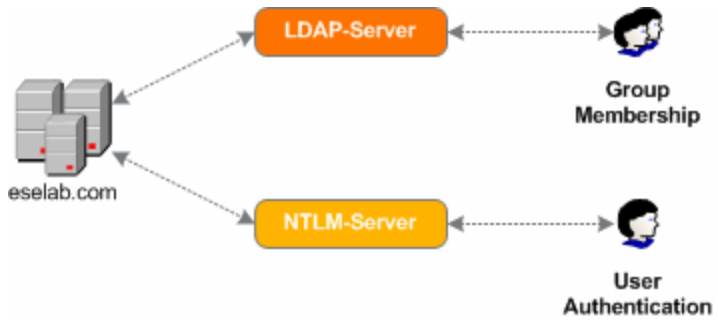
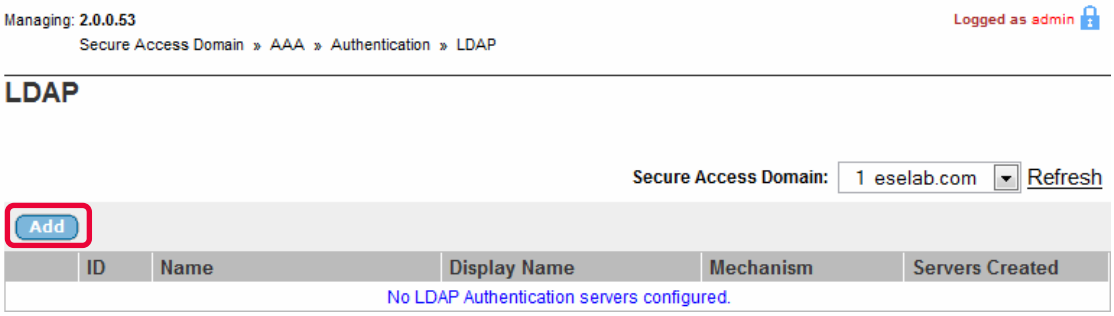


Figure 2.1.4 – LDAP and NTLM Servers

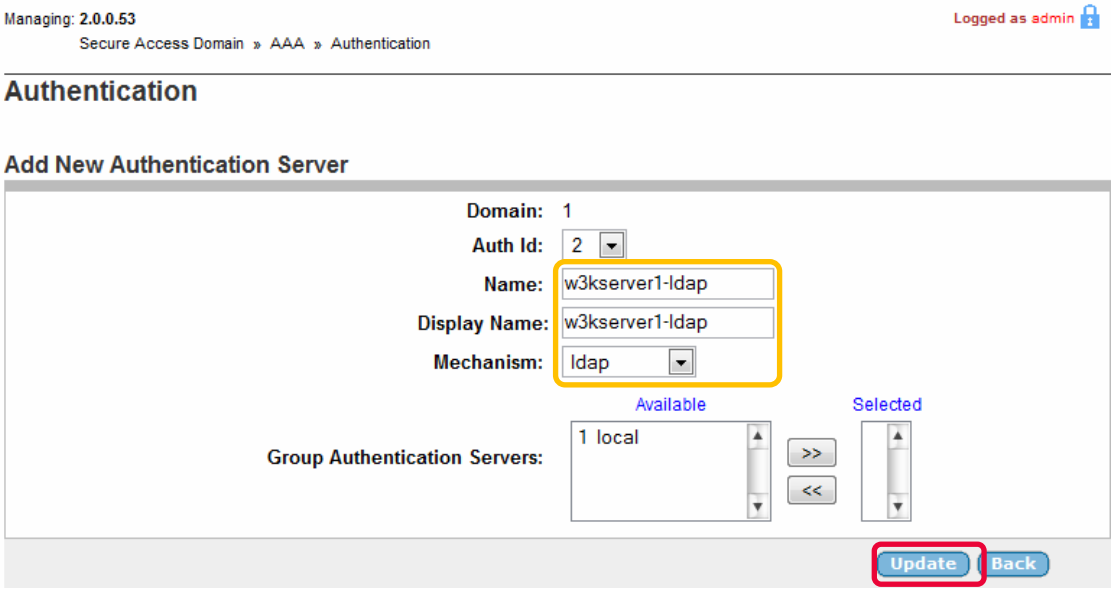
This section assumes that NTLMv1 is enabled on the Domain Controller. Details for enabling NTLMv1 authentication are provided by the following Microsoft Knowledge Base Article: http://support.microsoft.com/kb/942564.

LDAP and NTLM authentication servers can be created and the authentication order defined on the Secure Network Access Switch using the Browser Based Interface with the following steps:

1 Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *AAA*, *Authentication*, *LDAP* and then *Add*.

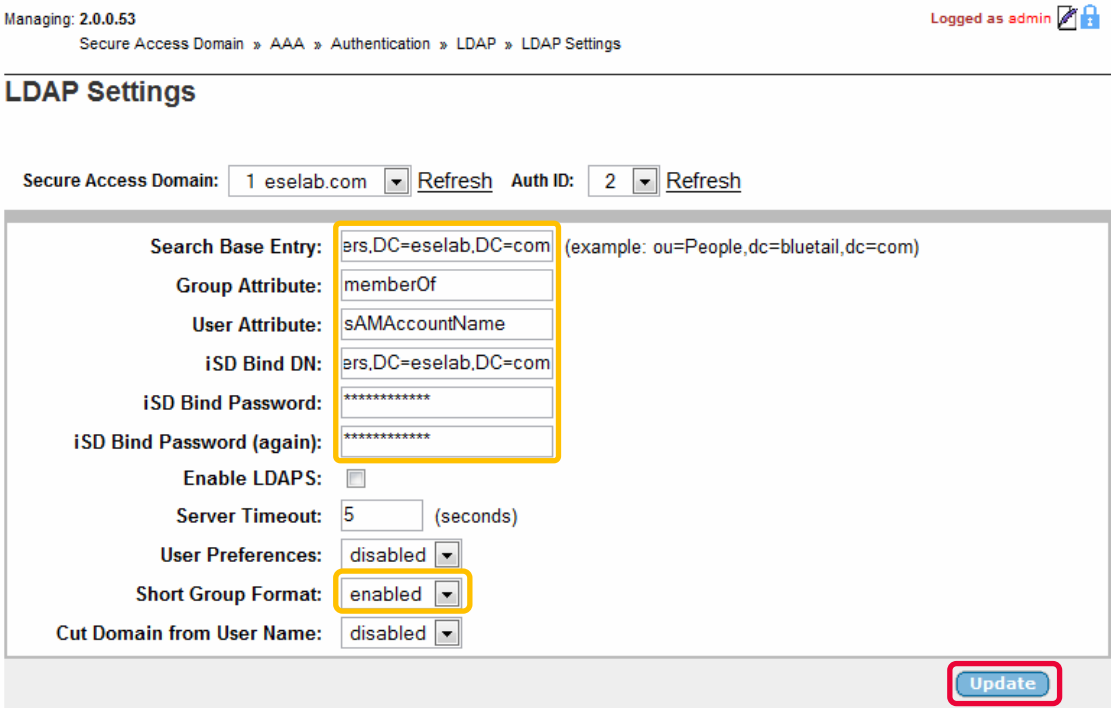


2 Specify an LDAP Server *Name*, *Display Name* and set the Mechanism to *LDAP* Click *Update*.

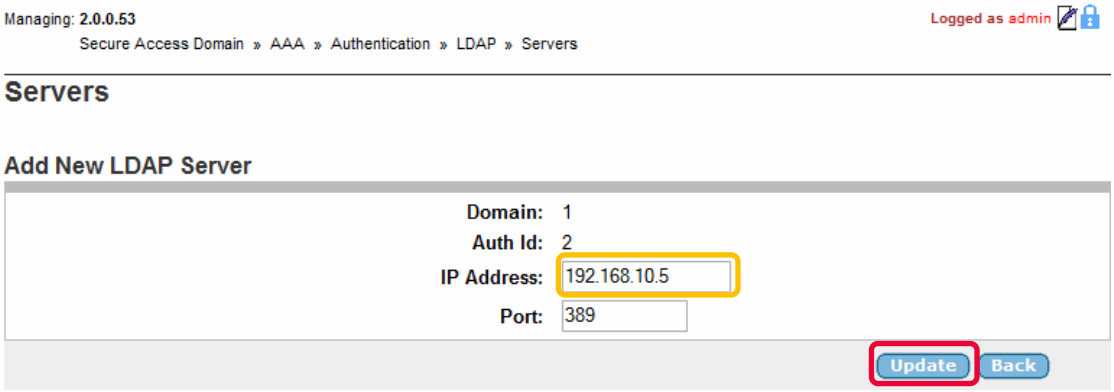


3 Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *AAA*, *Authentication*, *LDAP* and then *LDAP Settings*. Enter the following required information then click *Update*.

Search Base Entry	Assigns the DN (Distinguished Name) of the Active Directory container where the user entries are found. In this example the following DN was used: *CN=Users,DC=eselab,DC=com*. Note: To support both computer and user authentication for the eselab.com domain the searchbase *DC=eselab,DC=com* should be used.
Group Attribute	Defines the LDAP attribute that contains the name(s) of the group(s) of which a particular user is a member. For Active Directory this value needs to be set to: *memberOf*.
User Attribute	Defines the LDAP attribute that contains the user names used for authentication of a user in the domain. For Active Directory this value needs to be set to: *sAMAccountName*.
iSD Bind DN	Points to an entry in the Active Directory server used for authenticating the Nortel Secure Network Access Switch. In this example a user named 'nsnas' was created in Active Directory which requires the following DN to be used: *CN=nsnas,CN=Users,DC=eselab,DC=com*.
iSD Bind Password	Defines the password assigned to the Active Directory user defined by the iSD Bind DN.
Short Group Format	Specify if the short group format should be enabled or not. This value needs to be set to: *Enabled*.

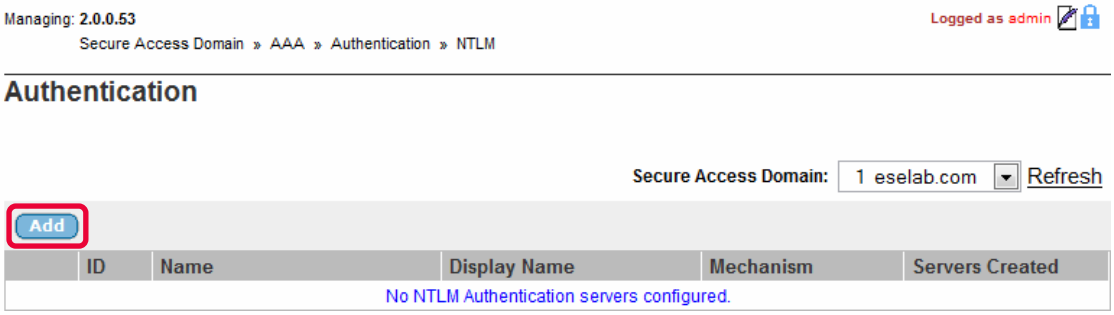


4 **Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *AAA*, *Authentication*, *LDAP* and then *Servers*. Specify the Active Directory Servers *IP Address* and click *Update*.**

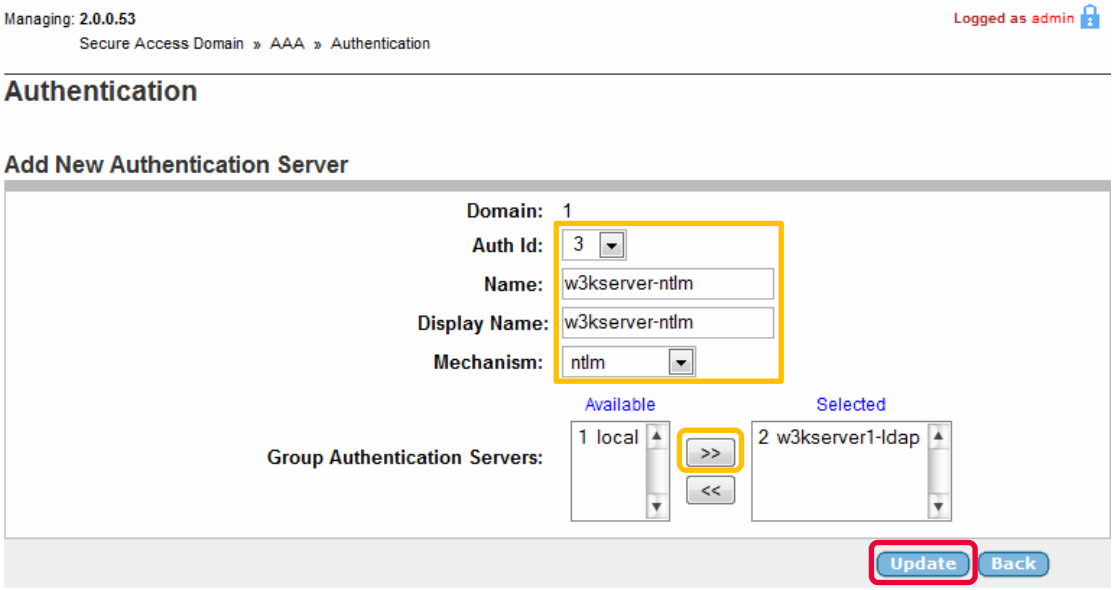


5 **Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*,**

***AAA*, *Authentication*, *NTLM* and then *Add*.**

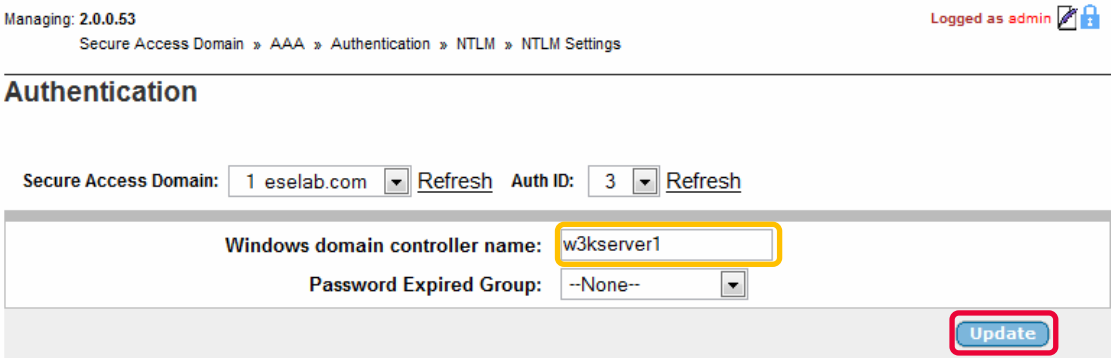


6 **Specify an NTLM Server *Name*, *Display Name* and set the Mechanism to *NTLM*. In the *Available* list highlight the LDAP server name created in step 2 and click *Move*. Click *Update*.**

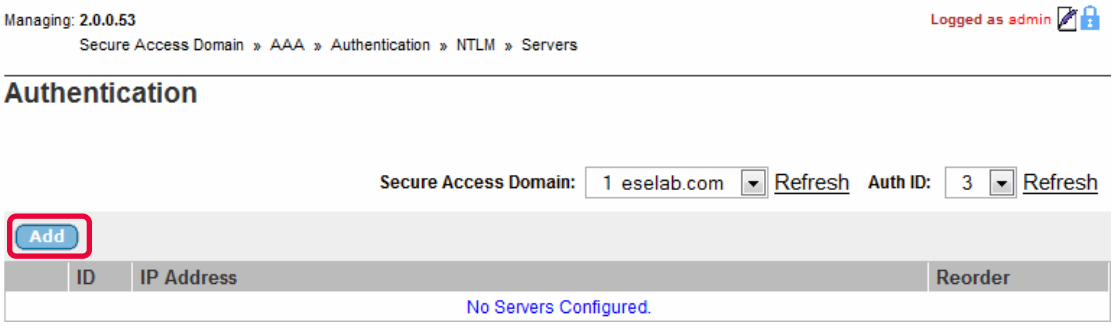


7 **Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *AAA*, *Authentication*, *NTLM*, *NTLM Settings*. Specify the hostname of the Windows**

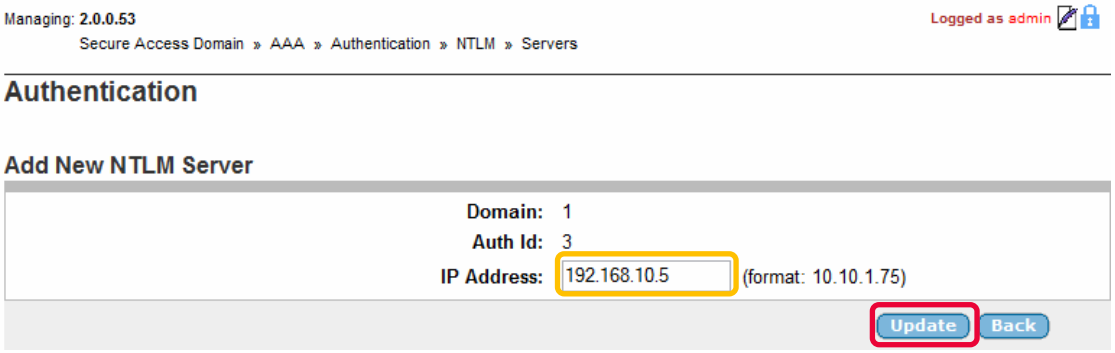
Domain Controller then click *Update*.



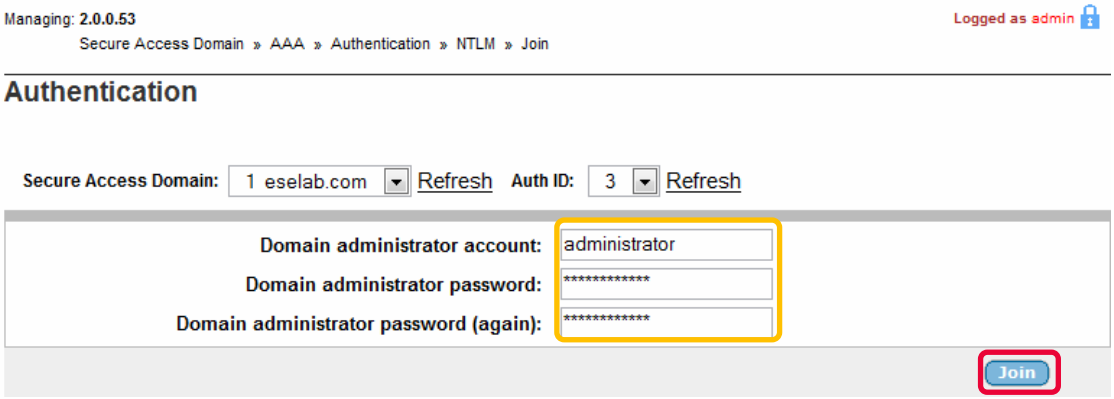
8 **Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *AAA*, *Authentication*, *NTLM*, *Servers* and click *Add*.**



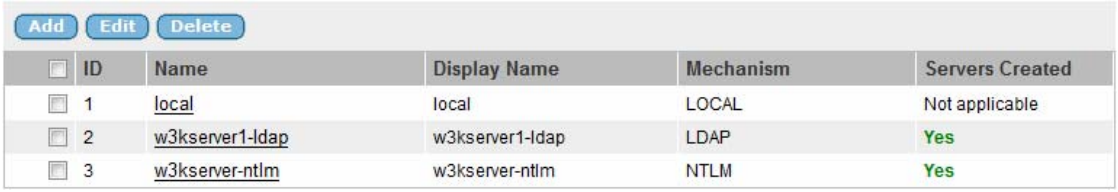
9 **Specify the IP Address of the Domain Controller and click *Update*.**



10 **Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *AAA*, *Authentication*, *NTLM* and then *Join*. Specify the Domain Administrator username and password and click *Join*.**



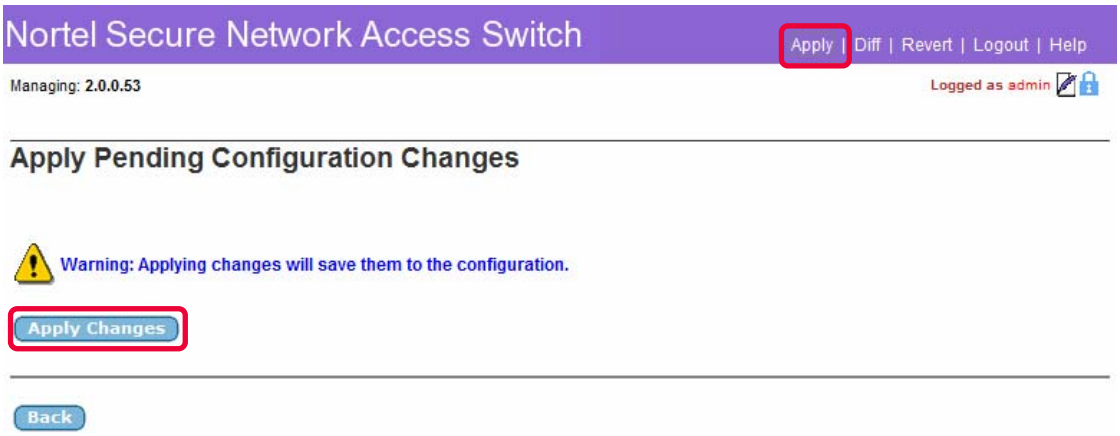
11 **The LDAP and NTLM servers will now be installed on the Secure Network Access Switch.**



ID	Name	Display Name	Mechanism	Servers Created
1	local	local	LOCAL	Not applicable
2	w3kserver1-ldap	w3kserver1-ldap	LDAP	Yes
3	w3kserver-ntlm	w3kserver-ntlm	NTLM	Yes

12 **In the navigation tree click *Secure Access Domain*, *AAA*, *Authentication* and *AuthOrder*. In the *Available* list highlight the name of the NLTM authentication server click *move* and then *Update*.**

13 **Apply and save the changes by clicking *Apply* and then *Apply Changes*.**



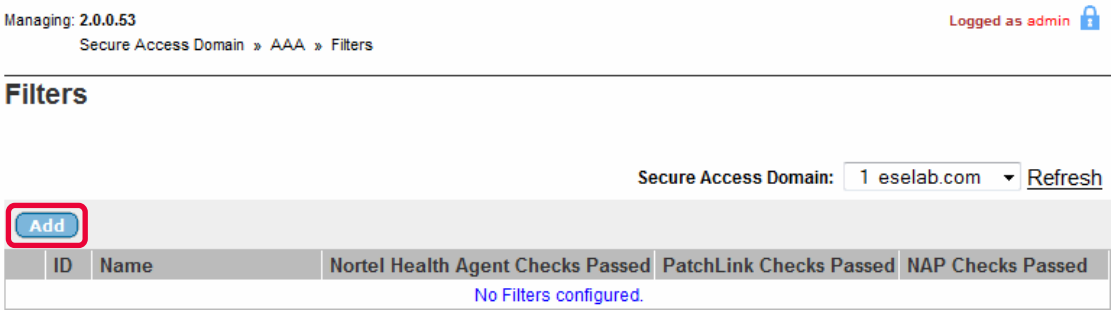
2.1.5 Filters:

Four filters will be defined on the Nortel Secure Network Access Switch that will be later associated with the extended profiles to determine user VLAN membership based on the end-points NHA and NAP compliance state:

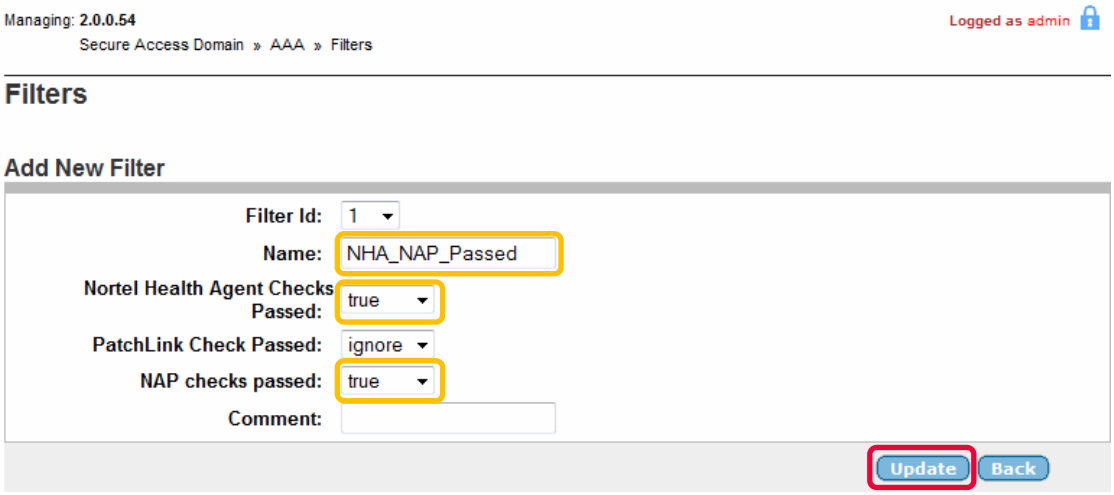
Filter Name	NHA Checks Passed	NAP Checks Passed	Application
NHA_NAP_Passed	True	True	Filter will be matched when both NHA and NAP compliance checks pass.
NHA_Passed_NAP_Failed	True	False	Filter will be matched when NHA compliance checks pass and NAP compliance checks fail.
NHA_Failed_NAP_Passed	False	True	Filter will be matched when NHA compliance checks fail and NAP compliance checks pass.
NHA_NAP_Failed	False	False	Filter will be matched when both NHA and NAP compliance checks fail.

Filters may be defined and installed on the Secure Network Access Switch using the Browser Based Interface with the following procedure:

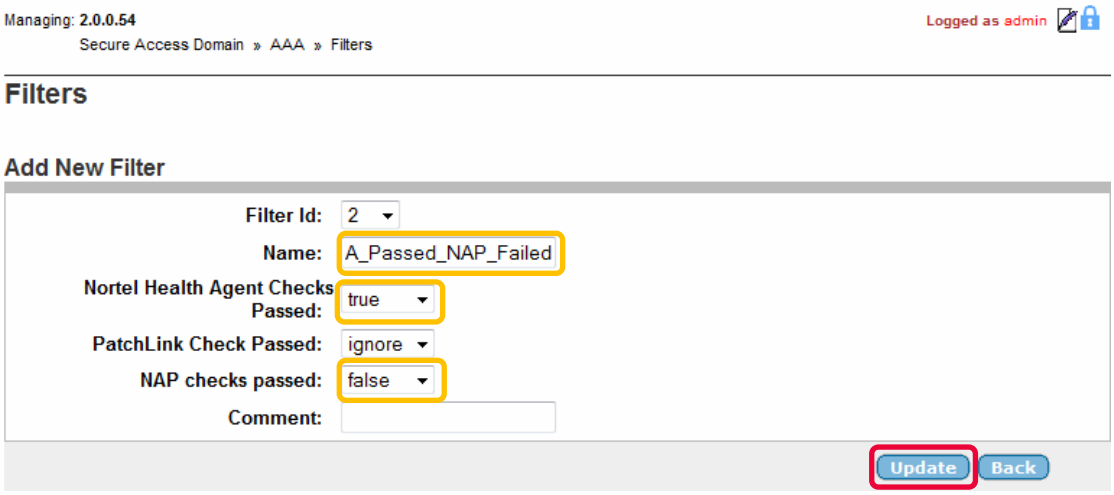
1	**Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *AAA*, *Filters* and then *Add*.**



2 **Specify the name *NHA_NAP_Passed* and set both the *Nortel Health Agent Checks Passed* and *Nap checks passed* fields to *true*. Click *Update*.**

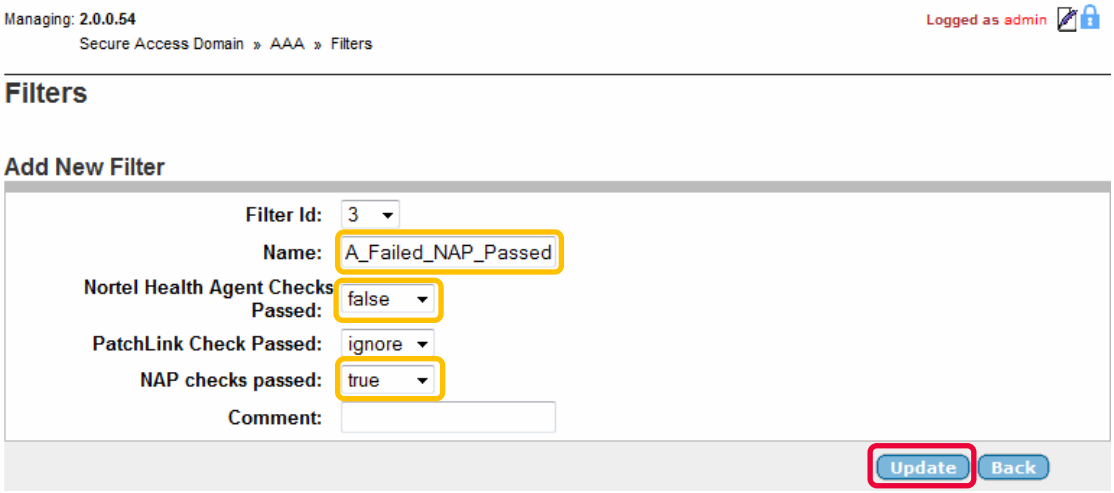


3 **Click *Add* to create a second filter. Specify the name *NHA_Passed_NAP_Failed* and set the *Nortel Health Agent Checks Passed* field to *true* and the *Nap checks passed* field to *false*. Click *Update*.**

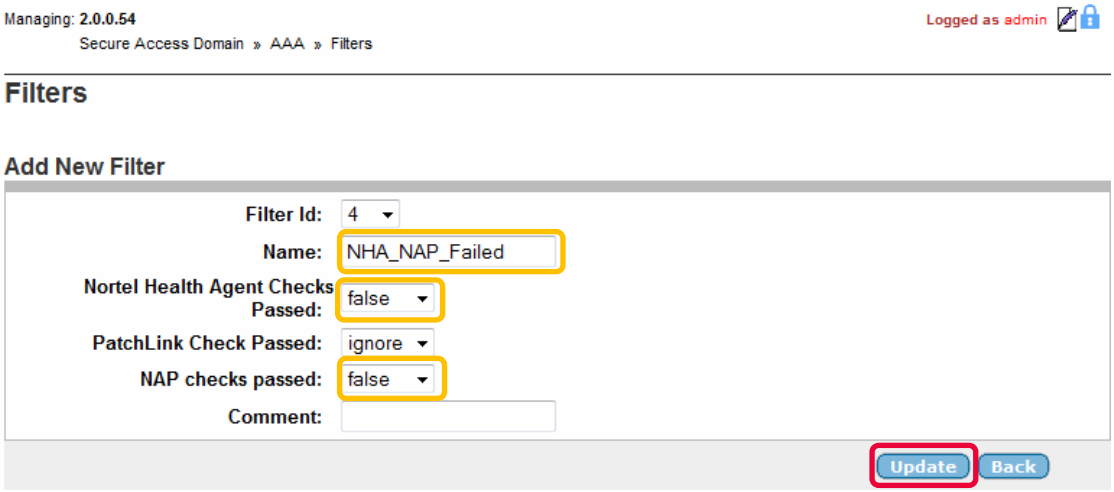


4 **Click *Add* to create a third filter. Specify the name *NHA_Failed_NAP_Passed* and set the *Nortel Health Agent Checks Passed* field to *false* and the *Nap checks passed* field**

to *true*. Click *Update*.



5 **Click *Add* to create a fourth filter. Specify the name *NHA_ NAP_Failed* and set both the *Nortel Health Agent Checks Passed* and *Nap checks passed* fields to *false*. Click *Update*.**

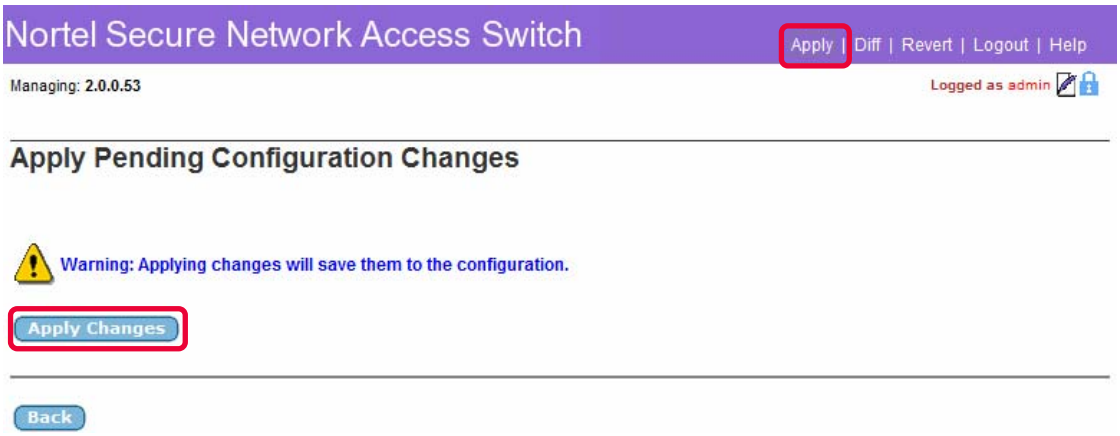


6 **Four filters will now be defined on the Nortel Secure Network Access Switch.**

Add Edit Delete

ID	Name	Nortel Health Agent Checks Passed	PatchLink Checks Passed	NAP Checks Passed
1	NHA_NAP_Passed	true	ignore	true
2	NHA_Passed_NAP_Failed	true	ignore	false
3	NHA_Failed_NAP_Passed	false	ignore	true
4	NHA_NAP_Failed	false	ignore	false

7 **Apply and save the changes by clicking *Apply* and then *Apply Changes*.**

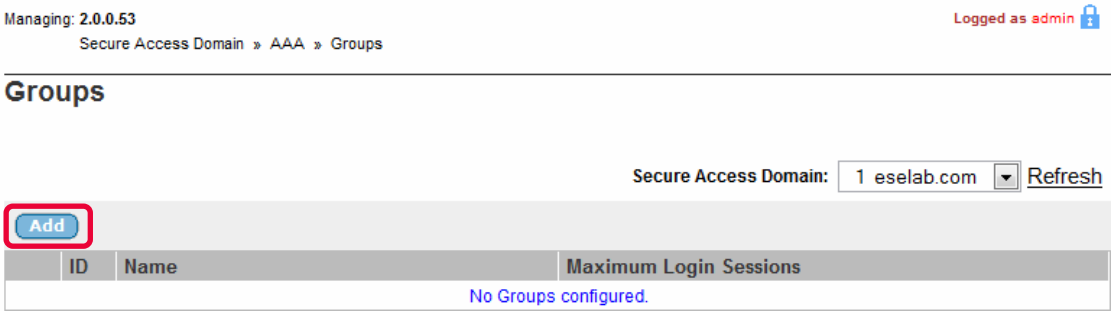


2.1.6 Groups:

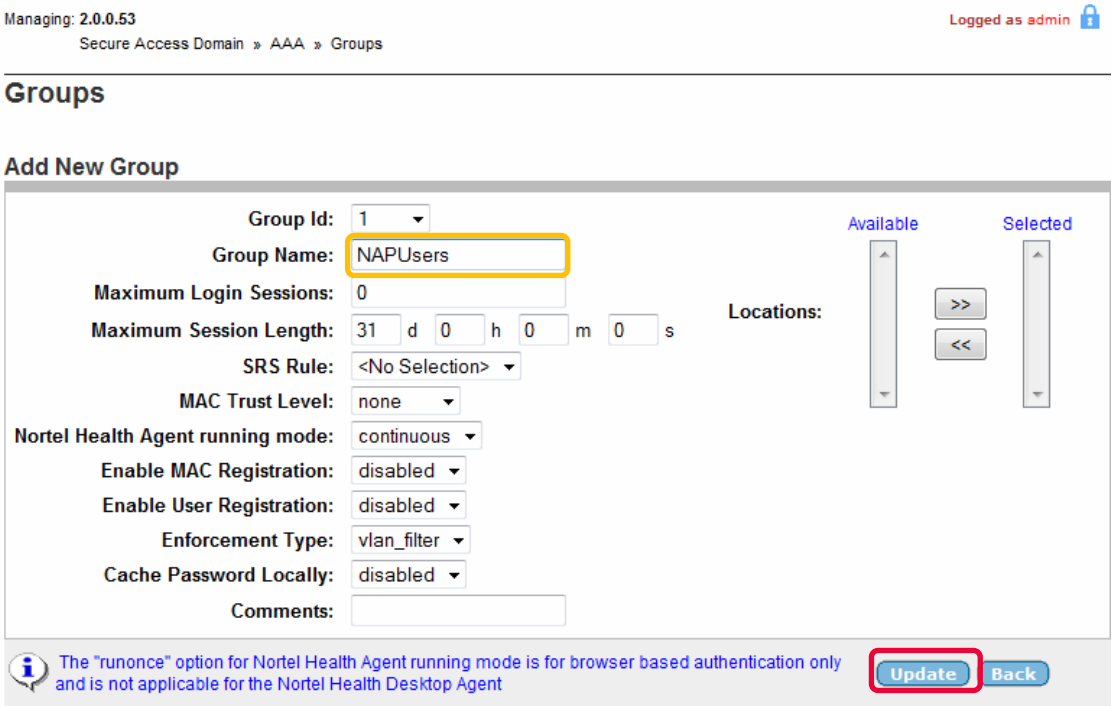
A local group named *NAPUsers* will be defined on the Secure Network Access Switch which will have Extended Profiles to determine user VLAN membership based on NAP / NHA compliance state.

A local group can be defined on the Secure Network Access Switch using the Browser Based Interface with the following steps:

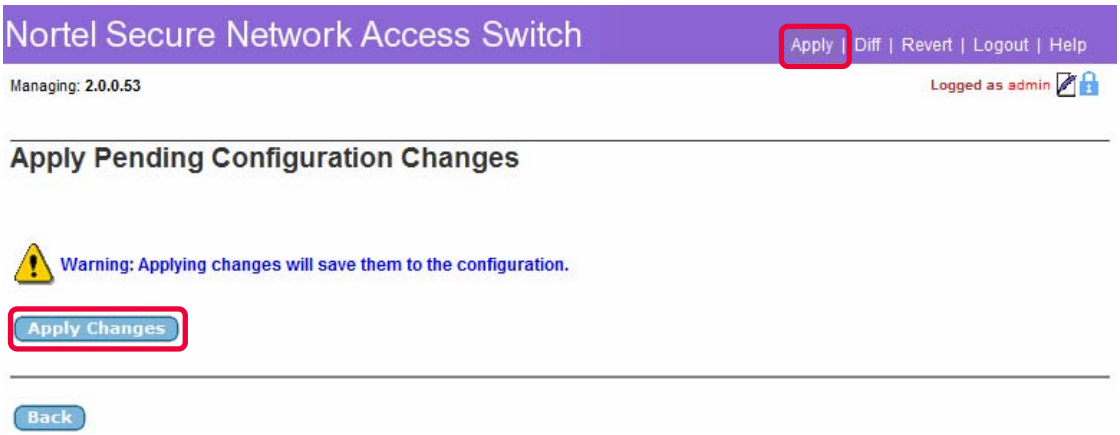
1 Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *AAA*, *Groups* and then *Add*.



2 In the *Group Name* field enter the name *NAPUsers* and then click *Update*.



3 Apply and save the changes by clicking *Apply* and then *Apply Changes*.



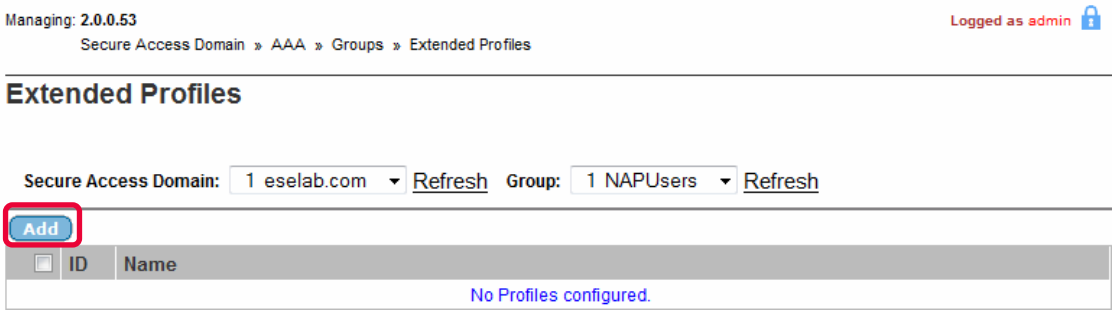
2.1.7 Extended Profiles:

Two extended profiles will be defined on the Nortel Secure Network Access Switch that will associate Groups and Filters to determine user VLAN membership based on NAP / NHA compliance state:

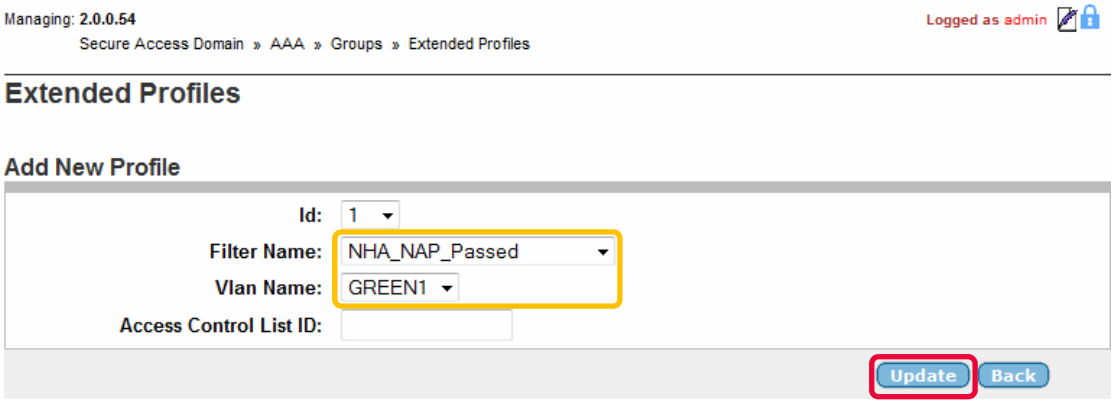
Group	Filter Name	VLAN Name
NAPUsers	NHA_NAP_Passed	GREEN1
NAPUsers	NHA_Passed_NAP_Failed	YELLOW
NAPUsers	NHA_Failed_NAP_Passed	YELLOW
NAPUsers	NHA_NAP_Failed	YELLOW

Extended Profiles may be defined and installed on the Secure Network Access Switch using the Browser Based Interface with the following procedure:

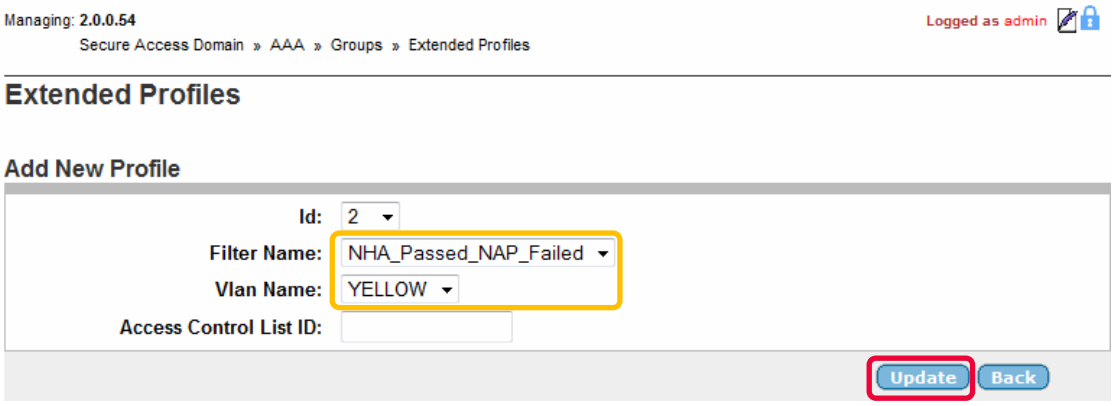
1 Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *AAA*, *Groups*, *Extended Profiles* and then *Add*.



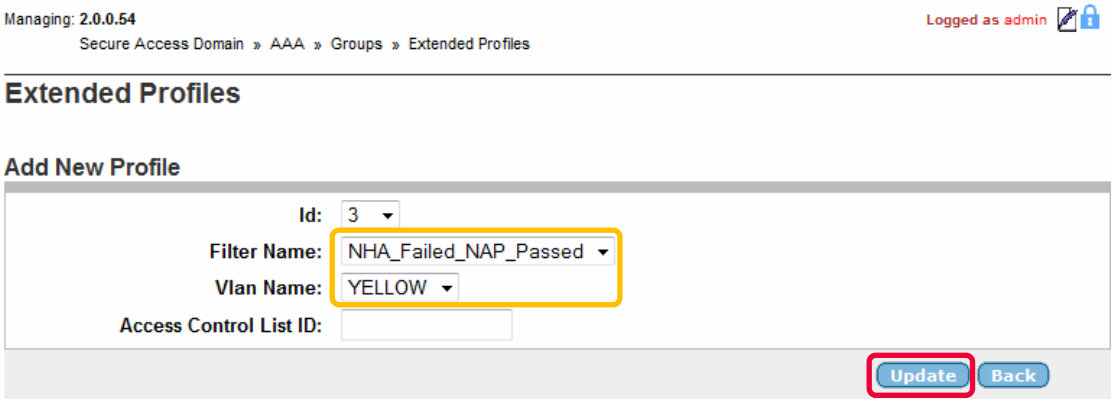
2 Select the filter name NHA_*NAP_Passed* and set the VLAN Name to *GREEN1*. Click *Update*.



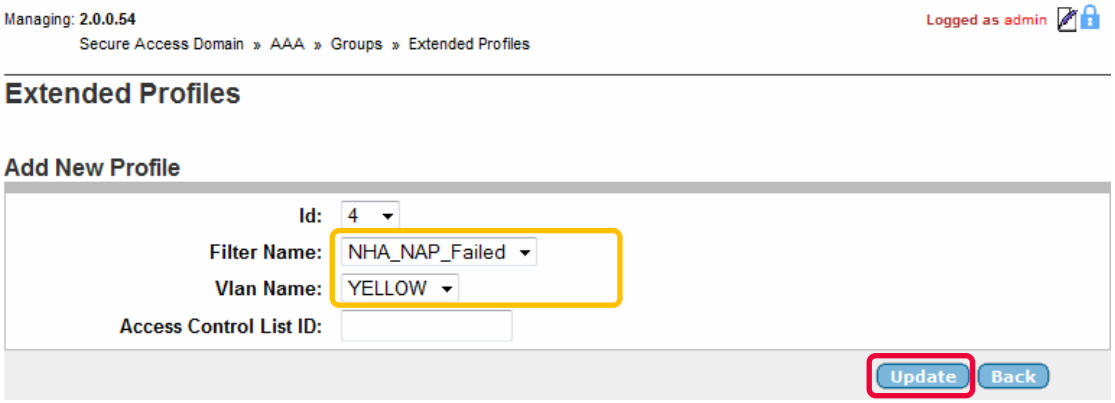
3 **Click Add to create a second profile. Select the filter name *NHA_Passed_NAP_Failed* and set the VLAN Name to *YELLOW*. Click *Update*.**



4 **Click Add to create a third profile. Select the filter name *NHA_Failed_NAP_Passed* and set the VLAN Name to *YELLOW*. Click *Update*.**



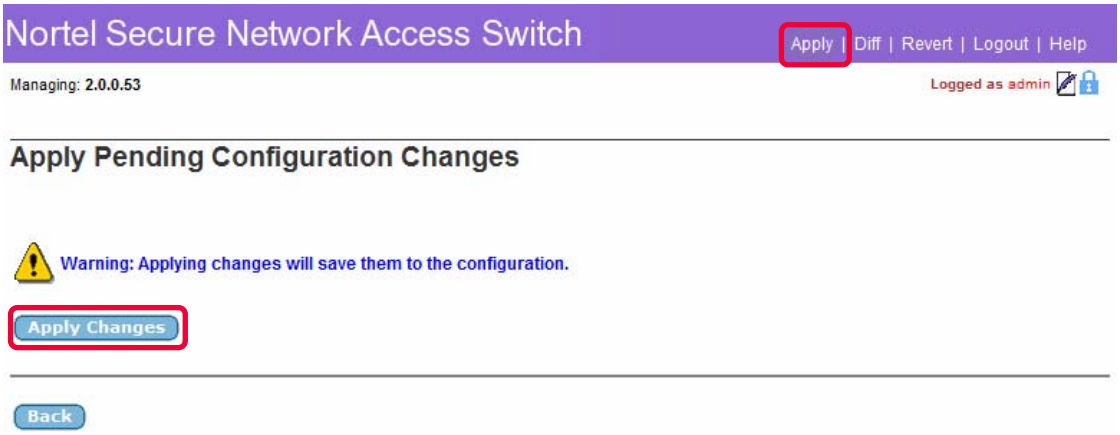
5 **Click Add to create a fourth profile. Select the filter name *NHA_NAP_Failed* and set the VLAN Name to *YELLOW*. Click *Update*.**



6 Four Extended Profiles will now be defined on the Nortel Secure Network Access Switch.

	ID	Name
	1	NHA_NAP_Passed
	2	NHA_Passed_NAP_Failed
	3	NHA_Failed_NAP_Passed
	4	NHA_NAP_Failed

7 Apply and save the changes by clicking *Apply* and then *Apply Changes*.



2.1.8 RADIUS Server:

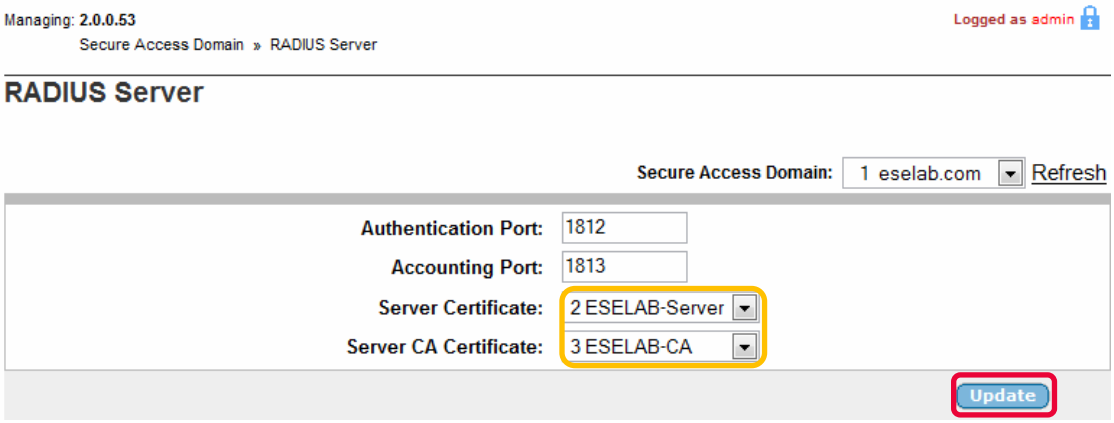
The RADIUS server needs to be configured on the Secure Network Access Switch to support PEAP authentication requests from the Nortel Ethernet Switch:

1. Certificates – The Server and Root CA Certificates created in Section 2.1.3 will be selected for use with PEAP authentication.

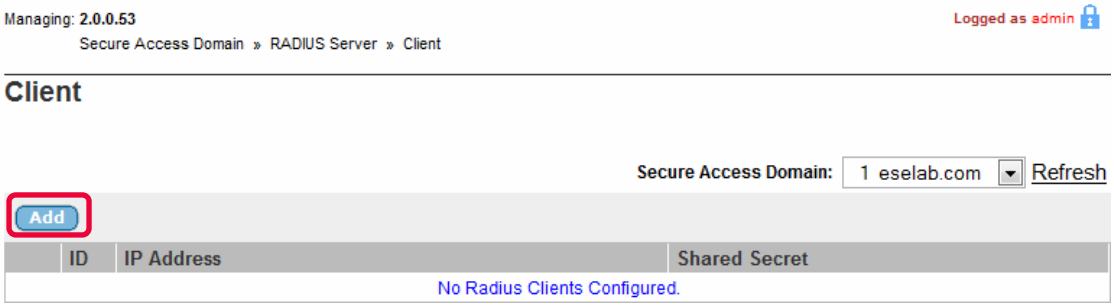
- Clients – The Ethernet Routing Switch 5500 will be defined as a RADIUS client.
- Realms – A realm will be defined to direct authentication requests to the NTLM server.

RADIUS Server configuration can be defined on the Secure Network Access Switch using the Browser Based Interface with the following steps:

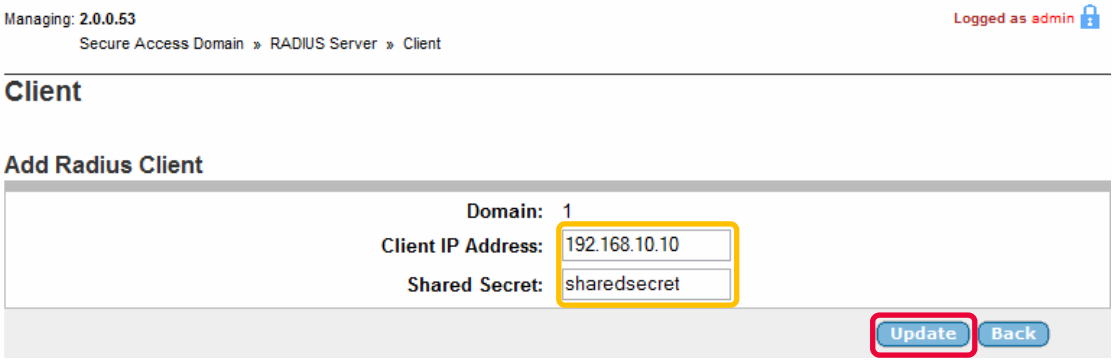
1 **Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain* then *RADIUS Server*. In the *Server Certificate* and *Server CA Certificate* pull-down menus select the Server certificate added in section 2.1.3. Click *Update*.**



2 **Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *RADIUS Server* then *Client*. Click *Add.***



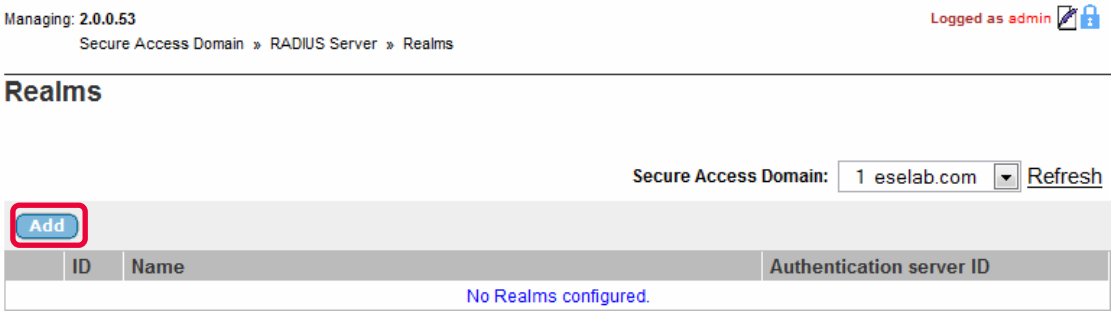
3 **Enter the *IP Address* and *Shared Secret* of the Ethernet Routing Switch 5500. Click *Update*.**



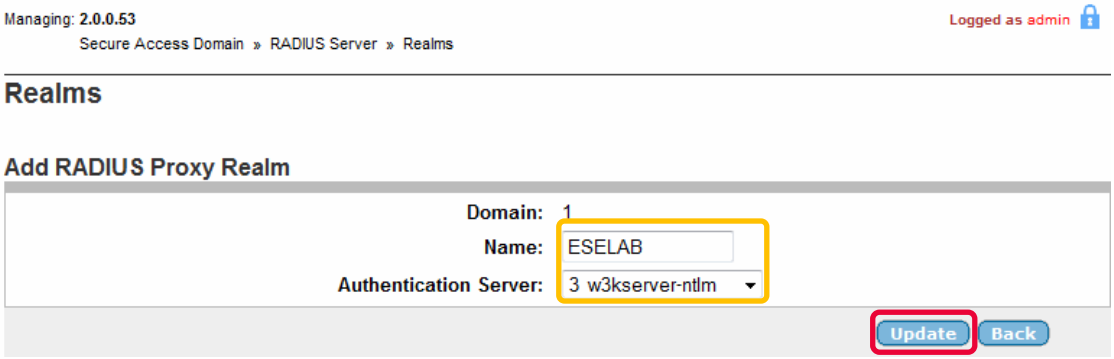
4 The Nortel Ethernet Switch will now be listed as a RADIUS client.

The RADIUS shared key must match the shared secret defined on the Nortel Ethernet Switch.

5 Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *RADIUS Server* then *Realms*. Click *Add.*

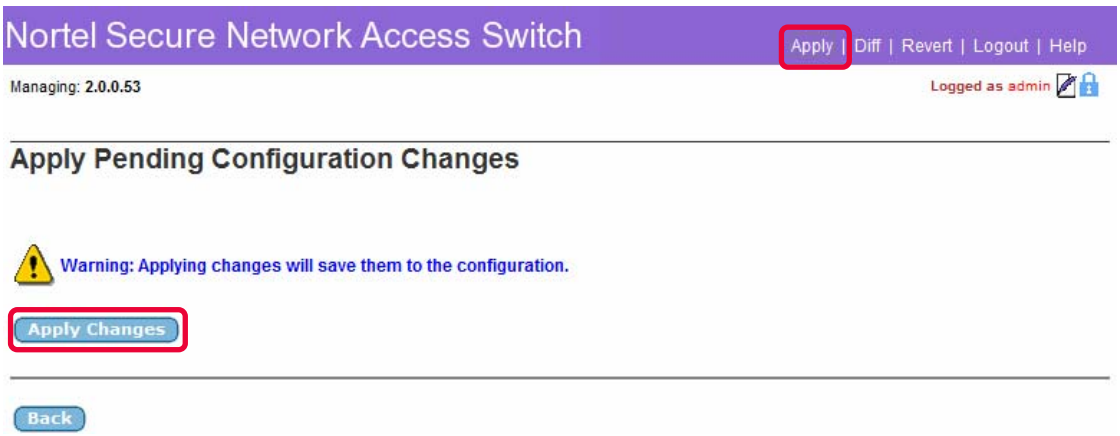


8 Active Directory Authentication – In the Name field type enter the name of the Active Directory Domain *ESELAB*. In the *Authentication Server* pull-down menu select the name of the NTLM authentication server created in section 2.1.4 then click *Update*.



Additional details on Realms may be located in the Appendix.

9 Apply and save the changes by clicking *Apply* and then *Apply Changes*.

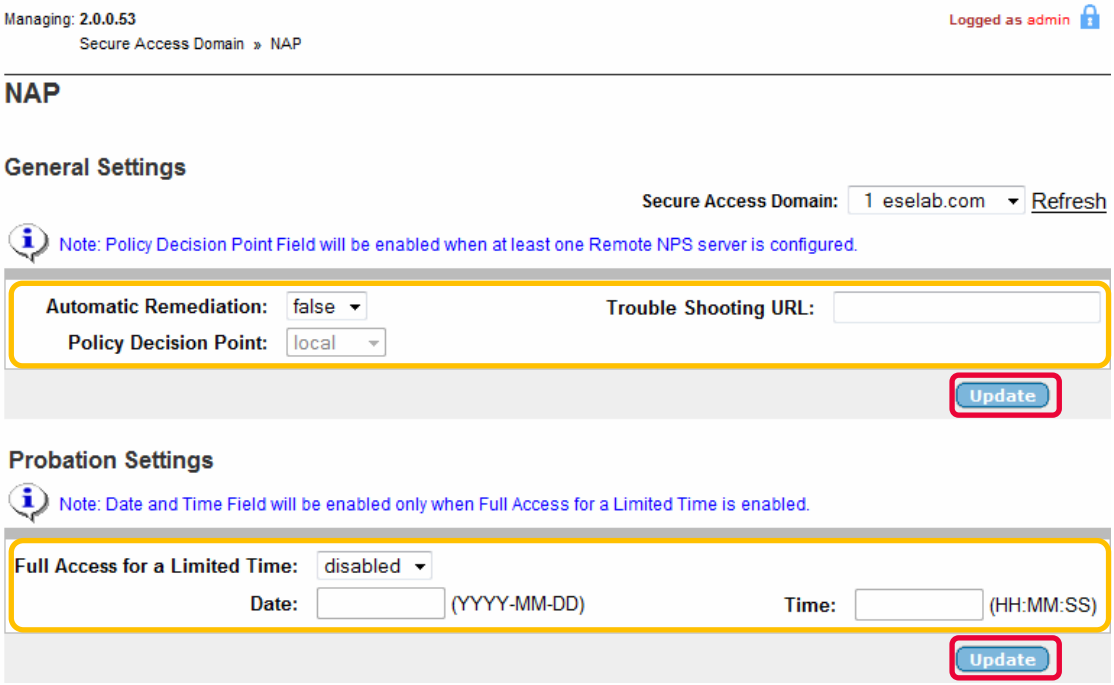


2.1.9 Network Access Protection:

The NAP settings will be configured to define the criteria that the Nortel Secure Network Access Switch uses to determine NAP compliance state. Optionally auto-remediation may be enabled to automatically correct client issues and a troubleshooting URL provided to non-compliant users if desired.

NAP configuration can be defined on the Secure Network Access Switch using the Browser Based Interface with the following steps:

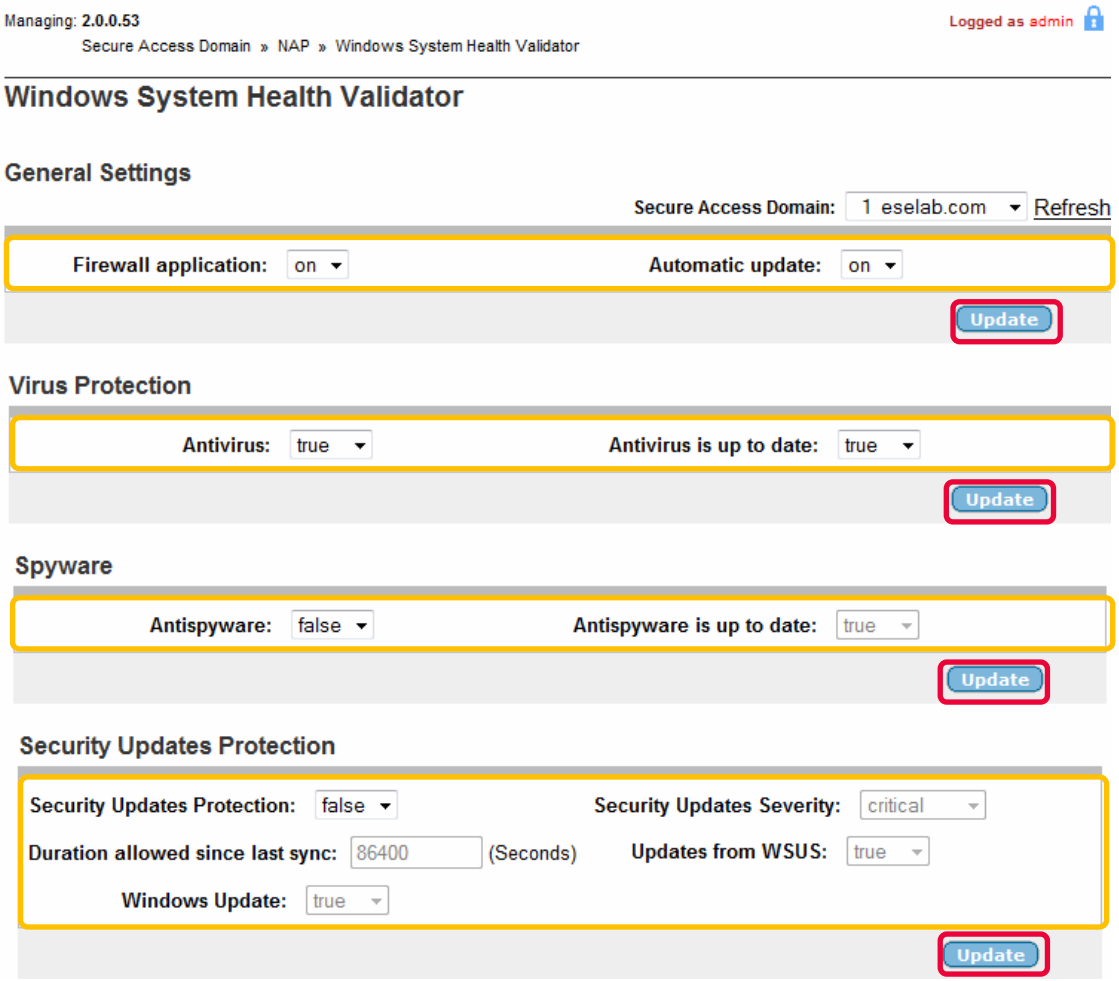
1 Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain* then *NAP*. Modify base NAP settings as needed and then click *Update*.



Automatic Remediation <true | false>	When true will automatically apply the necessary settings to allow a non-compliant computer to become compliant.
Trouble Shooting URL	Provides the NAP client with a URL to provide details for becoming compliant as well as obtaining the latest patches.
Full Access for a Limited Time <true | false>	When true provides full access for non-compliant devices for a limited time.
Date <YYYY-MM-DD>	Specifies a date where limited access for non-compliant devices starts.
Time <HH:MM:SS>	Specifies a time where limited access for non-compliant devices starts.

For each NAP setting modified click Update in the respected section to apply the changes.

2 Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *NAP* then *Windows System Health Validator*. Modify the Windows System Health Validator settings as required and then click *Update*.

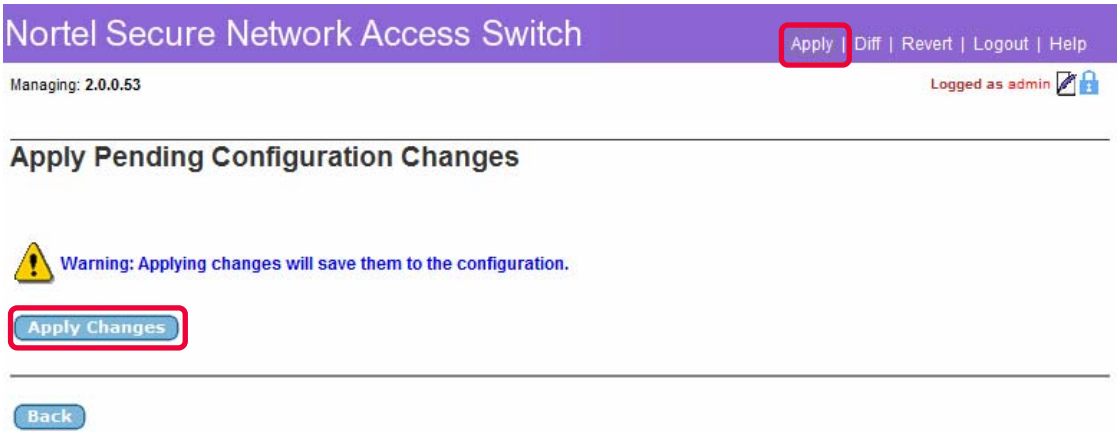


Firewall application <on | off>	When on verifies that a Firewall is present and operational on the client
Automatic update <on | off>	When on verifies that automatic updates are enabled for the firewall
Antivirus <true | false>	When true verifies that Antivirus is present and operational on the client
Antivirus is up to date <true | false>	When true verifies that automatic updates are enabled for Antivirus
Antispyware <true | false>	When true verifies that Antispyware is present and operational on the client.
Antispyware is up to date <true | false>	When true verifies that Antispyware is up to date and has the latest updates installed

Security Updates Protection <true | false>	When true the Windows System Health Verifier (WSHV) will validate the Windows endpoint's current software security patch levels.
Security Updates Severity < Critical | Important | Moderate | Low | All >	Instructs the windows System Health Verifier (WSHV) to validate the minimum level of all Windows security update patches on the Windows endpoint.
Duration allowed since last sync <3600 - 394200>	Designates the duration of time allowed to pass since the Windows endpoint was last updated its own copy of its Windows security update list from its security update source (Windows Update or Windows Server Update Service)
Updates from WSUS <true | false>	Designates whether Windows Server Update Service (WSUS) is an acceptable source for endpoints to obtain their Windows security update information.
Windows Update <true | false>	Designates whether Microsoft's Windows Update is an acceptable source for endpoints to obtain their Windows security update information.

For each NAP setting modified click Update in the respected section to apply the changes.

3 Apply and save the changes by clicking *Apply* and then *Apply Changes*.

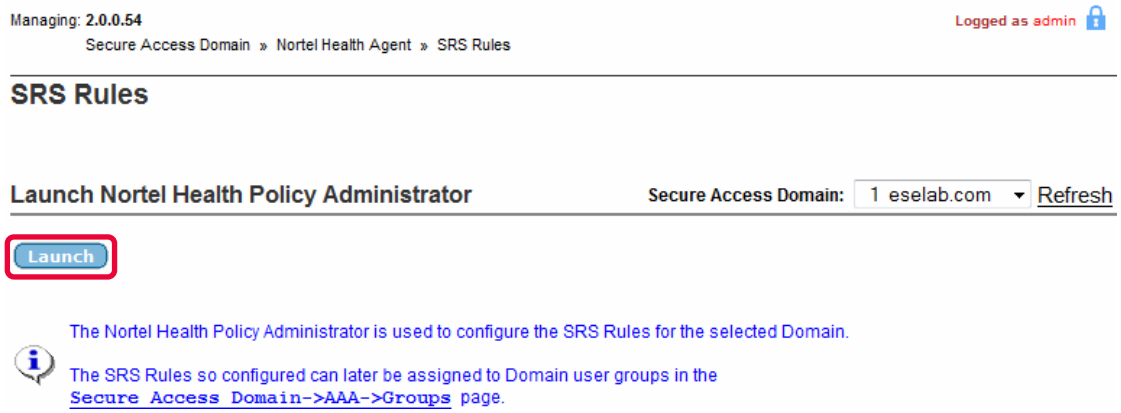


2.1.10 Nortel Health Agent Policy:

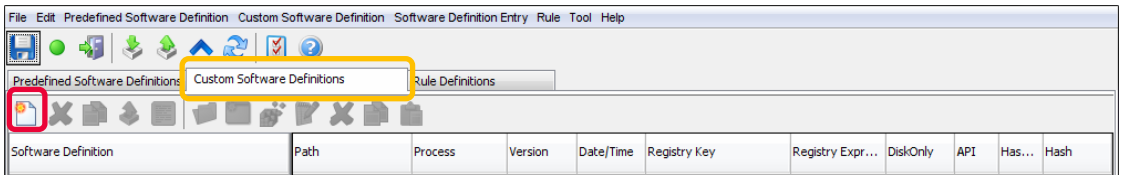
A Nortel Health Agent policy will be created on the Nortel Secure Network Access Switch and assigned to the NAPUsers group. The Nortel Health Agent Policy can be used to augment the NAP policy checks and in this example will be configured to check for the existence of a local file which must reside on the end-point for the Nortel Health Policy to pass.

A Nortel Health Agent Policy can be defined on the Secure Network Access Switch using the Browser Based Interface with the following steps:

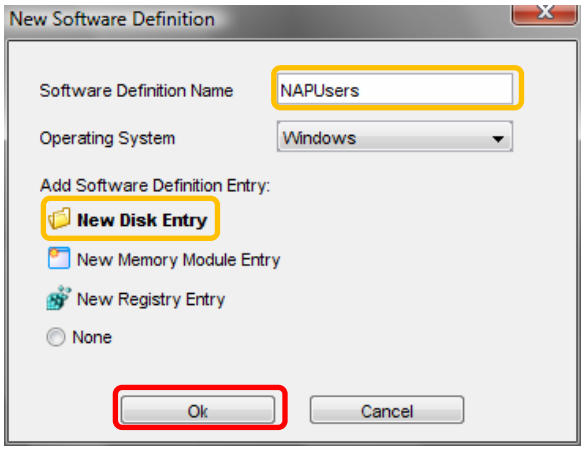
1 **Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *Nortel Health Agent* then *SRS Rules*. Create a new Nortel Health Policy by clicking *Launch*.**



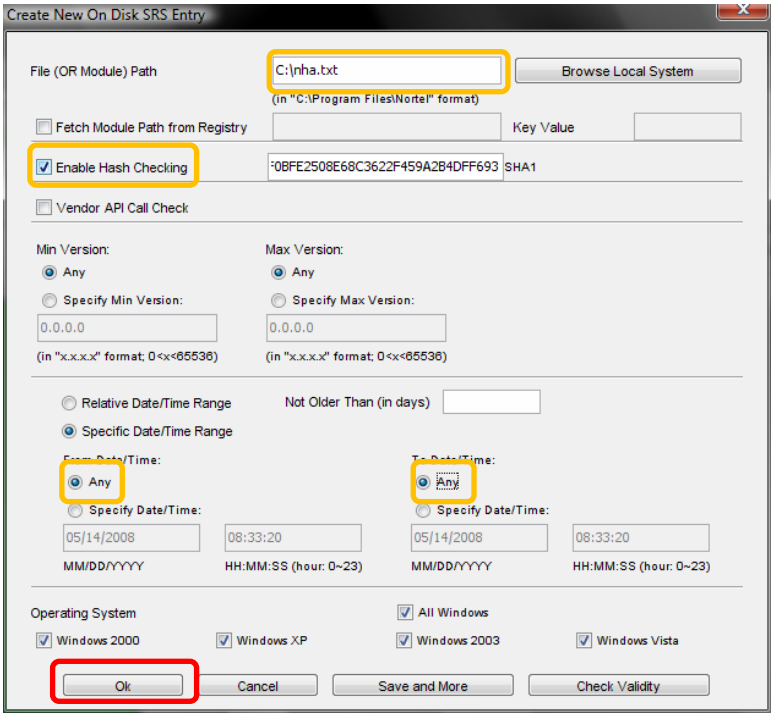
2 **In the Nortel Health Policy Administrator select the *Custom Software Definitions* tab and then click *New Definition*.**



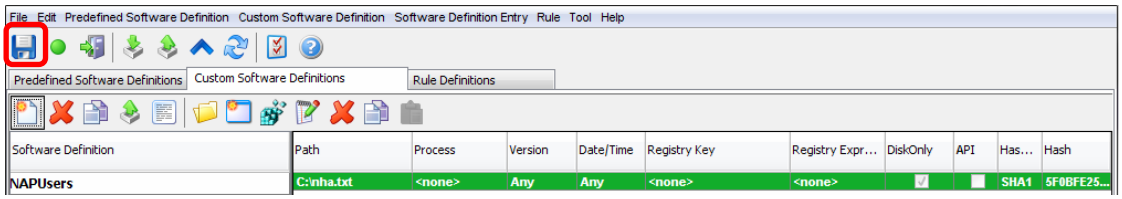
3 **In the New Software Definition window enter the name *NAPUsers* and select the option *New Disk Entry*. Click *Ok*.**



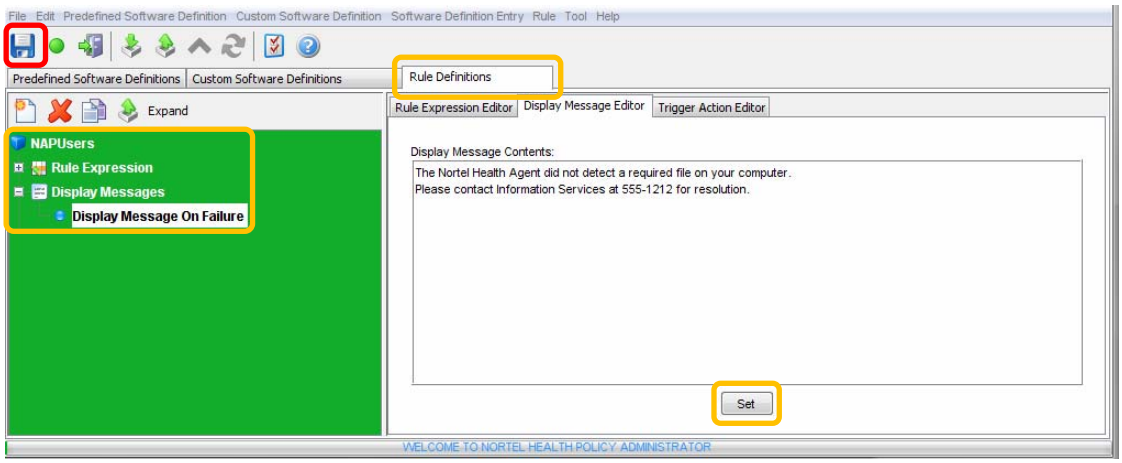
4 **In the *Create New On Disk SRS Entry* window click *Browse Local System* and select the location and name of the file to check (in this example c:\nha.txt). Optionally enable the option *Enable Hash Checking* and set the *From Date/Time* and *To Date/Time* options to *Any*. Click *OK*.**



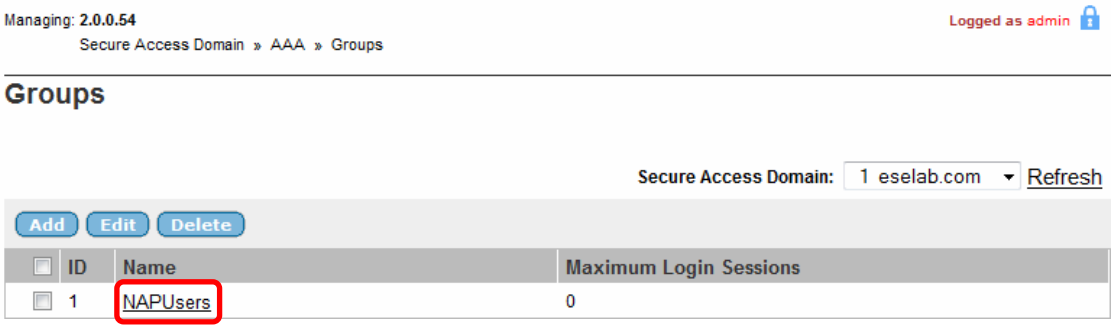
5 **A new Nortel Health Policy named NAPUsers has now created on the Secure Network Access Switch. Click *Save* and then exit the *Nortel Health Policy Administrator*.**



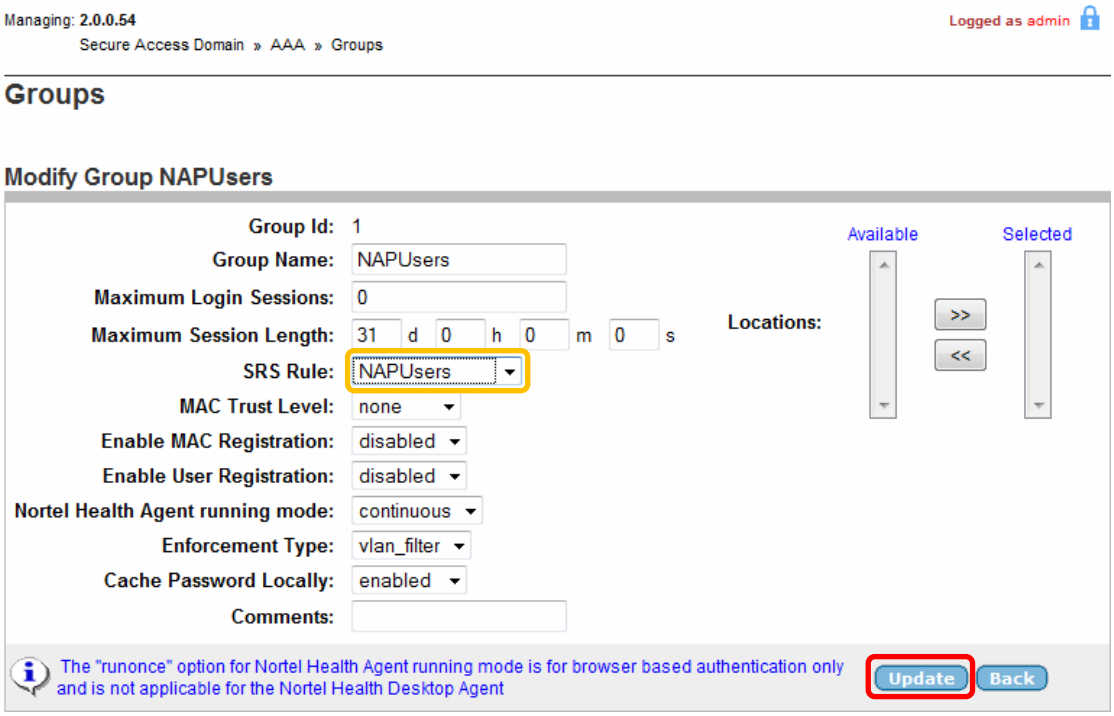
6 **Optionally specify a message that will be displayed to users in the event of policy failure. To specify a failure message click the *Rule Definition Tab*, expand the *NAPUsers* policy definition and then click *Display Message On Failure*. Type a message in the *Display Message Editor Content* field and click *Set* then *Save*.**



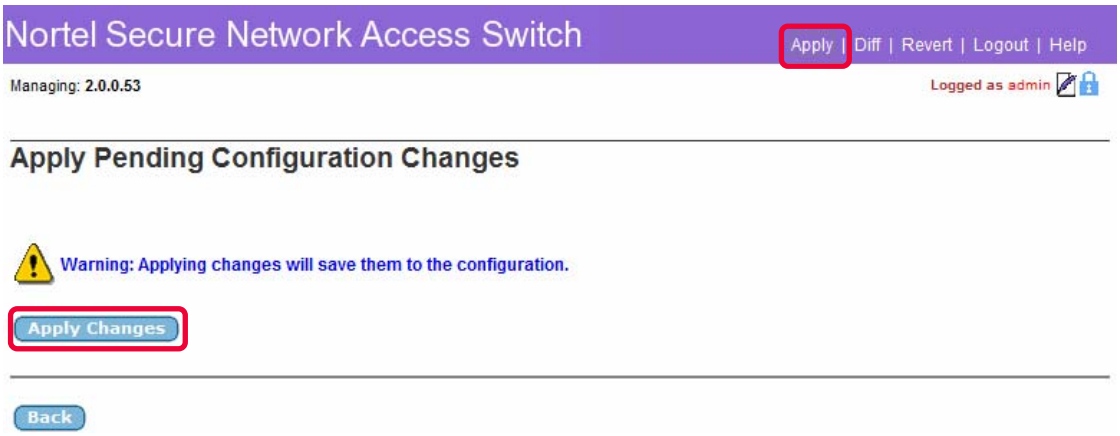
7 **Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *AAA* and then *Groups*. Click on the group named *NAPUsers*.**



8 **Using the SRS Rule pull-down menu select the Nortel Health Policy named *NAPUsers* then click *Update*.**



9 Apply and save the changes by clicking *Apply* and then *Apply Changes*.



2.2 Ethernet Routing Switch:

This section provides configuration steps required to configure a Nortel Ethernet Switch to support Microsoft Network Access Protection EAP clients. For this section the following configuration steps will be performed:

1. IP Addressing (Section 2.2.1)
2. Virtual LANs (Section 2.2.2)
3. RADIUS Server (Section 2.2.3)
4. EAPOL (Section 2.2.4)

2.2.1 IP Addressing:

The following IP addressing will be defined on the Nortel Ethernet Routing Switch to support switch management and RADIUS server communications:

- IP Address – 192.168.10.10
- Network Mask – 255.255.255.0
- Default Gateway – 192.168.10.1

IP addressing can be defined on a Nortel Ethernet Switch by using the following procedure:

1 Specify the IP address of the Ethernet Switch by issuing the *ip address switch <ip-address> netmask <network-mask>* command:

ERS5500(config)# ***ip address switch 192.168.10.10 netmask 255.255.255.0***

2 Specify a default gateway for the Ethernet Switch by issuing the *ip default-gateway <router-ip-address>* command:

ERS5500(config)# ***ip default-gateway 192.168.10.1***

2.2.2 Virtual LANs:

The following VLAN configuration will be defined on the Nortel Ethernet Switch:

- In compliance with Nortel's best practice implementation recommendations all ports will be removed from the default VLAN id 1.
- Three port based VLANs will be defined:
  - VLAN 10 – Dedicated management VLAN.
  - VLAN 30 – Unrestricted VLAN for workstations that pass NAP policy checks.
  - VLAN 50 – Remediated VLAN for workstations that fail NAP policy checks.
- The uplink port 48 will be configured to TagAll frames and will be added as a member of VLANs 10, 30 and 50.
- In compliance with Nortel's best practice implementation recommendations the uplink port 48 will be configured to discard untagged frames.

VLAN configuration can be defined on a Nortel Ethernet Switch by using the following procedure:

1 Rename the default VLAN by issuing the *vlan name <vlan-id> <vlan-name>* command:

ERS5500(config)# ***vlan name 1 Default***

2 **Create a management VLAN by issuing the *vlan create <vlan-id> name <vlan-name> type port* command:**

ERS5500(config)# ***vlan create 10 name SERVICES type port***

3 **Create a Green VLAN for trusted users by issuing the *vlan create <vlan-id> name <vlan-name> type port* command:**

ERS5500(config)# ***vlan create 30 name GREEN type port***

4 **Create a Yellow VLAN for remediated users by issuing the *vlan create <vlan-id> name <vlan-name> type port* command:**

ERS5500(config)# ***vlan create 50 name YELLOW type port***

5 **Enable 802.1Q tagging on the uplink port by issuing the *vlan ports <port-list> tagging tagall* command:**

ERS5500(config)# ***vlan ports 48 tagging tagall***

6 **Remove all port from the default VLAN by issuing the *vlan members remove <vlan-id> all* command.**

ERS5500(config)# ***vlan members remove 1 all***

7 **Add the management, Green and Yellow VLANs to the uplink port by issuing the *vlan members add <vlan-id> <port-list>* command.**

ERS5500(config)# ***vlan members add 10 48***

ERS5500(config)# ***vlan members add 30 48***

ERS5500(config)# ***vlan members add 50 48***

8 **Enabled the discard untagged frames feature on the uplink port by issuing the *vlan ports <port-list> filter-untagged-frame enable* command:**

ERS5500(config)# ***vlan ports 48 filter-untagged-frame enable***

9 **Specify the management VLAN ID created in step 2 by issuing the *vlan mgmt <vlan-id>* command:**

ERS5500(config)# ***vlan mgmt 10***

2.2.3 RADIUS Server:

The following RADIUS configuration will be defined on the Ethernet Routing Switch to authenticate NAP enabled Windows Vista and XP clients:

- RADIUS Server Host – 192.168.20.11 (Management IP Address of the SNAS)

- RADIUS Key – sharedkey

A RADIUS server host and shared key can be defined on a Nortel Ethernet Switch by using the following procedure:

1 Create a RADIUS server host entry specifying the Secure Network Access Servers management IP address by issuing the *radius-server host <ip-address>* command:

ERS5500(config)# ***radius-server host 192.168.20.11***

2 Enter and confirm a RADIUS shared key by issuing the *radius-server key* command:

ERS5500(config)# ***radius-server key***

Enter key: ******

Confirm key: ******

The RADIUS shared key must match the shared secret defined on the Secure Network Access Switch.

2.2.4 EAPOL:

The following EAPOL configuration will be defined on the Ethernet Routing Switch to authenticate NAP enabled Windows Vista and XP clients:

- EAPOL will be enabled on access ports 1 – 47 with the following parameters defined:
  - Re-authentication will be enabled with a re-authentication period of 300 seconds (5 minutes).
  - The quiet period will be lowered from 60 seconds to 10 seconds.
- EAPOL will be globally enabled on the switch.

EAPOL port settings and global status can be defined on a Nortel Ethernet Switch by using the following procedure:

1 Enable EAP support on access ports by issuing the *eapol status auto* command:

ERS5500(config)# ***interface fastEthernet 1-47***

ERS5500(config-if)# ***eapol status auto***

2 Enable EAP re-authentication support by issuing the *eapol re-authentication enable* command:

ERS5500(config-if)# ***eapol re-authentication enable***

3 Specify a re-authentication period by issuing the *eapol re-authentication-period <interval>* command:

ERS5500(config-if)# ***eapol re-authentication-period 300***

4 Specify a EAP quiet-interval by issuing the *eapol quiet-interval <interval>* command:

ERS5500(config-if)# ***eapol quiet-interval 10***

5 Globally enable EAPOL support on the Ethernet Switch by issuing the *eapol enable* command:

ERS5500(config-if)# ***exit***

ERS5500(config)# ***eapol enable***

2.3 Microsoft Windows Server 2003:

This section provides the minimum configuration steps required to configure a Windows 2003 Domain Controller to support authentication NTLM authentication requests and LDAP group associations from a Nortel Secure Network Access Switch. For this section the following configuration steps will be performed:

1. Active Directory Users (Section 2.3.1)
2. Active Directory Groups (Section 2.3.2)

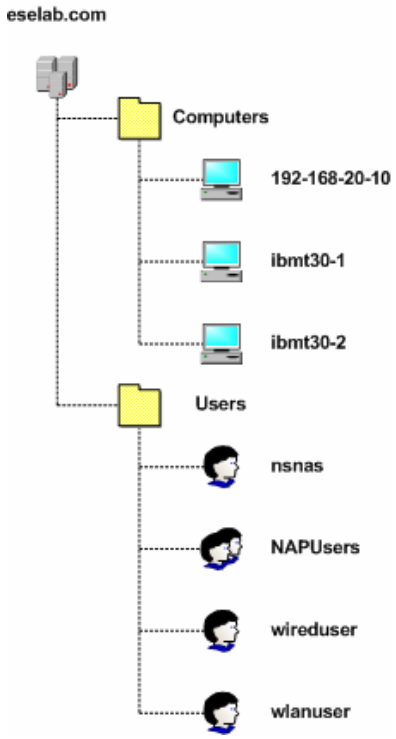


Figure 2.3 – Active Directory Tree

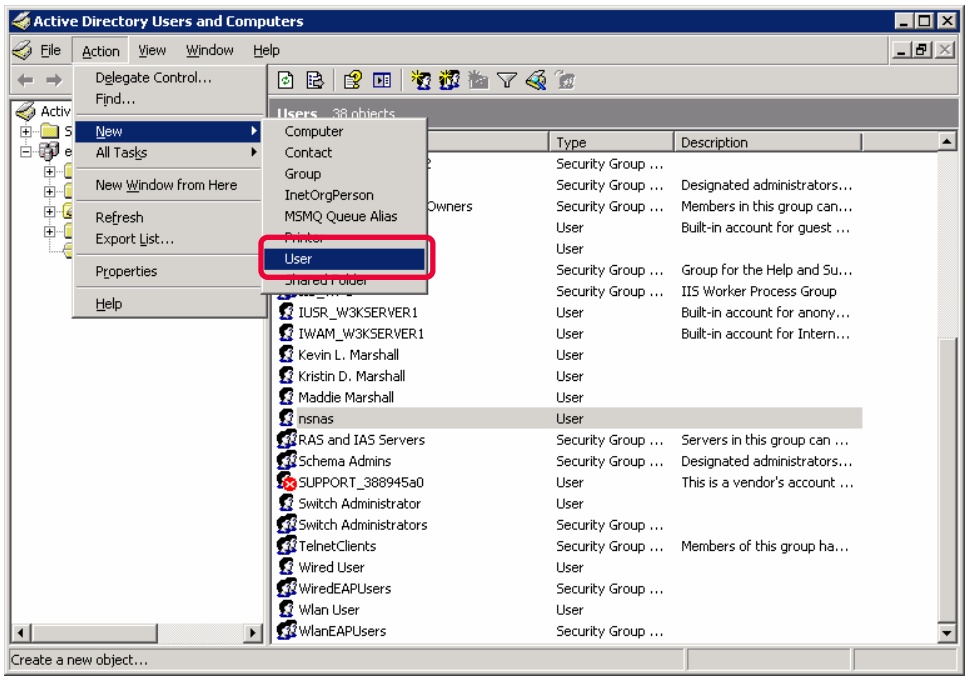
2.3.1 Active Directory Users:

The following Active Directory Users will be created on the Windows 2003 Domain Controller:

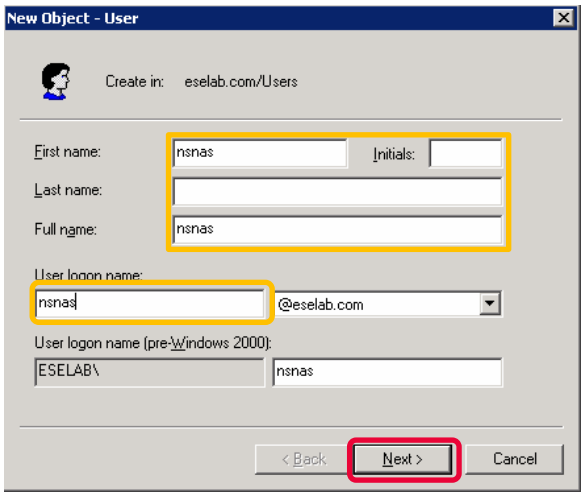
- A user named 'nsnas' used by the Nortel Secure Network Access Switch to perform the LDAP group lookup and associations.
- A user named 'wireduser' to test EAP authentication on the Nortel Ethernet Switch.

Active Directory Users may be created in Windows 2003 Server using the following steps:

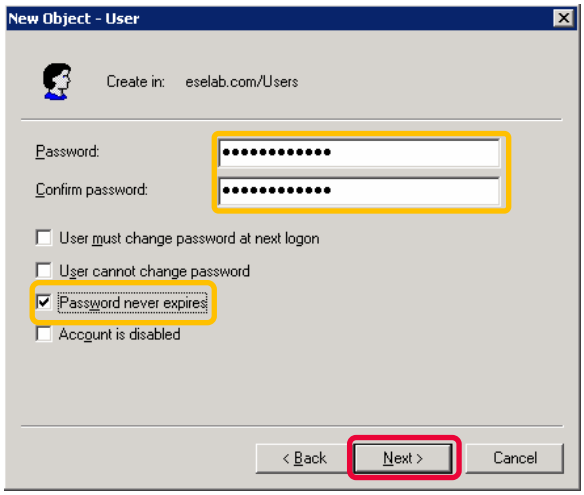
1 **Open the *Active Directory Users* Snap-In. Click on the *Users* container and then click *Action*, *New* and then *User*.**



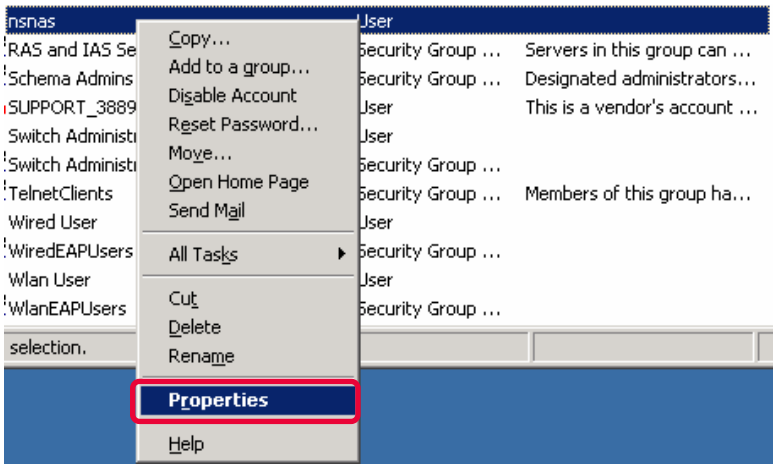
2 **In the *First Name* and *User logon name* fields enter the user name *nsnas* as defined in the *iSD Bind Name* field on the Nortel Secure Network Access Switch in Section 2.4. Click *Next*.**



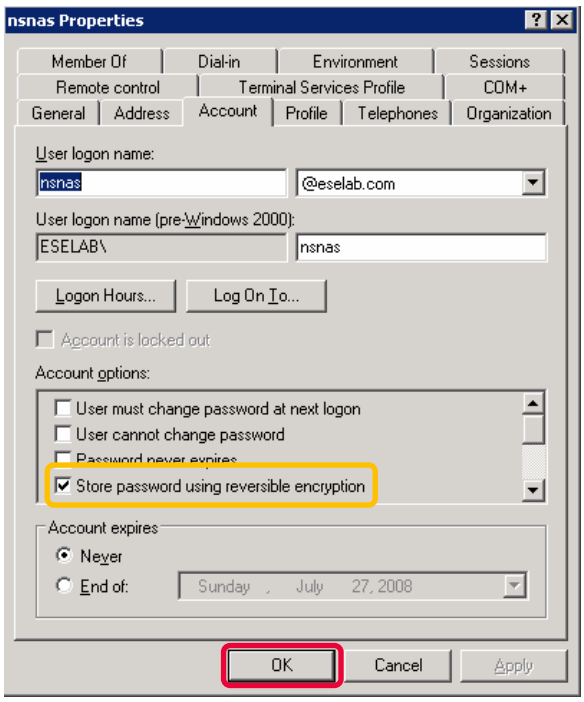
3 **In the *Password* fields enter and confirm the password as defined in the *iSD Bind Password* field on the Nortel Secure Network Access Switch in section 2.1.4.1. Check the option Password never expires and click *Next*. Verify the new account information and click *Finish*.**



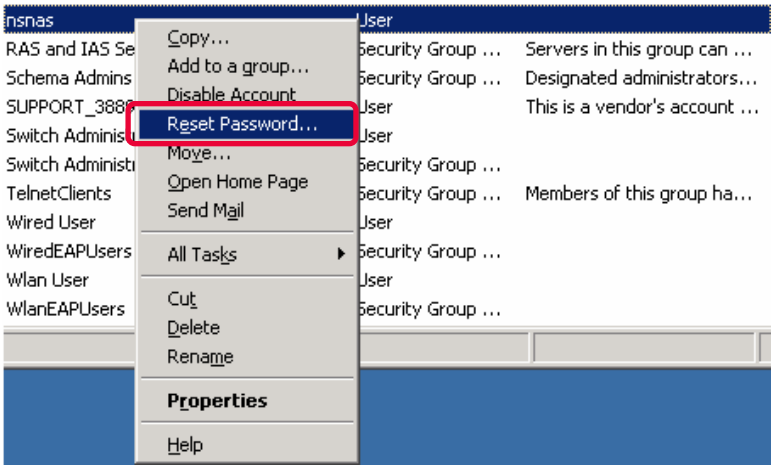
4 **In the *Active Directory Users* Snap-In highlight the user name *nsnas*, right click and then select *Properties*.**



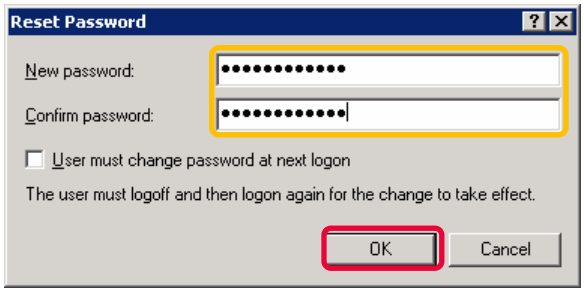
5 **Click on the *Account* tab and in *Account Options* check the option *Store password using reversible encryption*. Click *OK*.**



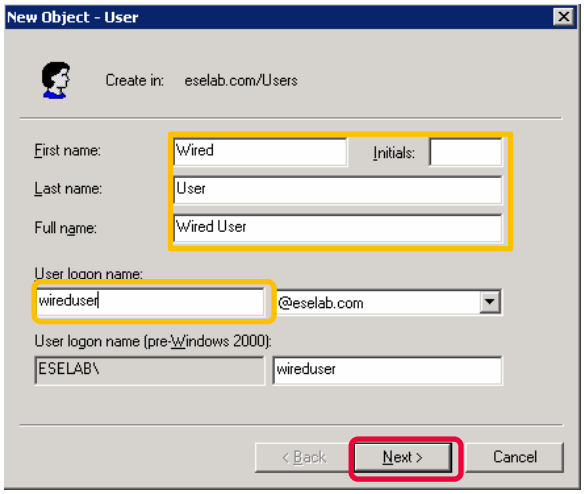
6 **In the *Active Directory Users* Snap-In highlight the user name *nsnas*, right click and then select *Reset Password*.**



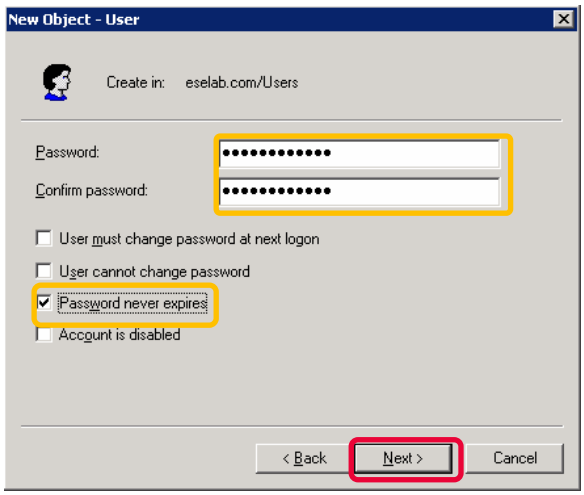
7 **In the *Password* fields enter and confirm the password as defined in the *iSD Bind Password* field on the Nortel Secure Network Access Switch in section 2.1.4. Click *OK*.**



8 **In the *Active Directory Users* Snap-In add a new user. Enter the appropriate user information for the Wired EAP test user and click *Next*.**



9 **Enter and confirm a password for the Wired EAP test user. Check the option *Password never expires* and click *Next*. Verify the new account information and click *Finish*.**



2.3.2 Active Directory Groups:

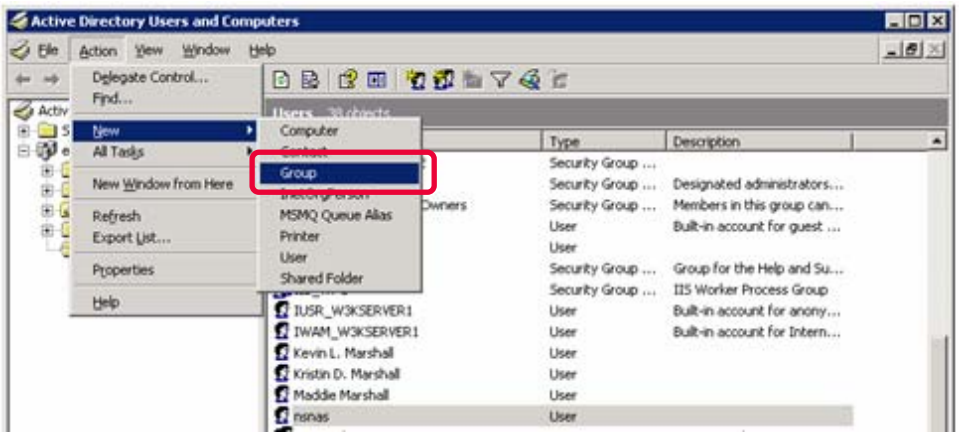
The following Active Directory Group will be created on the Windows 2003 Domain Controller:

- A group named 'NAPUsers' used for Wired PEAP user authentication will be created which matches the local group name defined on the Nortel Secure Network Access Switch.
- The user named 'wireduser' will be added as a member to the group 'NAPUsers'.

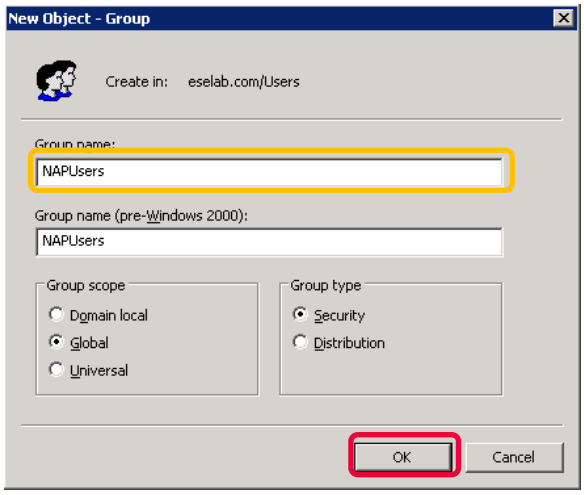
Windows does not return a specific group attribute for users that only belong to the Domain Users group. If the Domain Users group is used the default group setting on the Nortel Secure Network Access Switch is required.

Active Directory Groups may be created in Windows 2003 Server using the following steps:

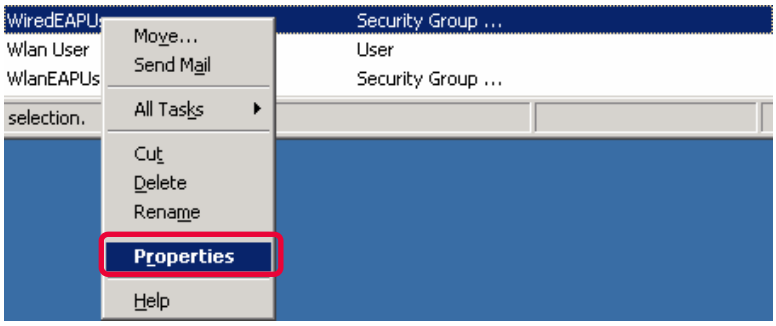
1 Open the *Active Directory Users* Snap-In. Click on the *Users* container and then click *Action*, *New* and then *Group*.



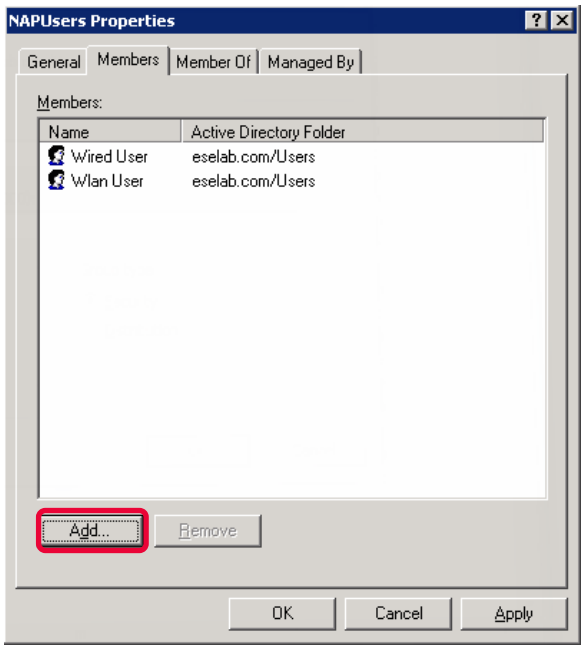
2 In the Group name field enter the name *NAPUsers* and click *OK*.



3 **In *Active Directory Users* Snap-In highlight the group *NAPUsers*, right click and select *Properties*.**



4 **Select the Members tab and click *Add*. Type the name of the Wired test user and click *OK* to add the user to the group. Click *Add* and type the name of the WLAN test user and click *OK*. Click *Apply*.**



2.4 Windows XP Professional:

This section provides configuration steps required on a Windows XP Professional SP3 Workstation to enable the Network Access Protection EAP client. For this section the following configuration tasks will be performed:

1. Services (Section 2.4.1)
2. NAP Enforcement Clients (Section 2.4.2)
3. Local Area Network Connection Properties (Section 2.4.3)

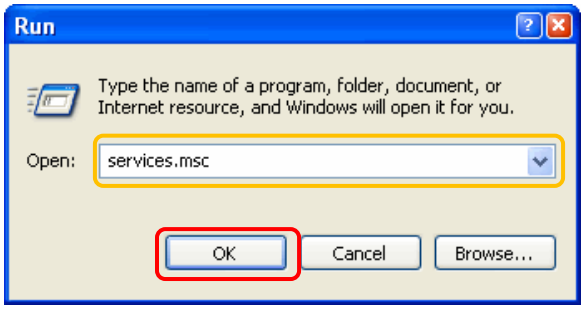
2.4.1 Services:

The following services need to be enabled on the Windows XP Professional SP3 workstation to support 802.1X authentication and Network Access Protection:

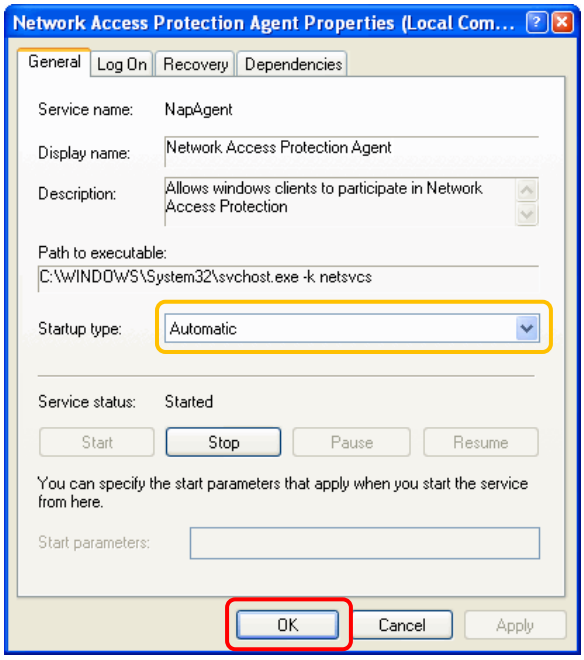
- Network Access Protection Agent – Allows the workstation to provide health information to the Network Policy Server on the Nortel Secure Network Access Switch.
- Wired AutoConfig – Provides 802.1X authentication services for wired interfaces.
- Nortel Health Agent – Allows the workstation to provide health information to the Nortel Health Policy Agent on the Nortel Secure Network Access Switch.

Network Access Protection and 802.1X services can be enabled on a Windows XP Professional SP3 workstation by using the following procedure:

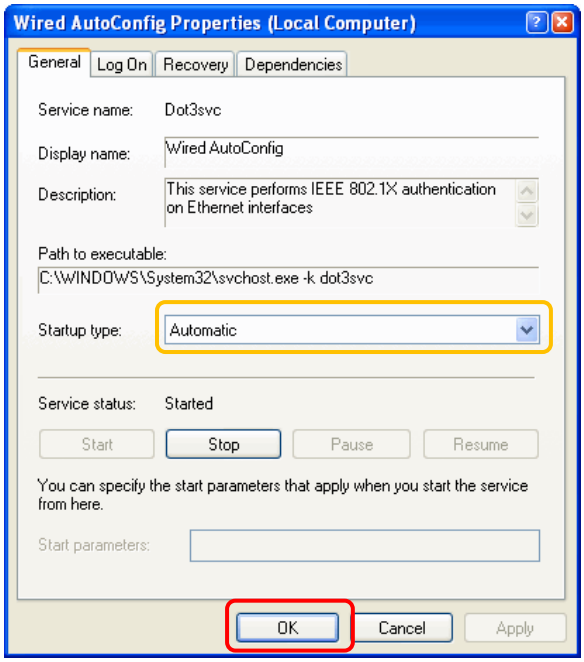
1 Click *Start* and then *Run*. Next to *Open* type *services.msc* and then click *OK*.



2 **In the list of services, right-click *Network Access Protection Agent* and select *Properties*. Set the *Startup type* to *Automatic* and then click *OK*.**

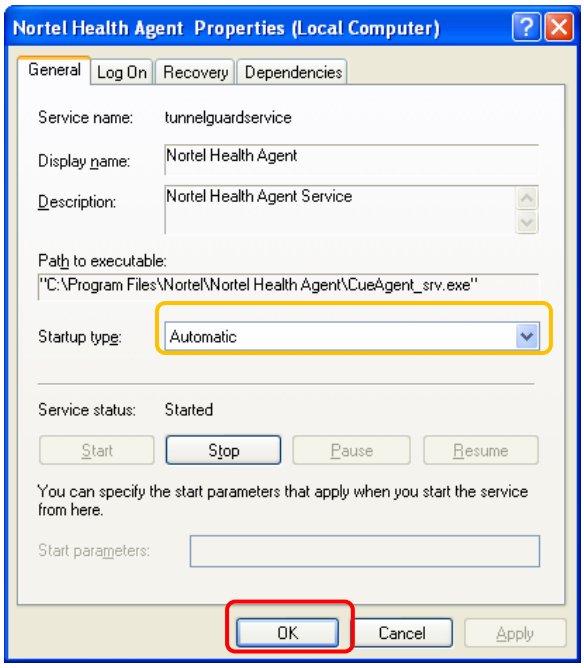


3 **In the list of services, right-click *Wired AutoConfig* and select *Properties*. Set the *Startup type* to *Automatic* and then click *OK*.**



4 **In the list of services, right-click *Nortel Health Agent* and select *Properties*. Set the**

***Startup type* to *Automatic* and then click *OK*.**



2.4.2 NAP Enforcement Clients:

The Network Access Protection Enforcement and Nortel NAP Enforcement Clients need to be enabled in Windows XP Professional SP3 to support endpoint inspection in an 802.1X Network Access Protection environment. Table 5.2 lists the Network Access Protection Enforcement Clients supported by a Windows XP SP3:

Enforcement Client	Client ID
DHCP Quarantine Enforcement Client	79617
Remote Access Quarantine Enforcement Client	79618
IPSec Relying Party	79619
Wireless Eapol Quarantine Enforcement Client	79620
TS Gateway Quarantine Enforcement Client	79621
EAP Quarantine Enforcement Client	79623
Nortel NAP Enforcement Client	10260993

Table 5.2 – Windows XP SP3 NAP Enforcement Clients

The EAP Quarantine Enforcement Client and Nortel NAP Enforcement Client can be enabled on a Windows XP Professional SP3 workstation by using the following procedure:

1 Click *Start*, *All Programs*, *Accessories* and then *Command Prompt*. At the command

prompt enable the EAP Quarantine Enforcement Client by entering the following:

C:\> ***netsh nap client set enforcement ID = 79623 ADMIN = "ENABLE"***

2 At the command prompt enable the Nortel NAP Enforcement Client by entering the following:

C:\> ***netsh nap client set enforcement ID = 10260993 ADMIN = "ENABLE"***

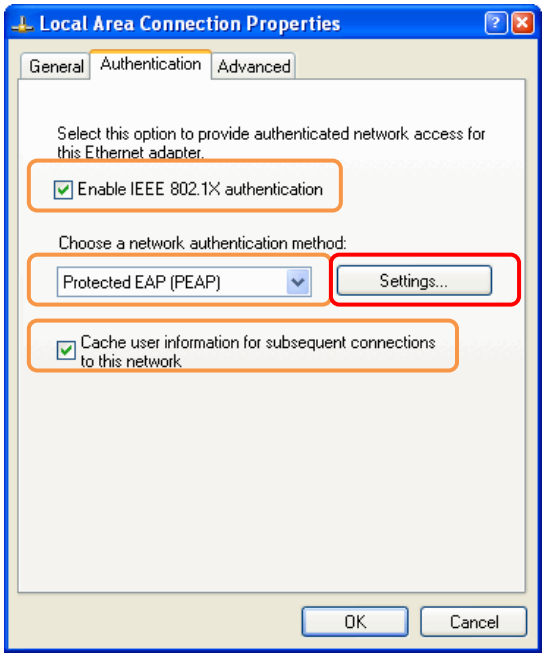
2.4.3 Local Area Connection Properties:

The following 802.1X configuration will be defined on a Windows XP Professional SP 3 workstation's Local Area Connection:

- IEEE 802.1X authentication will be enabled
- The EAP authentication method will be set to Protected EAP (PEAP) using MSCHAPv2
- User credential caching will be enabled
- TLS certificate validation will be enabled
- Quarantine checks will be enabled
- Single sign-on using domain credentials will be enabled

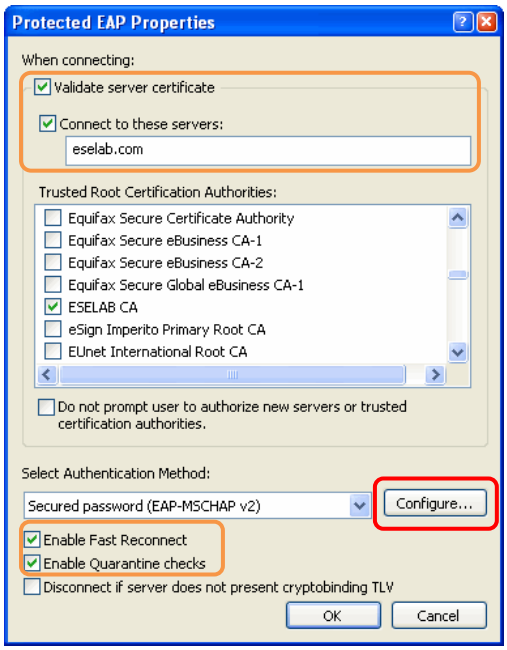
802.1X configuration can be configured on Windows XP Professional SP3 workstations Local Area Connection by using the following procedure:

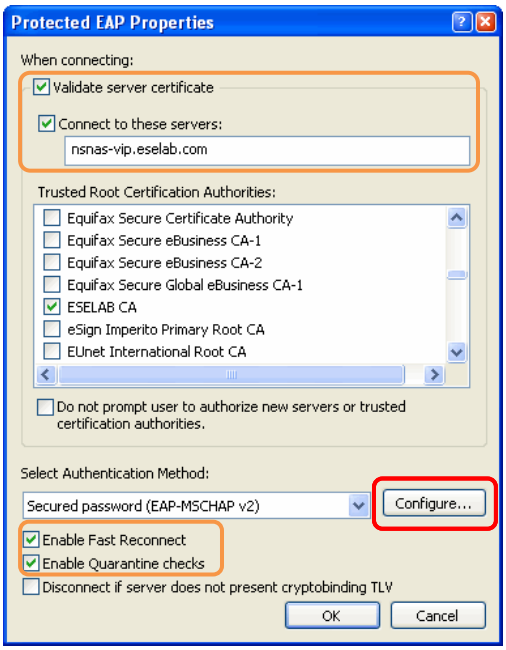
1 Click *Start*, *Control Panel* and then *Network Connections*. In the list of Network Connections right-click *Local Area Connection* and click *Properties*. Click on the *Authentication* tab and check the options *Enable IEEE 802.1X authentication* and *Cache user information for subsequent connections to this network*. Set the authentication method to *Protected EAP (PEAP)* and then click *Settings*.



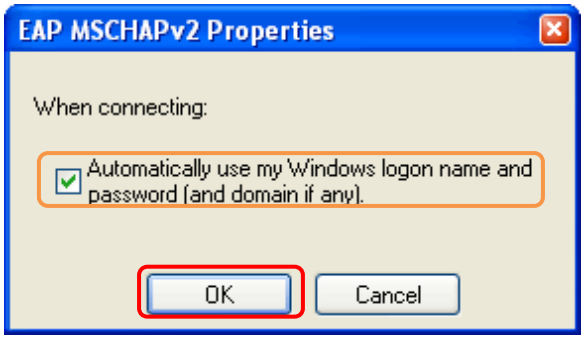
2 Check the options *Validate server certificate*, *Connect to these servers*, *Enable Fast*

***Reconnect* and *Enable Quarantine checks*. Below Connect to these servers enter the *domain name* for the network or *common name* of the server certificate installed on the SNAS. Click *Configure*.**





3 **Check the option *Automatically use my Windows logon name and password (and domain if any)*. Click *OK*. Close the Local Area Connection properties window.**



2.5 Windows Vista:

This section provides configuration steps required on a Windows Vista Workstation to enable the Network Access Protection EAP client. For this section the following configuration tasks will be performed:

1. Services (Section 2.5.1)
2. NAP Enforcement Client (Section 2.5.2)
3. Local Area Network Connection Properties (Section 2.5.3)

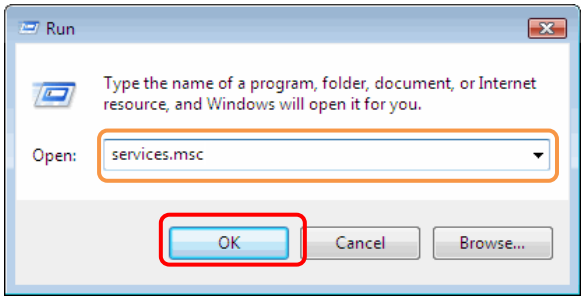
2.5.1 Services:

The following services need to be enabled on the Windows Vista workstation to support 802.1X authentication and Network Access Protection:

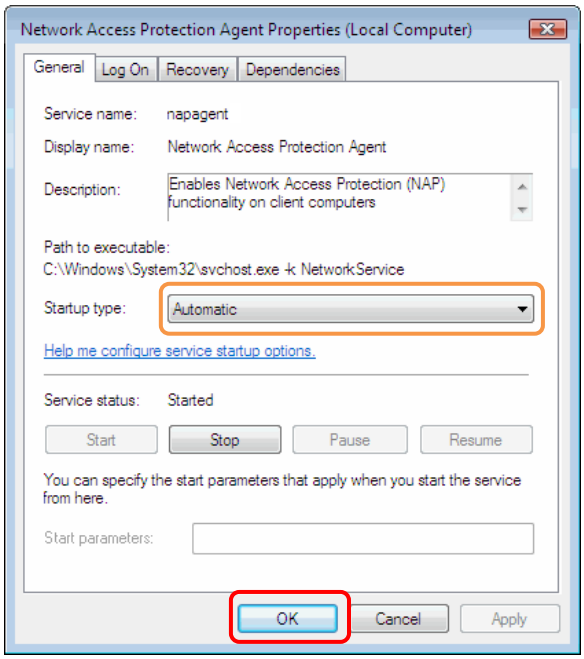
- Network Access Protection Agent – Allows the workstation to provide health information to the Network Policy Server on the Nortel Secure Network Access Switch.
- Wired AutoConfig – Provides 802.1X authentication services for wired interfaces.
- Nortel Health Agent – Allows the workstation to provide health information to the Nortel Health Policy Agent on the Nortel Secure Network Access Switch.

Network Access Protection and 802.1X services can be enabled on a Windows Vista using the following procedure:

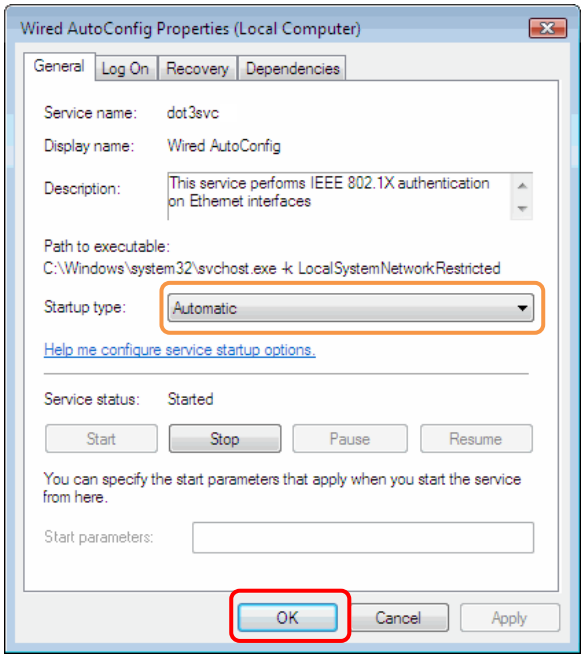
1 **Click *Start*, *All Programs*, *Accessories* and then *Run*. Next to *Open* type *services.msc* and then click *OK*.**



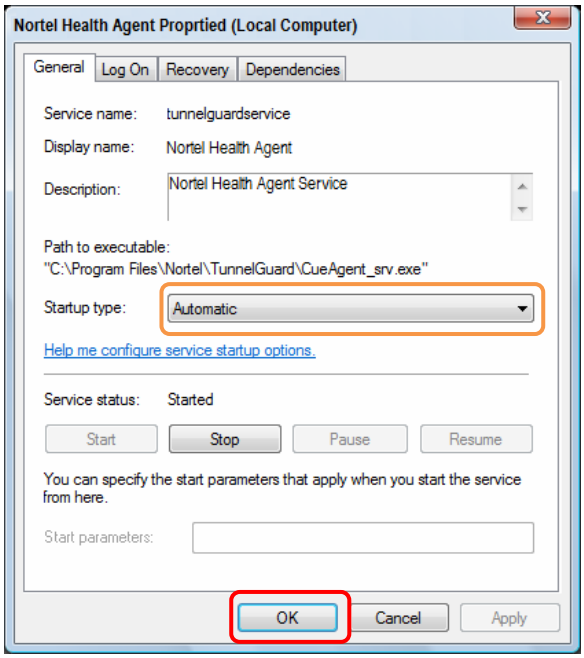
2 **In the list of services, right-click *Network Access Protection Agent* and select *Properties*. Set the *Startup type* to *Automatic* and then click *OK*.**



3 **In the list of services, right-click *Wired AutoConfig* and select *Properties*. Set the *Startup type* to *Automatic* and then click *OK*. Close the Services window.**



4 **In the list of services, right-click *Nortel Health Agent* and select *Properties*. Set the *Startup type* to *Automatic* and then click *OK*. Close the Services window.**



2.5.2 NAP Enforcement Client:

The Network Access Protection Enforcement and Nortel NAP Enforcement Clients need to be enabled in Windows Vista to support endpoint inspection in an 802.1X Network Access Protection environment. Table 6.2 lists the Network Access Protection Enforcement Clients supported by a Windows Vista:

Enforcement Client	Client ID
DHCP Quarantine Enforcement Client	79617
Remote Access Quarantine Enforcement Client	79618
IPSec Relying Party	79619
TS Gateway Quarantine Enforcement Client	79621
EAP Quarantine Enforcement Client	79623
Nortel NAP Enforcement Client	10260993

Table 6.2 – Windows Vista NAP Enforcement Clients

The EAP Quarantine Enforcement Client and Nortel NAP Enforcement Client can be enabled on a Windows Vista workstation by using the following procedure:

1 **Click *Start*, *All Programs*, *Accessories* and then *Command Prompt*. At the command prompt enable the EAP Quarantine Enforcement Client by entering the following:**

C:\> ***netsh nap client set enforcement ID = 79623 ADMIN = "ENABLE"***

2 At the command prompt enable the Nortel NAP Enforcement Client by entering the following:

C:\> ***netsh nap client set enforcement ID = 10260993 ADMIN = "ENABLE"***

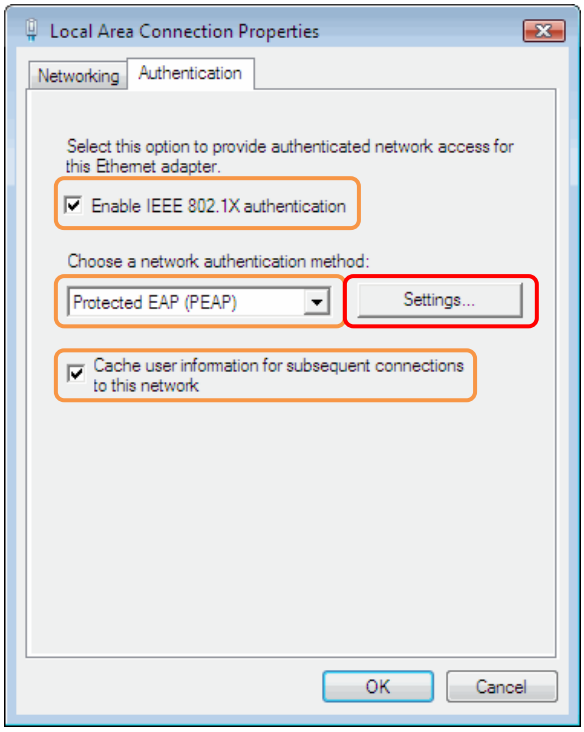
NAP enforcement client configuration may also be performed using Group Policy.

2.5.3 Local Area Connection Properties:

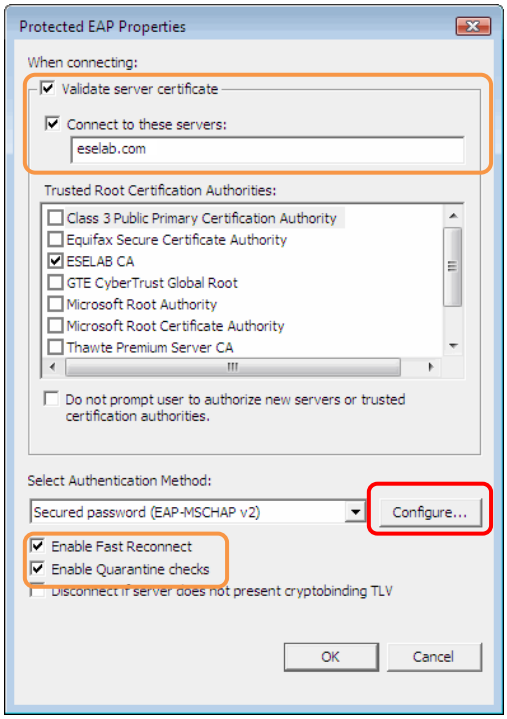
The following 802.1X configuration will be defined on a Windows Vista workstation's Local Area Connection:

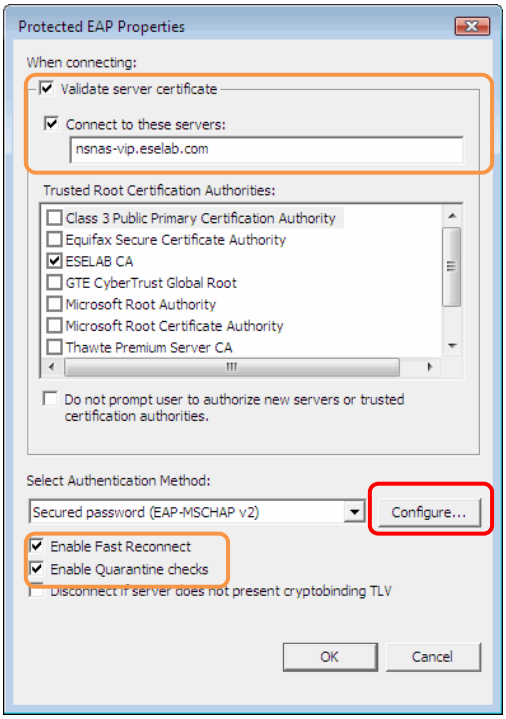
- IEEE 802.1X authentication will be enabled.
- The EAP authentication method will be set to Protected EAP (PEAP) using MSCHAPv2.
- User credential caching will be enabled.
- TLS certificate validation will be enabled.
- Quarantine checks will be enabled.
- Single sign-on using domain credentials will be enabled.

1	**Click *Start*, *Control Panel, Network and Internet* and *Network and Sharing Center*. In the left pane click *Manage Network Connections*. Right-click *Local Area Connection* and then click *Properties*. Click on the *Authentication* tab and check the options *Enable IEEE 802.1X authentication* and *Cache user information for subsequent connections to this network*. Set the authentication method to *Protected EAP (PEAP)* and then click *Settings*.**

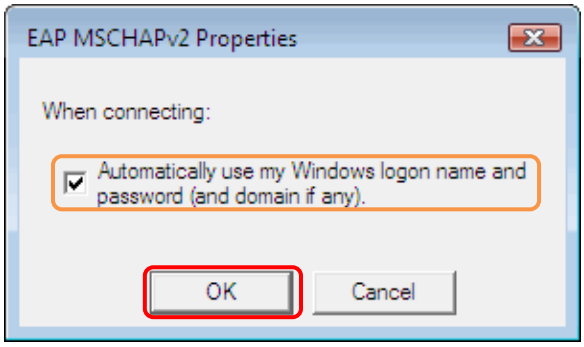


2	**Check the options *Validate server certificate*, *Connect to these servers*, *Enable Fast Reconnect* and *Enable Quarantine checks*. Below Connect to these servers enter the domain name for the network or common name of the server certificate installed on the SNAS. Click Configure.**





3 **Check the option *Automatically use my Windows logon name and password (and domain if any)*. Click *OK*. Close the Local Area Connection properties window.**

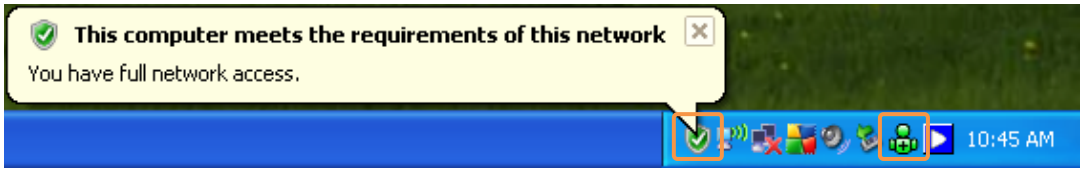


3. Verification:

3.1 Windows Workstation Compliant NAP / NHA State:

The following behavior will be seen on a Windows XP / Vista workstation upon successful PEAP authentication with compliant Network Access Protection and Nortel Health Agent client states:

1 The following message and icons will be displayed in the Windows toolbar upon successful PEAP authentication with compliant Network Access Protection and Nortel Health Agent client states.



2 The *ipconfig* command can be issued on the workstation to view the current IP addressing configuration which can be used to verify VLAN membership. In this example the DHCP scope for the Green VLAN *30* has been configured to provide the DNS suffix *green.eselab.com* which provides an easy way to identify VLAN membership.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : green.eselab.com
        IP Address. . . . . . . . . . . . : 192.168.30.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.30.1
```

3 On the Ethernet Switch the *show vlan interface vids <port-number>* NNCLI command can be used to view which VLANs are assigned to switch port. In this example a compliant Windows Workstation is connected to port *1* and has been placed in an unrestricted VLAN id *30* named *GREEN*.

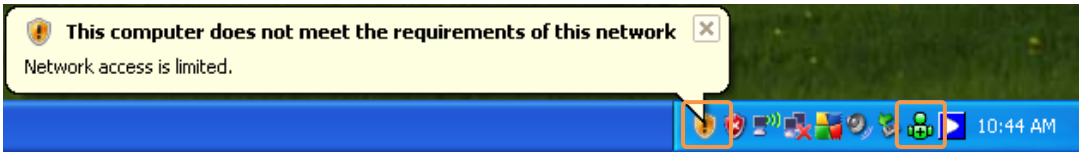
5500-1# ***show vlan interface vids 1***

```
Port VLAN VLAN Name         VLAN VLAN Name         VLAN VLAN Name
---- ---- ----------------  ---- ----------------  ---- ----------------
1    30   GREEN1
---- ---- ----------------  ---- ----------------  ---- ----------------
```

3.2 Windows Workstation Non-Compliant NAP State:

The following behavior will be seen on a Windows XP / Vista workstation upon successful PEAP authentication with non-compliant Network Access Protection and compliant Nortel Health Agent client states:

1 The following message and icons will be displayed in the Windows toolbar upon successful PEAP authentication with non-compliant Network Access Protection and compliant Nortel Health Agent client states.



2 The *ipconfig* command can be issued on the workstation to view the current IP addressing configuration which can be used to verify VLAN membership. In this example the DHCP scope for the Yellow VLAN 5*0* has been configured to provide the DNS suffix *yellow.eselab.com* which provides an easy way to identify VLAN membership.

C:\>***ipconfig***

```
Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : yellow.eselab.com
        IP Address. . . . . . . . . . . . : 192.168.50.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.50.1
```

3 On the Ethernet Switch the *show vlan interface vids <port-number>* NNCLI command can be used to view which VLANs are assigned to switch port. In this example a compliant Windows Workstation is connected to port *1* and has been placed in an unrestricted VLAN id *30* named *GREEN*.

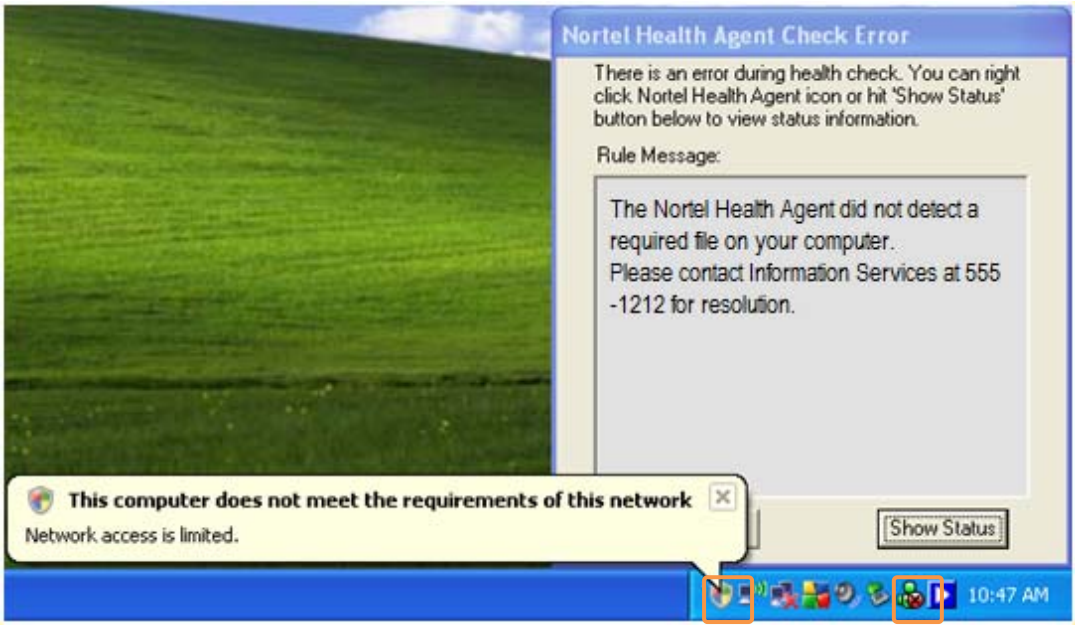
5500-1# ***show vlan interface vids 1***

```
Port VLAN VLAN Name         VLAN VLAN Name         VLAN VLAN Name
---- ---- ----------------  ---- ----------------  ---- ----------------
1    50   YELLOW
---- ---- ----------------  ---- ----------------  ---- ----------------
```

3.3 Windows Workstation Non-Compliant NHA State:

The following behavior will be seen on a Windows XP / Vista workstation upon successful EAP authentication with compliant Network Access Protection and non-compliant Nortel Health Agent client states:

1 The following message and icons will be displayed in the Windows toolbar upon successful PEAP authentication with compliant Network Access Protection and non-compliant Nortel Health Agent client states.



2 The *ipconfig* command can be issued on the workstation to view the current IP addressing configuration which can be used to verify VLAN membership. In this example the DHCP scope for the Yellow VLAN 5*0* has been configured to provide the DNS suffix *yellow.eselab.com* which provides an easy way to identify VLAN membership.

C:\>***ipconfig***

```
Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : yellow.eselab.com
        IP Address. . . . . . . . . . . . : 192.168.50.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.50.1
```

3 **On the Ethernet Switch the *show vlan interface vids <port-number>* NNCLI command can be used to view which VLANs are assigned to switch port. In this example a compliant Windows Workstation is connected to port *1* and has been placed in an unrestricted VLAN id *30* named *GREEN*.**

5500-1# ***show vlan interface vids 1***

```
Port VLAN VLAN Name         VLAN VLAN Name         VLAN VLAN Name
---- ---- ----------------  ---- ----------------  ---- ----------------
1    50   YELLOW
---- ---- ----------------  ---- ----------------  ---- ----------------
```

3.4 Nortel Secure Network Access Switch:

The following CLI commands can be issued on the Nortel Secure Network Access Switch to view sessions and debug RADIUS operations:

1 **Active 802.1X session information can be viewed by issuing the *info/sessions* command.**

>> Main# *info/sessions*

```
Number of currently active sessions: 2

Domain  Switch   Port    User                Source IP        Source Mac
        Login    Type    Vlan                Portal IP        Session Type
------- ------- -------- ------------------- ---------------- -----------------
      1       0        1 ESELAB\wireduser    0.0.0.0          00:09:6b:13:23:89
          15:23    dn_pc red(0)              -                802.1x
```

2 **Debugging may be enabled by issuing the *maint / starttrace* command. Note that tracing may be disabled by issuing *stoptrace*.**

>> Main# ***maint/starttrace***

```
Enter tags (list of all,aaa,dhcp,dns,ssl,nha,snas,patchlink,radius,nap) [all]:
Enter Domain (or 0 for all Domains) [0]:
Output mode (interactive/tftp/ftp/sftp) [interactive]:

>> Maintenance#
15:55:26.579662: Trace started
```

3.5 Nortel Ethernet Switch:

The following NNCLI commands can be issued on the Nortel Ethernet Switch to verify configuration and debug failed 802.1X authentications.

1 The EAP configuration and authentication status of a switch port may be viewed by issuing the *show eapol port <port-number>* command.

ERS5500-1# *show eapol port 1*

```
EAPOL Administrative State:  Enabled
EAPOL User Based Policies:  Disabled
EAPOL User Based Policies Filter On MAC Addresses:  Disabled
     Admin         Admin Oper ReAuth ReAuth Quiet  Xmit   Supplic Server  Max
Port Status   Auth Dir   Dir  Enable Period Period Period Timeout Timeout Req
---- -------- ---- ----- ---- ------ ------ ------ ------ ------- ------- ---
1    Auto     Yes  Both  Both Yes    3600   10     30     30      30      2
```

2 The VLAN membership of a specific port may be viewed by issuing the *show vlan interface vids <port-number>* command.

ERS5500-1# *show vlan interface vids 1-2*

```
Port VLAN VLAN Name         VLAN VLAN Name         VLAN VLAN Name
---- ---- ----------------  ---- ----------------  ---- ----------------
1    30   GREEN
2    40   YELLOW
---- ---- ----------------  ---- ----------------  ---- ----------------
```

3 The RADIUS Server configuration may be viewed by issuing the *show radius-server* command.

ERS5500-2# *show radius-server*

```
Password Fallback:  Disabled
Primary Host:  192.168.20.11
Secondary Host:  0.0.0.0
Port:  1812
Time-out:  2
Key:  ***************
Radius Accounting is  Disabled
AcctPort:  1813
```

4 **The list of configured VLANs and port membership may be viewed by issuing the *show vlan* command.**

ERS5500-1# *show vlan*

```
Id  Name                 Type     Protocol         User PID Active IVL/SVL Mgmt
--- -------------------- -------- ---------------- -------- ------ ------- ----
1   DEFAULT              Port     None             0x0000   Yes    IVL     No
        Port Members: NONE
10  SERVICES             Port     None             0x0000   Yes    IVL     Yes
        Port Members: 48
30  GREEN                Port     None             0x0000   Yes    IVL     No
        Port Members: 48
50  YELLOW               Port     None             0x0000   Yes    IVL     No
        Port Members: 48
Total VLANs: 3
```

5 **Advanced EAPOL diagnostics for a port may be viewed by issuing the *show eapol auth-diags interface <port-number>* command.**

ERS5500-1# ***show eapol auth-diags interface 1***

```
Port:  1
    EntersConnecting:                      5
    EapLogoffsWhileConnecting:             0
    EntersAuthenticating:                  2
    AuthSuccessWhileAuthenticating:        2
    AuthTimeoutsWhileAuthenticating:       0
    AuthFailWhileAuthenticating:           0
    AuthReauthsWhileAuthenticating:        0
    AuthEapStartsWhileAuthenticating:      0
    AuthEapLogoffWhileAuthenticating:      0
    AuthReauthsWhileAuthenticated:         0
    AuthEapStartsWhileAuthenticated:       0
    AuthEapLogoffWhileAuthenticated:       0
    BackendResponses:                      22
    BackendAccessChallenges:               20
    BackendOtherRequestsToSupplicant:      20
    BackendNonNakResponsesFromSupplicant:  18
    BackendAuthSuccesses:                  2
    BackendAuthFails:                      0
```

6 **EAPOL statistics for a port may be viewed by issuing the *show eapol auth-stats interface <port-number>* command.**

ERS5500-1# ***show eapol auth-stats interface 1***

```
Port:  1
    EapolFramesRx:          24
    BackendAuthFails:       0
    EapolFramesTx:          29
    EapolStartFramesRx:     2
    EapolLogoffFramesRx:    0
    EapolRespIdFramesRx:    2
    EapolRespFramesRx:      20
    EapolReqIdFramesTx:     3
    EapolReqFramesTx:       26
    InvalidEapolFramesRx:   0
    EapLengthErrorFramesRx: 0
    LastEapolFrameVersion:  1
    LastEapolFrameSource:   0009:6B13:2389
```

4. Appendix:

4.1 Realms:

Realms provide the ability for the Secure Network Access Server to route an authentication request to a specific authentication server (local, LDAP, NTLM etc) based on the user information contained within the RADIUS access request packet.

When a RADIUS client sends user credentials for authentication, a user name is often included. Within the user name are two elements:

1. Identification of the user account name
2. Identification of the user account location

For example the user name kmarshall@eselab.com includes the account name *kmarshall* and the account location *eselab.com*.

A realm name may be a prefix or suffix depending on the operating system, authentication type and client. Before defining a realm name it's important to understand the formatting of the authentication request to ensure that the authentication request will be processed correctly by the Nortel Secure Network Access Switch.

For example a PEAP authentication request from a Microsoft Windows XP client may include the Windows Domain name as a prefix such as *ESELAB\username*. To authenticate users in this example a realm named *ESELAB* or *eselab* would need to be created.

An EAP-TLS authentication request as well as host authentication will include the realm name in the suffix such as *user@eselab.com* or host/computer*@eselab.com*. To authenticate users in this example a realm named *eselab.com* would need to be created.

Username	Realm Name
kmarshall@eselab.com	eselab.com
host/ibm-t30-1@eselab.com	eselab.com
ESELAB\kmarshall	ESELAB or eselab

Table 4.1 – Example Realms

5. Software Baseline:

The following table provides the individual software releases for each Nortel Ethernet Routing Switch used in this document:

Nortel Platform	Software Release
Nortel Secure Network Access Switch 4050	v2.0.0.55
Nortel Health Agent	vV5.0.0.33
Nortel Ethernet Routing Switch 5500	v5.1.0.015
Microsoft Platform	**Software Release**
Windows Server 2003 Enterprise Edition	Service Pack 2
Windows XP Professional	Service Pack 3
Windows Vista Ultimate	Service Pack 1

Table 5.0 – Software Baseline

6. Reference Documentation:

Table 7.0 provides a list of additional Nortel and Microsoft Publications which may be referenced to for additional information:

Nortel Document Title	Location
Nortel Ethernet Routing Switch 5500 Series Configuration - Security (217463-C)	http://www.nortel.com/support
Nortel Secure Network Access Switch Configuration - Using BBI (323857-B)	http://www.nortel.com/support

Table 6.0 – Reference Documentation

Contact us

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact Nortel Technical Support. To obtain contact information online, go to www.nortel.com/contactus.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to www.nortel.com/erc.