
RWL Tech Note

Wireless 802.1x Authentication with Windows NPS



Prepared by
Richard Litchfield
HP Networking Solution Architect

Hewlett-Packard Australia Limited
410 Concord Road
Rhodes NSW 2138
AUSTRALIA

Date Prepared: 12-Aug-12



RWL Tech Note Wireless 802.1x Authentication with Windows NPS

Document Information

Prepared By: Richard Litchfield	Document Version No: 1.00
Reviewed By:	Document Version Date: 12-Aug-12
	Review Date:

Version History

Ver.	Ver. Date	Revised By	Description	Filename
0.80	10-Aug-12	Richard Litchfield	Initial draft	RWL TechNote – Wireless 802.1x Auth Config Guide v0.80.doc
1.00	12-Aug-12	Richard Litchfield	First release, with error conditions defined	RWL TechNote – Wireless 802.1x Auth Config Guide v1.00.doc

Proprietary Notice

Hewlett-Packard believes the information contained in this document is accurate as of its publication date.

Hewlett-Packard makes no warranty of any kind with regards to this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose

Hewlett-Packard shall not be held liable for errors contained herein and/or direct indirect, special, incidental or consequential damages in connection with furnishing, performance, and/or use of this material.

All information contained within this document, which relates to Hewlett-Packard and its partners (including but not limited to its functions, policies, procedures, decisions, officers, employees, agents, clients and all financial matters) shall be kept absolutely confidential.

No part of this document may be distributed to third parties unless authorised by Hewlett-Packard Australia.

© Copyright Hewlett-Packard Australia, 2012



Table of Contents

Proprietary Notice	2
1. Introduction	5
1.1. Purpose and Scope.....	5
1.2. Sample Configurations.....	5
1.3. Definitions and Abbreviations	5
1.4. Related Documents and References	6
1.5. Public References	6
1.5.1. <i>General Information</i>	6
1.5.2. <i>HP Networking</i>	6
1.5.3. <i>Specific References</i>	6
2. Solution Overview.....	7
3. Configuration	7
3.1. Equipment Used.....	7
3.2. Windows 2008 Server	7
3.2.1. <i>Windows Component Installation</i>	8
3.2.2. <i>Microsoft NPS</i>	8
3.2.3. <i>Windows Active Directory Users</i>	14
3.3. Controller Configuration	15
3.3.1. <i>Network Settings</i>	15
3.3.2. <i>Authentication Settings</i>	16
3.3.3. <i>Security – Certificates</i>	17
3.3.4. <i>Virtual Service Community Profiles</i>	18
3.4. Client Configuration.....	21
4. Testing	23
4.1. Wireless Client	23
4.2. Server Side	24
4.2.1. <i>Event Logs</i>	24
4.2.2. <i>Accounting</i>	26
5. Troubleshooting.....	27
5.1. Microsoft Event Viewer	27
5.1.1. <i>Microsoft Event Viewer Configuration</i>	27
5.1.2. <i>Microsoft Event Viewer Examples</i>	27
5.2. RADIUS Accounting.....	30
5.2.1. <i>Setup</i>	30
5.2.2. <i>Sample Account Output</i>	31
5.3. Other Available Diagnostic Tools.....	32
5.4. NTRadPing.....	32
6. Appendix A: Example Errors	33
6.1. Client Side Errors	33
6.1.1. <i>Incorrect Username</i>	33
6.1.2. <i>Incorrect Windows Domain</i>	34
6.1.3. <i>Incorrect Password</i>	35
6.1.4. <i>Server Certificate Required</i>	36
6.1.5. <i>Username Setting not Specified</i>	37



RWL Tech Note
Wireless 802.1x Authentication with Windows NPS

6.1.6. *Server Certificate Required and Username Setting*.....37
6.1.7. *Wireless Profile with TKIP or WPA*38
6.2. *Server Side Errors*.....39
6.2.1. *Invalid NAS Port Type*.....39
6.2.2. *Incorrect EAP*40



1. Introduction

1.1. Purpose and Scope

HP Networking is the networking division of Hewlett Packard. The extensive product line-up includes products that range from high-end core network functionality down to small SMB unmanaged switches. Products from a number of different families are brought together under the FlexNetwork banner, with the functional groupings of FlexFabric, FlexCampus and FlexBranch.

The information provided in this document is designed to assist a suitably skilled practitioner to implement 802.1x RADIUS authentication of wireless clients against a Windows 2008 NPS server.

1.2. Sample Configurations

HP Networking has developed one or more sample configurations to show possible use cases. They are samples only, and do not take into account specific requirements or restrictions that may be present in a customer production environment.

1.3. Definitions and Abbreviations

HP	Hewlett Packard
HPN	HP Networking
HPGM	HP Global Method (Project Management)
AP	Access Point (wireless)
CA	Certificate Authority
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
HA	High Availability
MSM	Multi-Service Mobility (the HP Wireless Solution)
NIC	Network Interface Card
NPS	Network Policy Server (part of Microsoft Windows)
OS	Operating System
POE	Power over Ethernet
RADIUS	Remote Authentication Dial In User Service
SSH	Secure Shell
SSID	Service Set Identifier (wireless)
VLAN	Virtual Local Area Network
VSC	Virtual Service Community (MSM wireless)



1.4. Related Documents and References

Version/Date	Author	Document Name
1.02 / Aug-2012	Richard Litchfield	RWL TechNote - RADIUS Authentication for ProCurve Switches
2.4b / Jun-2011	Brown / Kotsiopoulos / McCormick / Litchfield	MSM Example Configurations

1.5. Public References

1.5.1. General Information

<http://www.hp.com/go/convergedinfrastructure>

HP Converged Infrastructure

<http://support.hp.com>

Manuals, updates, guides, white papers are available for all HP products

<http://h30499.www3.hp.com/t5/Switching/ct-p/switching>

Support forums for all HP Networking products

1.5.2. HP Networking

<http://www.hp.com/go/networking>

The HP Networking starting point!

1.5.3. Specific References

<http://blogs.technet.com/b/nap/archive/2008/06/19/nap-802-1x-configuration-walkthrough.aspx>

TechNet blog covering multiple 802.1x switch configs with MS Win2008 NPS

<http://aaronwalrath.wordpress.com/2010/06/22/install-windows-2008-r2-nps-for-radius-authentication-for-cisco-router-logins/>

Installing Windows 2008 R2 NPS for RADIUS Authentication

[http://technet.microsoft.com/en-us/library/cc753655\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc753655(WS.10).aspx)

Microsoft reference material for NPS



2. Solution Overview

The example solution used in this document provides wireless connectivity to users authenticating to Microsoft Active Directory using 802.1x. The RADIUS server providing 802.1x functionality is NPS running on Microsoft 2008 Enterprise Server.

The MSM wireless controller is configured to proxy access to the Windows NPS RADIUS server. The controller is therefore in the pathway for authentication. A different configuration where the APs act as proxies instead of the controller is also possible, thereby removing the controller as a possible single point of failure.

3. Configuration

3.1. Equipment Used

The following components were used to build the example solution described in Section 2.

Device	IP Address	Location/Function
Windows 2008 R2 Enterprise Server	192.0.2.100	Running AD, DHCP, DNS, CA, NPS
HP ProCurve 2520-8G switch	192.0.2.254	POE switch
MSM710 Mobility Wireless Controller	192.0.2.101	Wireless controller
1 or more MSM wireless access points (these were MSM410s)	DHCP assigned	Access Points for wireless connection

3.2. Windows 2008 Server

A Windows 2008 R2 Enterprise server is the basis of this configuration. Other Windows server versions (eg Windows 2003) and variations (eg Windows Standard) would also work, but there are likely to be differences in specific configuration options and settings.

The Enterprise server is usually chosen to host RADIUS, because it allows clients to be defined as ranges of IP addresses, and does not have an upper limit on the number of RADIUS clients that can be defined.

The key Windows components in this configuration are:

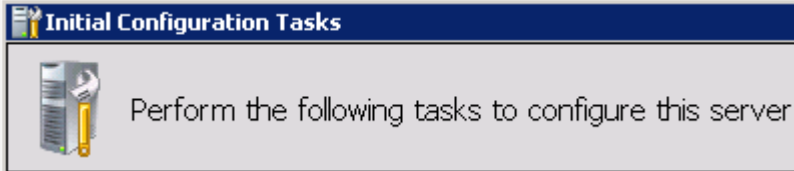
- Windows Server 2008 R2
- Active Directory (AD)
- Certificate Authority (CA)
- Dynamic Host Configuration Protocol (DHCP)
- Dynamic Name Service (DNS)
- Network Policy Server (NPS)

In a lab environment (such as the one described here), all of these components can be run on a single server. However, in a production environment, they may be run on multiple servers, including servers with clustering and replication facilities to provide high availability (HA).



3.2.1. Windows Component Installation

On a new server, you can install additional components using the “Add roles” option from the “Initial Configuration Tasks” window that automatically launches.

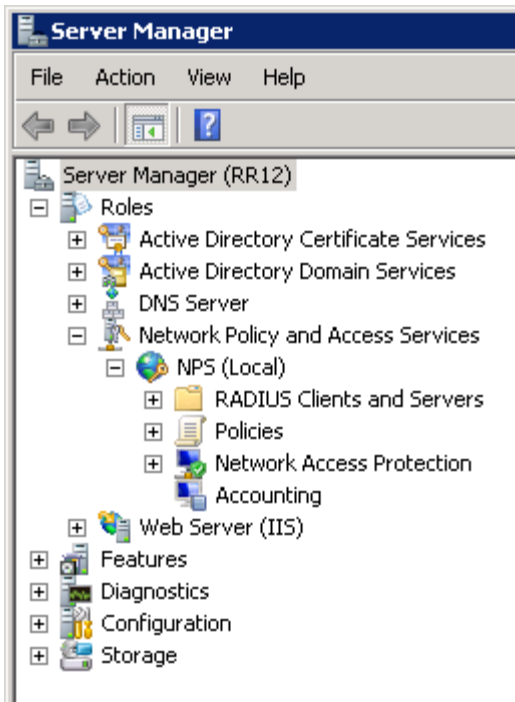


3.2.2. Microsoft NPS

In Windows 2008, Network Policy Server (NPS) replaces Internet Authentication Service (IAS) found in previous versions of Windows server operating systems.

3.2.2.1. Installation

- Install NPS by adding a server role from the Server Manager.
- The NPS console is available from the Server Manager.

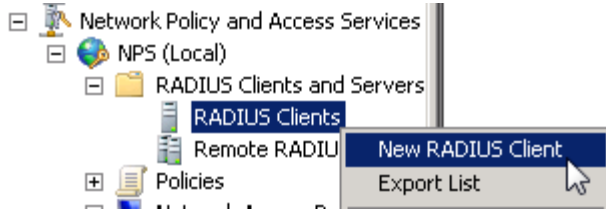




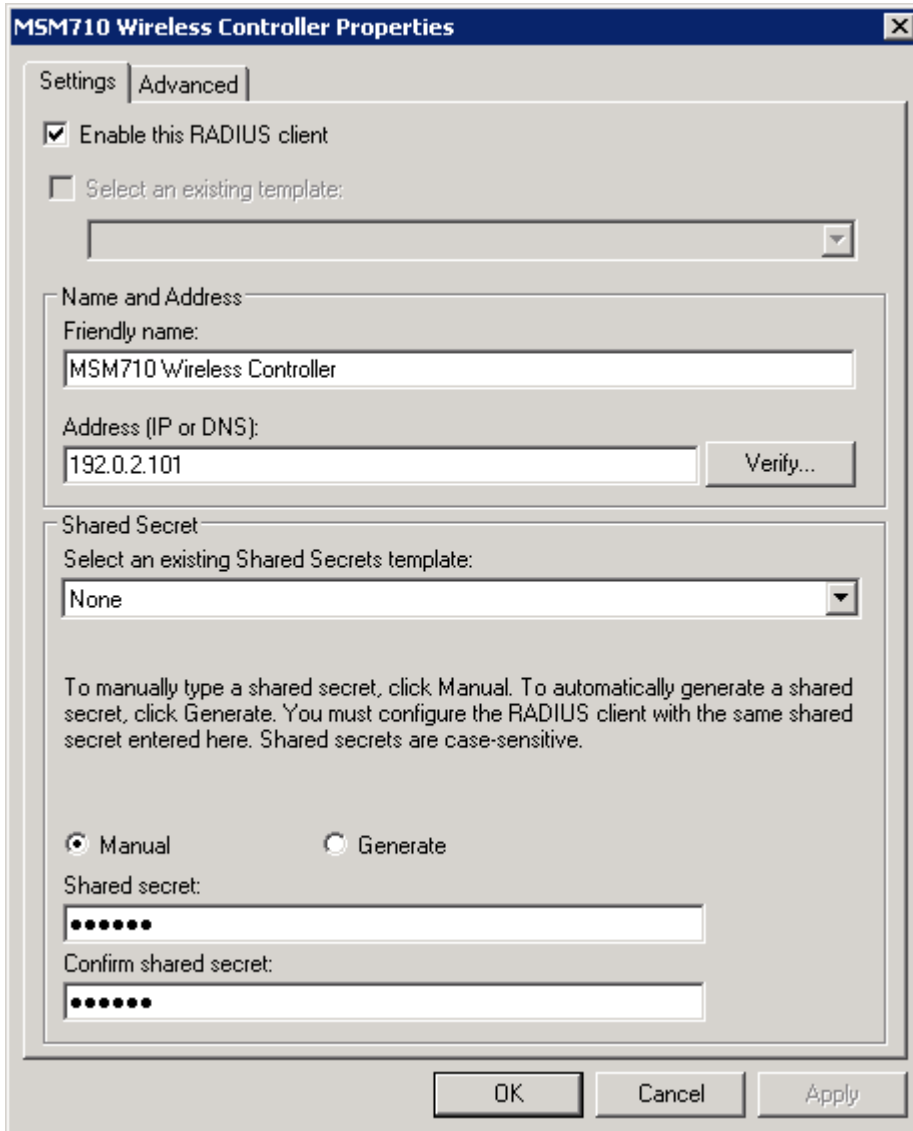
3.2.2.2. Add RADIUS Client

Add the MSM wireless controller to the RADIUS client list.

- Under RADIUS clients and Servers, right-click RADIUS Clients, and select New RADIUS Client.



- Enter the relevant details of the new device. Shared secrets must match the MSM secret.



- In the screenshot below, the new device “Switch-bvcore01” is shown at the top of the list.

RADIUS Clients					
RADIUS clients allow you to specify the network access servers, that provide access to your network.					
Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status	
MSM710 Wireless Controller	192.0.2.101	RADIUS Standard	No	Enabled	
RWL notebook	192.0.2.203	RADIUS Standard	No	Enabled	



3.2.2.3. Network Policy

A network policy needs to be defined to define who can connect, and with what criteria. The easiest way to create a new policy is to use the Standard configuration wizard (select NPS (local) in the Server Manager).

NPS (Local)

Getting Started

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

Standard Configuration

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

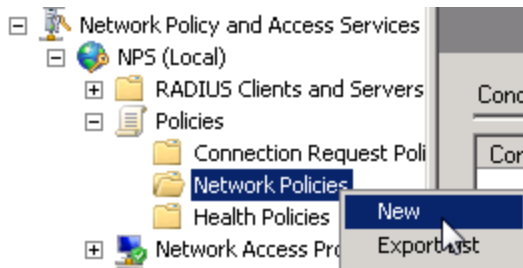
RADIUS server for 802.1X Wireless or Wired Connections

RADIUS server for 802.1X Wireless or Wired Connections

When you configure NPS as a RADIUS server for 802.1X connections, you create network policies that allow NPS to authenticate and authorize connections from wireless access points and authenticating switches (also called RADIUS clients).

[Configure 802.1X](#) [Learn more](#)

Or you can manually create a new one: under Policies, right-click Network Policies and select New.



The following screenshots show the correctly configured options for the network policy.

Network Policies

Network policies allow you to designate who is authorized to connect to the network, and the circumstances under which the

Policy Name	Status	Processing Order	Access Type	Source
Secure Wireless Connections (from wizard)	Enabled	1	Grant Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	999999	Deny Access	Unspecified
Connections to other access servers	Enabled	1000000	Deny Access	Unspecified



RWL Tech Note Wireless 802.1x Authentication with Windows NPS

- Use an appropriate name (this will appear in the logs); leave Type as unspecified.

The screenshot shows the 'Secure Wireless Connections (from wizard) Properties' dialog box with the 'Settings' tab selected. The 'Policy name' field contains 'Secure Wireless Connections (from wizard)'. The 'Policy State' section has 'Policy enabled' checked. The 'Access Permission' section has 'Ignore user account dial-in properties' checked. The 'Network connection method' section has 'Type of network access server' selected, with a dropdown menu showing 'Unspecified'. The 'Vendor specific' section has a text box containing '10'. Buttons for 'OK', 'Cancel', and 'Apply' are at the bottom right.

- Check that the conditions are specified correctly.
In this case, an additional condition is added – membership of a specific Windows group.

The screenshot shows the 'Secure Wireless Connections (from wizard) Properties' dialog box with the 'Conditions' tab selected. The text reads: 'Configure the conditions for this network policy. If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.' Below this is a table with two columns: 'Condition' and 'Value'.

Condition	Value
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11
Windows Groups	HPN\Wireless



RWL Tech Note Wireless 802.1x Authentication with Windows NPS

- Configure Constraints as shown. There are only changes in Authentication Methods; the other items remain unchanged from default.

The screenshot displays the 'Secure Wireless Connections (from wizard) Properties' dialog box, specifically the 'Constraints' tab. The 'Constraints' list on the left includes 'Authentication Methods', 'Idle Timeout', 'Session Timeout', 'Called Station ID', 'Day and time restrictions', and 'NAS Port Type'. The 'Authentication Methods' constraint is selected, showing a list of EAP types: 'Microsoft: Protected EAP (PEAP)'. Below this list are 'Add...' and 'Less secure authentication methods' checkboxes, with several options checked: 'Microsoft Encrypted Authentication', 'User can change password', 'Microsoft Encrypted Authentication', 'User can change password', 'Encrypted authentication', 'Unencrypted authentication', 'Allow clients to connect to this network', and 'Perform machine authentication'. Two smaller dialog boxes are overlaid: 'Edit Protected EAP Properties' and 'EAP MSCHAPv2 Properties'. The 'Edit Protected EAP Properties' dialog shows the 'Certificate issued' dropdown set to 'LABserver.hpn.demo', with fields for 'Friendly name', 'Issuer: hpn-LABSERVER-CA', and 'Expiration date: 5/08/2013 10:22:50 PM'. It also has checkboxes for 'Enable Fast Reconnect' and 'Disconnect Clients without Cryptobinding', and a list of EAP types including 'Secured password (EAP-MSCHAP v2)'. The 'EAP MSCHAPv2 Properties' dialog shows 'Number of authentication retries' set to 2 and the 'Allow client to change password after it has expired' checkbox checked.

- Microsoft PEAP needs to be added.
- Select PEAP, and edit so that the correct certificate is associated with it.



- No changes need to be made in the Settings tab.

Secure Wireless Connections (from wizard) Properties

Overview | Conditions | Constraints | Settings

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

- Standard
- Vendor Specific

Network Access Protection

- NAP Enforcement
- Extended State

Routing and Remote Access

- Multilink and Bandwidth Allocation Protocol (BAP)
- IP Filters
- Encryption
- IP Settings

To send additional attributes to RADIUS clients, select a RADIUS attribute, then click Edit. If you do not configure an attribute, it is not sent to your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

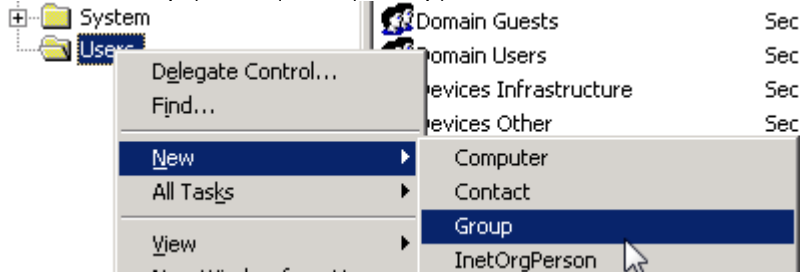
Add... Edit... Remove



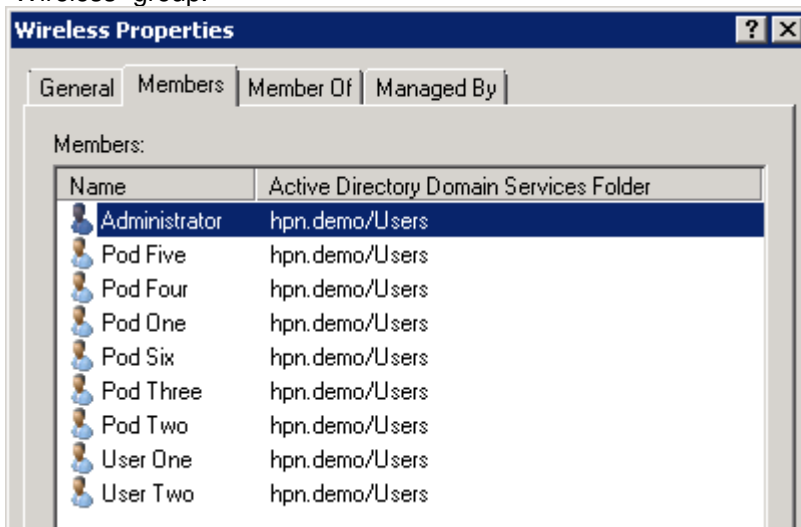
3.2.3. Windows Active Directory Users

You will need to have one or more groups that will have access to the devices via RADIUS. If a suitable group does not already exist, create one in AD.

- Create a Group (Users | New | Group)



- Select Global Security Group.
- Name and describe the group appropriately.
- Add users as required. The example bellow shows user1, user2 and several Pod Users in the "Wireless" group.





3.3. Controller Configuration

The wireless controller manages the APs, and in this configuration, also proxies the RADIUS requests to the Windows NPS server.

3.3.1. Network Settings

Configuration of the network for this example is very simple. The two APs are connected (untagged) to the VLAN for the controller LAN port, and the egress VLAN for the authenticated users is tagged on VLAN 100.

3.3.1.1. Controller

The controller LAN and Internet ports are configured as shown below.

IPv4 interfaces			
Interface	IP address	Mask	Allocation method
Internet port	192.0.2.101	255.255.255.0	STATIC
LAN port	192.168.1.1	255.255.255.0	STATIC

The LAN port (192.168.1.1) is also configured to provide DHCP addresses (which are used by the APs).

3.3.1.2. Network Profile

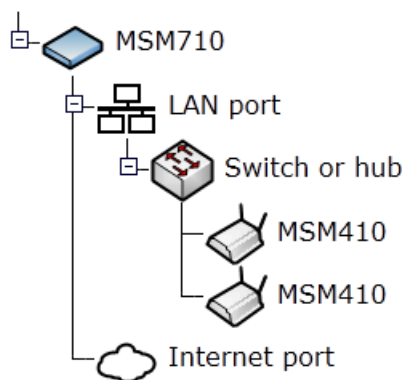
A network profile was created with VLAN 100. This is later used as the egress VLAN for the VSC.

Network profiles	
Name	VLAN ID
Hotel Lab	100
Internet port network	N/A
LAN port network	N/A

3.3.1.3. Access Point Connections

The APs get an IP address from the controller DHCP server on the LAN port (DHCP range 192.168.1.0/24). The network port of the AP is also tagged in VLAN 100, which is defined in the VSC as the egress VLAN for authenticated users (in Section 3.3.3).

Network topology





3.3.2. Authentication Settings

Configure a RADIUS server profile to communicate with Microsoft NPS. Here, the profile name is LabServer, connecting to NPS on 192.0.2.100.

RADIUS profiles			
Name	Primary server	Secondary server	NAS ID
LabServer	192.0.2.100	not configured	K062-00194

The Secret must match the secret configured in Section 3.2.2.2. All other settings are default.

Add/Edit RADIUS profile

Profile name

Profile name:

Settings

Authentication port:

Accounting port:

Retry interval: seconds

Retry timeout: seconds

Authentication method:

NAS ID:

Always try primary server first

Use message authenticator

Force NAS-Port to ingress VLAN ID

Override NAS ID when acting as a RADIUS proxy

Primary RADIUS server

Server address:

Secret:

Confirm secret:

Secondary RADIUS server (optional)

Server address:

Secret:

Confirm secret:

Authentication realms

Changing the realm configuration will logout all authenticated users.

Associated realms:

Support regular expressions in realm names

New realm:



RWL Tech Note Wireless 802.1x Authentication with Windows NPS

3.3.3. Security – Certificates

No changes were made to the certificates in the certificate store, or any certificate usage. The settings shown below are all default.

Trusted CA certificate store ?

ID	Issued to	Current usage	Start date	Expiration date	CRL	Delete
1	SOAP API Certificate Authority	SOAP Server	2005-04-06	2025-04-01	No	
2	Dummy Authority	RADIUS EAP	2007-04-12	2017-04-09	No	
3	Entrust.net Secure Server Certification Authority	Authorize.Net	1999-05-25	2019-05-25	No	
4	Management Console Dummy Authority	HP Management console	2010-05-19	2020-05-16	No	

PKCS #7 file or X.509 certificate:

Certificate and private key store ?

ID	Issued to	Issued by	Current usage	Start date	Expiration date	Delete
1	wireless.hp.internal	wireless.hp.internal	Web Management Tool, SOAP Server, HTML authentication, Billing records logging system	2010-11-03	2038-10-27	
2	Dummy Server Certificate	Dummy Authority	RADIUS EAP	2007-04-12	2017-04-09	
3	Management Console Default client certificate	Management Console Dummy Authority	HP Management console	2010-05-19	2020-05-16	

PKCS #12 file: PKCS #12 password:



3.3.4. Virtual Service Community Profiles

A VSC (virtual service community) is a collection of configuration settings that define key operating characteristics of the controller and controlled APs. One of the key elements of the VSC is the wireless SSID.

3.3.4.1. VSC for 802.1x Authentication

Create a VSC configured for 802.1x authentication (via the controller) based on the settings shown below. These settings can be modified as required, but the ones shown here are a good starting point.

VSC: LabTest | VSC profile

Global ?	Wireless protection WPA ?
Profile name: LabTest	Mode*: WPA2 (AES/CCMP)
Use Controller for: <input checked="" type="checkbox"/> Authentication <input type="checkbox"/> Access control	Key source: Dynamic
	<input type="checkbox"/> Terminate WPA at the controller
	*On radios in pure 802.11n mode WPA2 is always used instead of WPA
VSC ingress mapping ?	802.1X authentication ?
<input checked="" type="radio"/> SSID <input type="radio"/> Ethernet Switch	Authentication
	<input type="checkbox"/> Local <input checked="" type="checkbox"/> Remote
<input checked="" type="checkbox"/> Virtual AP ?	<input type="radio"/> Active directory <input checked="" type="radio"/> RADIUS: LabServer
WLAN	<input type="checkbox"/> Request RADIUS CUI
Name (SSID): LabTestX	General
DTIM count: 1	<input type="checkbox"/> RADIUS accounting: LabServer
<input checked="" type="checkbox"/> Broadcast name (SSID) <input type="checkbox"/> Advertise TX power <input checked="" type="checkbox"/> Broadcast filtering <input type="checkbox"/> Band steering	<input checked="" type="checkbox"/> Called-Station-Id content: BSSID
Wireless clients	RADIUS authentication realms ?
Max clients per radio: 100	<input type="checkbox"/> Use authentication realms <input type="checkbox"/> Use realms for accounting
Allow traffic between: all wireless clients	
<input type="checkbox"/> Quality of service	



RWL Tech Note Wireless 802.1x Authentication with Windows NPS

Priority mechanism: DiffServ

IP QoS profiles: <No IP QoS profiles defi...>

Upstream DiffServ tagging

Enable WMM advertising

+ Allowed wireless rates

Wireless mobility

Mobility traffic manager

If no matching network is assigned:

Block user

Consider the user at home

Subnet-based mobility

Fast wireless roaming

WPA2 opportunistic key caching

Wireless security filters

Restrict wireless traffic to:

Access point's default gateway

MAC address:

Custom:

MAC-based authentication

Authentication

Local

Remote

General

RADIUS accounting:

LabServer

Called-Station-Id content: Wireless Radio

Wireless MAC filter

Address list:

MAC address:

Remove Add

Allow Block

Wireless IP filter

Only allow traffic addressed to:

IP address: Mask: Add

Remove Selected Entry

Notes:

- The “Wireless mobility” check-box is enabled in this image, but it is not required for the 802.1x solution described.
- The “WPA2 opportunistic key caching” check-box is not enabled, but it could be.
- Wireless mobility and Fast wireless roaming both require the premium licence to enable.



3.3.4.2. Overview of Configured VSCs

The completed VSC: note the encryption type of AES and Authentication type 802.1x.

VSC: All | VSC profiles ?

Name	Ingress		Egress		Encryption			Authentication		
	SSID	VLAN	GRE	VLAN	TKIP	AES	WEP	802.1x	MAC	HTML
HP (Default)	HP		-	-	-	-	-	-	-	
LabTest	LabTestX		-	-	-		-		-	-

Add New VSC Profile...

= Access controlled
 = SSID Off
 = SSID On
 = SSID On and configured for broadcast

The two APs configured in Section 3.3.1.3 are both members of the “Lab” group. The Lab group has a single binding to the “Labtest” VSC.

Group: Lab | VSC bindings

VSC Name	VSC SSID	Egress network	Dual-radio behavior
LabTest	LabTestX	Hotel Lab (100)	Active on radios 1 and 2

The APs are shown below with the VSC mapping.

VSC: All | VSC mappings ? ?

Number of VSC mappings: 2

VSC name	AP name	Serial number	SSID	Radio	BSSID	Clients
LabTest	AP-labswitch-7-TW124C50G7	TW124C50G7	LabTestX	Radio 1	3c:d9:2b:7d:2f:70	1
LabTest	AP-labswitch-8-TW124C50MX	TW124C50MX	LabTestX	Radio 1	3c:d9:2b:7d:df:70	0



3.4. Client Configuration

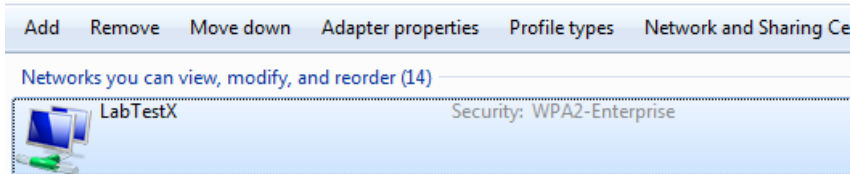
The client in this example is a Windows 7 notebook.

To avoid requests for certificates, a manually configured Wireless Network Profile is required.

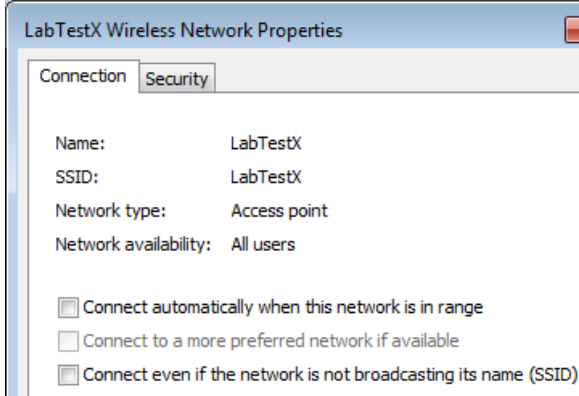
- From the “Manage wireless networks” dialog box, create a new network, and modify as shown below.

[Manage wireless networks that use \(Wireless Network Connection\)](#)

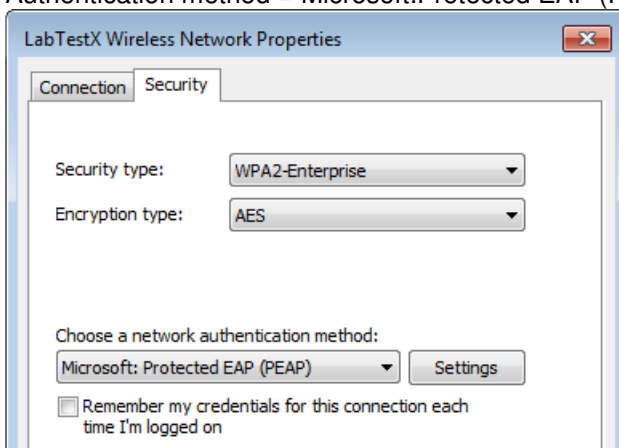
Windows tries to connect to these networks in the order listed below.



- Leave the settings on the Connection tab at default.

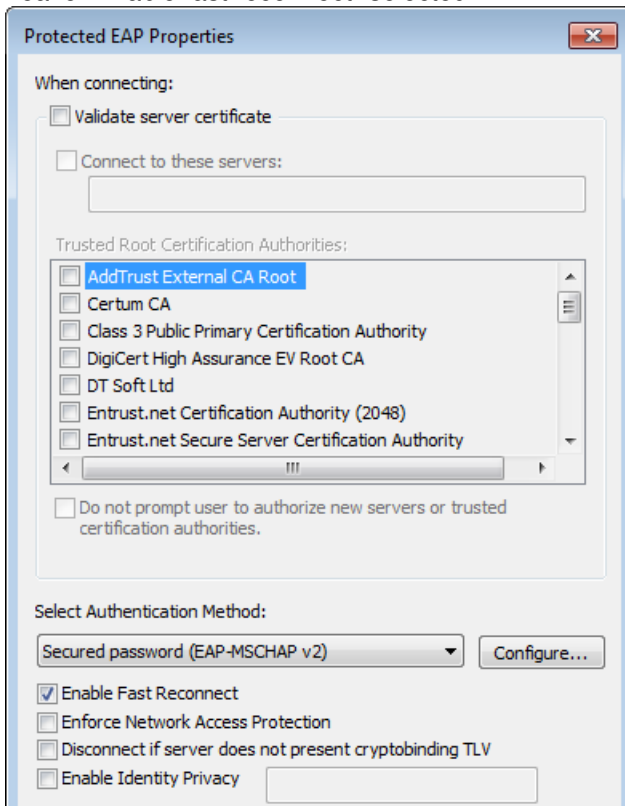


- On the Security tab, check the settings:
Security type = WPA2-Enterprise
Encryption type = AES
Authentication method = Microsoft:Protected EAP (PEAP)

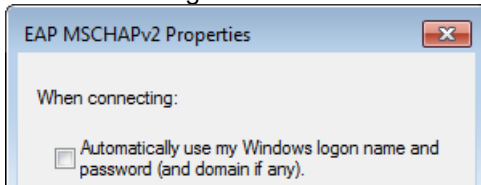




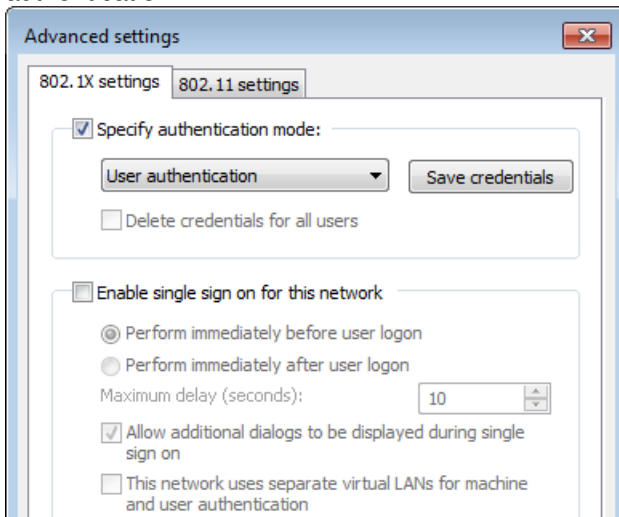
- Click the “Settings” button, and deselect the “Validate server certificate” check-box. Leave “Enable fast reconnect” selected.



- Click the “Configure...” button and deselect the “Automatically use...” check-box.



- On the Security tab, click the “Advanced settings” button, and change the authentication mode to “User authentication”.





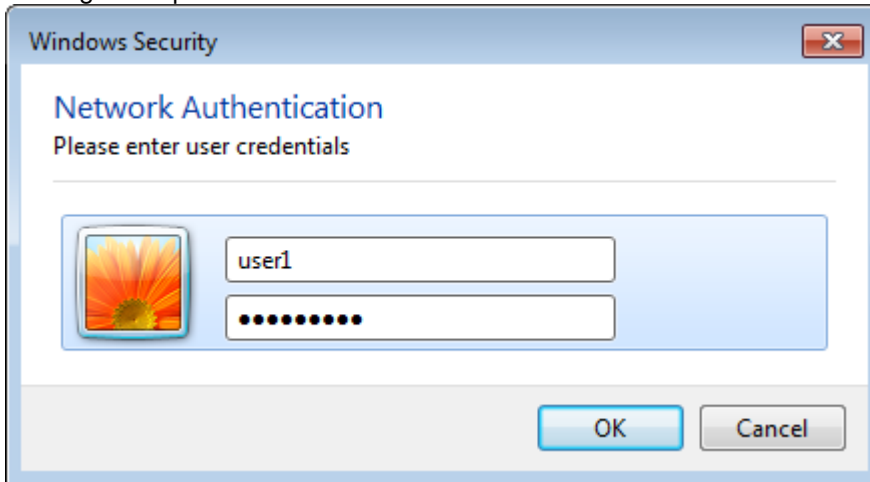
4. Testing

The test results after configuring the system as described are shown in this Section.

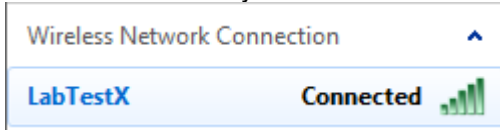
4.1. Wireless Client

The Windows client can successfully authenticate via 802.1x solution hosted by NPS.

- The login box presents OK



- Wireless connectivity is established



- An appropriate IP address is assigned.

```
C:\Users\rwl>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:

    Connection-specific DNS Suffix . : hpn.demo
    IPv4 Address. . . . . : 192.0.2.201
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.0.2.254
```



4.2. Server Side

4.2.1. Event Logs

The top two entries are the events recorded when user1 logged in (Section 4.1).

Network Policy and Access Services Number of events: 56				
Number of events: 56				
Level	Date and Time	Source	Event ID	Task Category
Information	8/08/2012 11:50:45 PM	Microsoft Windows secur...	6278	Network Policy Server
Information	8/08/2012 11:50:45 PM	Microsoft Windows secur...	6272	Network Policy Server
Information	8/08/2012 11:50:19 PM	Microsoft Windows secur...	6278	Network Policy Server
Information	8/08/2012 11:50:19 PM	Microsoft Windows secur...	6272	Network Policy Server
Information	8/08/2012 11:50:19 PM	NPS	4400	None

Event Properties - Event 6272, Microsoft Windows security auditing.

General | Details

Network Policy Server granted access to a user.

User:

- Security ID: HPN\user1
- Account Name: user1
- Account Domain: HPN
- Fully Qualified Account Name: HPN\user1

Client Machine:

- Security ID: NULL SID
- Account Name: -
- Fully Qualified Account Name: -
- OS-Version: -
- Called Station Identifier: 3C-D9-2B-7D-2F-70
- Calling Station Identifier: 10-0B-A9-D2-FB-90

NAS:

- NAS IPv4 Address: 192.168.1.5
- NAS IPv6 Address: -
- NAS Identifier: K062-00194
- NAS Port-Type: Wireless - IEEE 802.11
- NAS Port: 4

RADIUS Client:

- Client Friendly Name: MSM710 Wireless Controller
- Client IP Address: 192.0.2.101

Authentication Details:

- Connection Request Policy Name: Secure Wireless Connections (from wizard)
- Network Policy Name: Secure Wireless Connections (from wizard)
- Authentication Provider: Windows
- Authentication Server: LABserver.hpn.demo
- Authentication Type: PEAP
- EAP Type: Microsoft: Secured password (EAP-MSCHAP v2)
- Account Session Identifier: 3338316433332312D3030303030303033
- Logging Results: Accounting information was written to the local log file.

Quarantine Information:

- Result: Full Access
- Session Identifier: -

Log Name: Security

Source: Microsoft Windows security Logged: 8/08/2012 11:50:45 PM

Event ID: 6272 Task Category: Network Policy Server

Level: Information Keywords: Audit Success

User: N/A Computer: LABserver.hpn.demo

OpCode: Info

More Information: [Event Log Online Help](#)



RWL Tech Note Wireless 802.1x Authentication with Windows NPS

Event Properties - Event 6278, Microsoft Windows security auditing.

General | Details

Network Policy Server granted full access to a user because the host met the defined health policy.

User:
Security ID: HPN\user1
Account Name: user1
Account Domain: HPN
Fully Qualified Account Name: HPN\user1

Client Machine:
Security ID: NULL SID
Account Name: -
Fully Qualified Account Name: -
OS-Version: -
Called Station Identifier: 3C-D9-2B-7D-2F-70
Calling Station Identifier: 10-0B-A9-D2-FB-90

NAS:
NAS IPv4 Address: 192.168.1.5
NAS IPv6 Address: -
NAS Identifier: K062-00194
NAS Port-Type: Wireless - IEEE 802.11
NAS Port: 4

RADIUS Client:
Client Friendly Name: MSM710 Wireless Controller
Client IP Address: 192.0.2.101

Authentication Details:
Connection Request Policy Name: Secure Wireless Connections (from wizard)
Network Policy Name: Secure Wireless Connections (from wizard)
Authentication Provider: Windows
Authentication Server: LABserver.hpn.demo
Authentication Type: PEAP
EAP Type: Microsoft: Secured password (EAP-MSCHAP v2)
Account Session Identifier: 3338316433332312D3030303030303033

Quarantine Information:
Result: Full Access
Extended-Result: -
Session Identifier: -
Help URL: -
System Health Validator Result(s): -

Log Name: Security
Source: Microsoft Windows security
Event ID: 6278
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 8/08/2012 11:50:45 PM
Task Category: Network Policy Server
Keywords: Audit Success
Computer: LABserver.hpn.demo



4.2.2. Accounting

Accounting data was also captured. (Refer to Section 5.2).

```
<Event><Timestamp data_type="4">08/08/2012 23:50:45.003</Timestamp><Computer-Name
data_type="1">LABSERVER</Computer-Name><Event-Source data_type="1">IAS</Event-
Source><Class data_type="1">311 1 192.0.2.100 08/06/2012 08:56:03 88</Class><Acct-
Session-Id data_type="1">381d3321-00000003</Acct-Session-Id><Session-Timeout
data_type="0">30</Session-Timeout><Quarantine-Update-Non-Compliant
data_type="0">1</Quarantine-Update-Non-Compliant><Client-IP-Address
data_type="3">192.0.2.101</Client-IP-Address><Client-Vendor data_type="0">0</Client-
Vendor><Client-Friendly-Name data_type="1">MSM710 Wireless Controller</Client-Friendly-
Name><NP-Policy-Name data_type="1">Secure Wireless Connections (from wizard)</NP-
Policy-Name><Proxy-Policy-Name data_type="1">Secure Wireless Connections (from
wizard)</Proxy-Policy-Name><Provider-Type data_type="0">1</Provider-Type><SAM-Account-
Name data_type="1">HPN\user1</SAM-Account-Name><Fully-Qualified-User-Name
data_type="1">HPN\user1</Fully-Qualified-User-Name><Authentication-Type
data_type="0">5</Authentication-Type><Packet-Type data_type="0">11</Packet-
Type><Reason-Code data_type="0">0</Reason-Code></Event>
<Event><Timestamp data_type="4">08/08/2012 23:50:45.018</Timestamp><Computer-Name
data_type="1">LABSERVER</Computer-Name><Event-Source data_type="1">IAS</Event-
Source><Acct-Multi-Session-Id data_type="1">3C-D9-2B-7D-2F-70-10-0B-A9-D2-FB-90-50-22-
6E-8F-00-0D-16-F4</Acct-Multi-Session-Id><Acct-Session-Id data_type="1">381d3321-
00000003</Acct-Session-Id><NAS-Port data_type="0">4</NAS-Port><NAS-Port-Type
data_type="0">19</NAS-Port-Type><NAS-Identifier data_type="1">K062-00194</NAS-
Identifier><NAS-IP-Address data_type="3">192.168.1.5</NAS-IP-Address><Framed-MTU
data_type="0">1496</Framed-MTU><Calling-Station-Id data_type="1">10-0B-A9-D2-FB-
90</Calling-Station-Id><Called-Station-Id data_type="1">3C-D9-2B-7D-2F-70</Called-
Station-Id><Service-Type data_type="0">2</Service-Type><Vendor-Specific
data_type="2">00002228000F737369643D4C616254657374580016696E636F6D696E672D766C616E2D696
43D313030000B67726F75703D4C616200117673632D756E697175652D69643D320017706879747970653D49
4545383032646F74313120</Vendor-Specific><Vendor-Specific
data_type="2">00002228FA0600000001</Vendor-Specific><Vendor-Specific
data_type="2">00002228F906C0000264</Vendor-Specific><Client-IP-Address
data_type="3">192.0.2.101</Client-IP-Address><Client-Vendor data_type="0">0</Client-
Vendor><Client-Friendly-Name data_type="1">MSM710 Wireless Controller</Client-Friendly-
Name><User-Name data_type="1">user1</User-Name><Proxy-Policy-Name data_type="1">Secure
Wireless Connections (from wizard)</Proxy-Policy-Name><Provider-Type
data_type="0">1</Provider-Type><SAM-Account-Name data_type="1">HPN\user1</SAM-Account-
Name><Fully-Qualified-User-Name data_type="1">HPN\user1</Fully-Qualified-User-Name><NP-
Policy-Name data_type="1">Secure Wireless Connections (from wizard)</NP-Policy-
Name><Class data_type="1">311 1 192.0.2.100 08/06/2012 08:56:03 89</Class><Quarantine-
Update-Non-Compliant data_type="0">1</Quarantine-Update-Non-Compliant><MS-Extended-
Quarantine-State data_type="0">0</MS-Extended-Quarantine-State><MS-Quarantine-State
data_type="0">0</MS-Quarantine-State><Authentication-Type
data_type="0">11</Authentication-Type><Packet-Type data_type="0">1</Packet-
Type><Reason-Code data_type="0">0</Reason-Code></Event>
```



5. Troubleshooting

This section has some information about RADIUS troubleshooting and diagnostic tools.

5.1. Microsoft Event Viewer

5.1.1. Microsoft Event Viewer Configuration

Sometimes you can get useful data from here, but it often isn't very helpful with default configuration options. The settings below should enable successful event logging.

Additional material about logging events in NPS:

<http://social.technet.microsoft.com/Forums/en-US/winserverNAP/thread/107ef2be-33cf-4eba-a4c7-c07eff8096eb?prof=required>

Disable and re-enable logging (from an Admin-level command line).

```
auditpol /set /subcategory:"Network Policy Server" /success:disable /failure:disable  
auditpol /set /subcategory:"Network Policy Server" /success:enable /failure:enable
```

Restarting the NPS service is also recommended.

The locale should also be United States.

1. Start->Control Panel->Regional and Language Options
2. Click "Administrative" Tab, check the current applied System Locale, if it is different from "English (United States)", then click "Change system locale..." button.
3. Select "English (United States)", click OK and reboot the computer.

This finally showed some useful data! (Look for event ID 6273 – failed authentication.)

5.1.2. Microsoft Event Viewer Examples

Level	Date and Time	Source	Event ID	Task Category
Information	7/02/2012 10:28:36 PM	NPS	4400	None
Information	5/02/2012 12:54:38 AM	Microsoft Wi...	6278	Network Polic...
Information	5/02/2012 12:54:38 AM	Microsoft Wi...	6272	Network Polic...
Information	5/02/2012 12:54:30 AM	Microsoft Wi...	6278	Network Polic...
Information	5/02/2012 12:54:30 AM	Microsoft Wi...	6272	Network Polic...
Information	5/02/2012 12:46:08 AM	Microsoft Wi...	6278	Network Polic...
Information	5/02/2012 12:46:08 AM	Microsoft Wi...	6272	Network Polic...
Information	5/02/2012 12:30:03 AM	Microsoft Wi...	6278	Network Polic...
Information	5/02/2012 12:30:03 AM	Microsoft Wi...	6272	Network Polic...
Information	5/02/2012 12:29:50 AM	Microsoft Wi...	6278	Network Polic...
Information	5/02/2012 12:29:50 AM	Microsoft Wi...	6272	Network Polic...

Event 4400, NPS

General | Details

A LDAP connection with domain controller rr12.bv.litchwan.net for domain LITCHWAN is established.



RWL Tech Note Wireless 802.1x Authentication with Windows NPS

Event viewer entry showing a successful connection (viewed in the "Network Policy and Access" filter).

Level	Date and Time	Source	Event ID	Task
Information	7/02/2012 10:35:24 PM	Microsoft Wi...	6278	Netv
Information	7/02/2012 10:35:24 PM	Microsoft Wi...	6272	Netv
Information	7/02/2012 10:34:18 PM	Microsoft Wi...	6278	Netv
Information	7/02/2012 10:34:18 PM	Microsoft Wi...	6272	Netv
Information	7/02/2012 10:28:36 PM	NPS	4400	Non
Information	5/02/2012 12:54:38 AM	Microsoft Wi...	6278	Netv
Information	5/02/2012 12:54:38 AM	Microsoft Wi...	6272	Netv
Information	5/02/2012 12:54:30 AM	Microsoft Wi...	6278	Netv
Information	5/02/2012 12:54:30 AM	Microsoft Wi...	6272	Netv
Information	5/02/2012 12:46:08 AM	Microsoft Wi...	6278	Netv
Information	5/02/2012 12:46:08 AM	Microsoft Wi...	6272	Netv
Information	5/02/2012 12:38:08 AM	Microsoft Wi...	6278	Netv

Event 6272, Microsoft Windows security auditing.

General | Details

Network Policy Server granted access to a user.

User:

Security ID: LITCHWAN\rwl
Account Name: rwl
Account Domain: LITCHWAN
Fully Qualified Account Name: LITCHWAN\rwl

Client Machine:

Security ID: NULL SID
Account Name: -
Fully Qualified Account Name: -
OS-Version: -
Called Station Identifier: -
Calling Station Identifier: 172.20.100.111

NAS:

NAS IPv4 Address: 172.20.100.1
NAS IPv6 Address: -
NAS Identifier: bvcore01
NAS Port-Type: -
NAS Port: -

RADIUS Client:

Client Friendly Name: Switch-bvcore01
Client IP Address: 172.20.100.1

Authentication Details:

Proxy Policy Name: Use Windows authentication for all users
Network Policy Name: ProCurve switch logins
Authentication Provider: -
Authentication Server: rr12.bv.litchwan.net
Authentication Type: PAP
EAP Type: -
Account Session Identifier: -



RWL Tech Note Wireless 802.1x Authentication with Windows NPS

Event ID 6273 – failed authentication.

Level	Date and Time	Source	Event ID	Task Category
Information	26/07/2012 12:14:00 AM	Microsoft Windows sec...	6273	Network Policy Server
Information	26/07/2012 12:13:57 AM	Microsoft Windows sec...	6273	Network Policy Server
Information	26/07/2012 12:13:54 AM	Microsoft Windows sec...	6273	Network Policy Server

Event 6273, Microsoft Windows security auditing.

General Details

Network Policy Server denied access to a user.

Contact the Network Policy Server administrator for more information.

User:

Security ID: LITCHWAN\rwl
Account Name: rwl
Account Domain: LITCHWAN
Fully Qualified Account Name: LITCHWAN\rwl

RADIUS Client:

Client Friendly Name: RWLPC
Client IP Address: 172.20.100.111

Authentication Details:

Proxy Policy Name: Use Windows authentication for all users
Network Policy Name: ProCurve switch logins
Authentication Provider: Windows
Authentication Server: rr12.bv.litchwan.net
Authentication Type: PAP
EAP Type: -
Account Session Identifier: -
Reason Code: 70
Reason: The user attempted to connect using a dial-in medium that did not

match the restricted dial-in media. Check the dial-in constraints for the matching network policy.

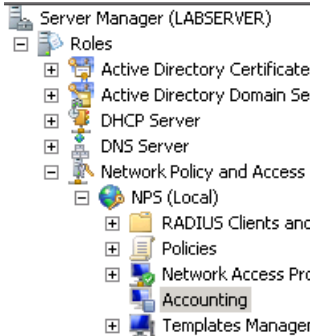


5.2. RADIUS Accounting

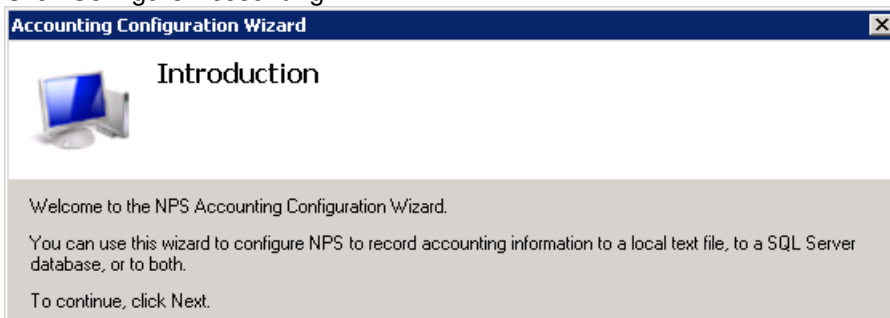
Accounting can be configured in Windows 2008 to log all relevant traffic. It can log far more data than the NPS events seen in MS Event Viewer.

5.2.1. Setup

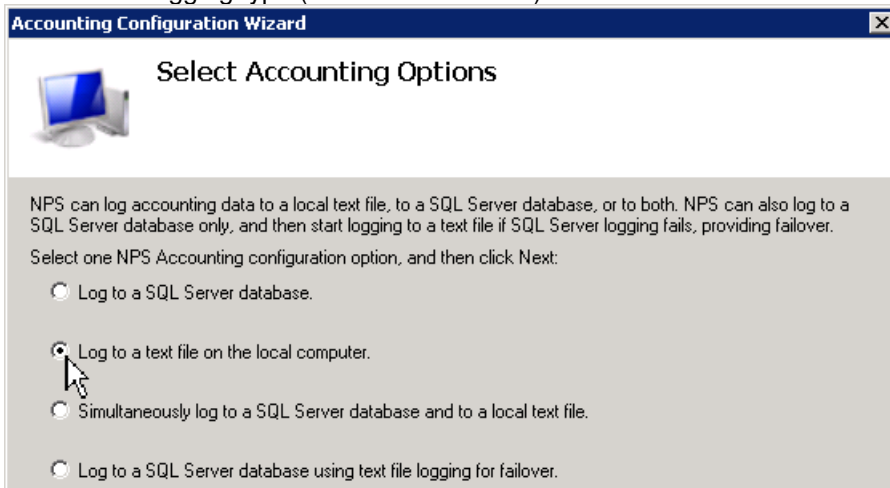
- The NPS console is available from the Server Manager; select Accounting.



- Click Configure Accounting

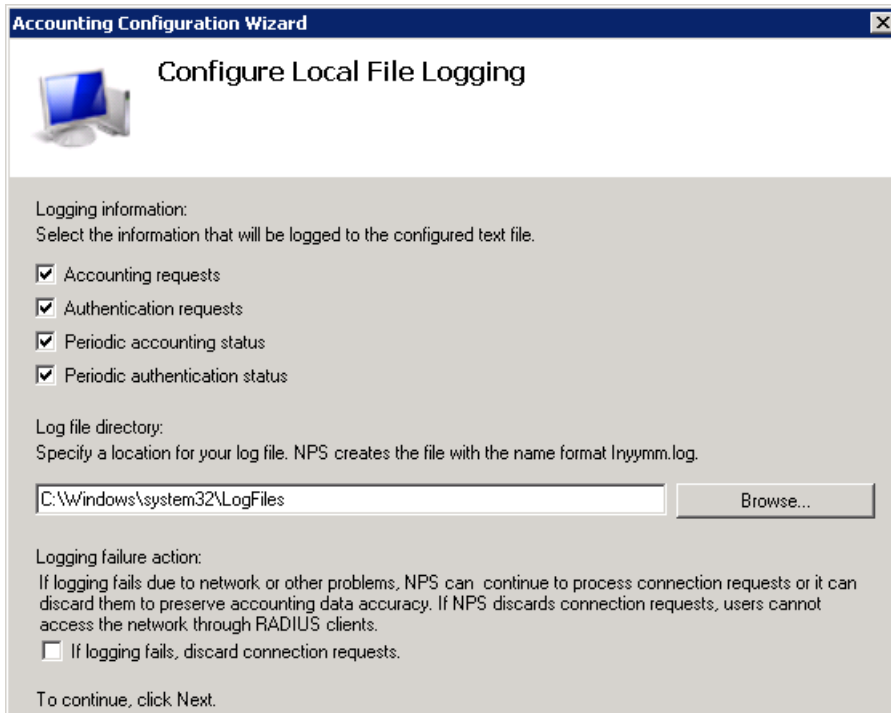


- Choose the logging type (text file in this case)

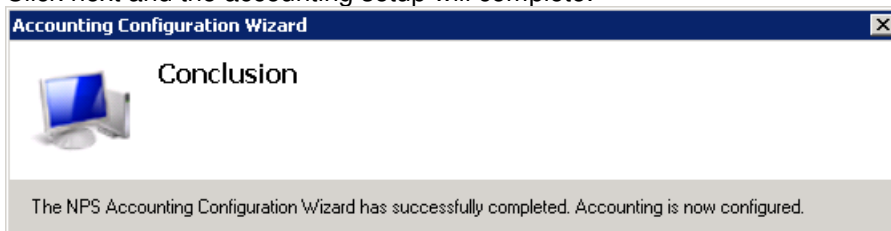




- Choose the items to log, logfile location, and whether you want logging failure to cause authentication failure.

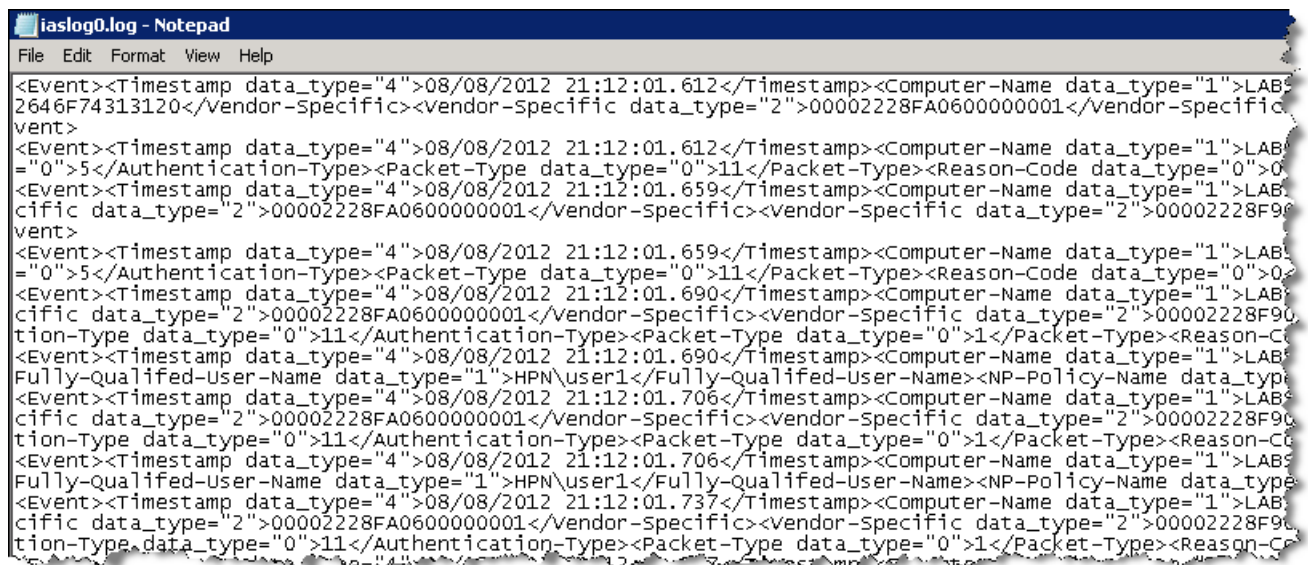


- Click next and the accounting setup will complete.



5.2.2. Sample Account Output

An example of the text-based log output.



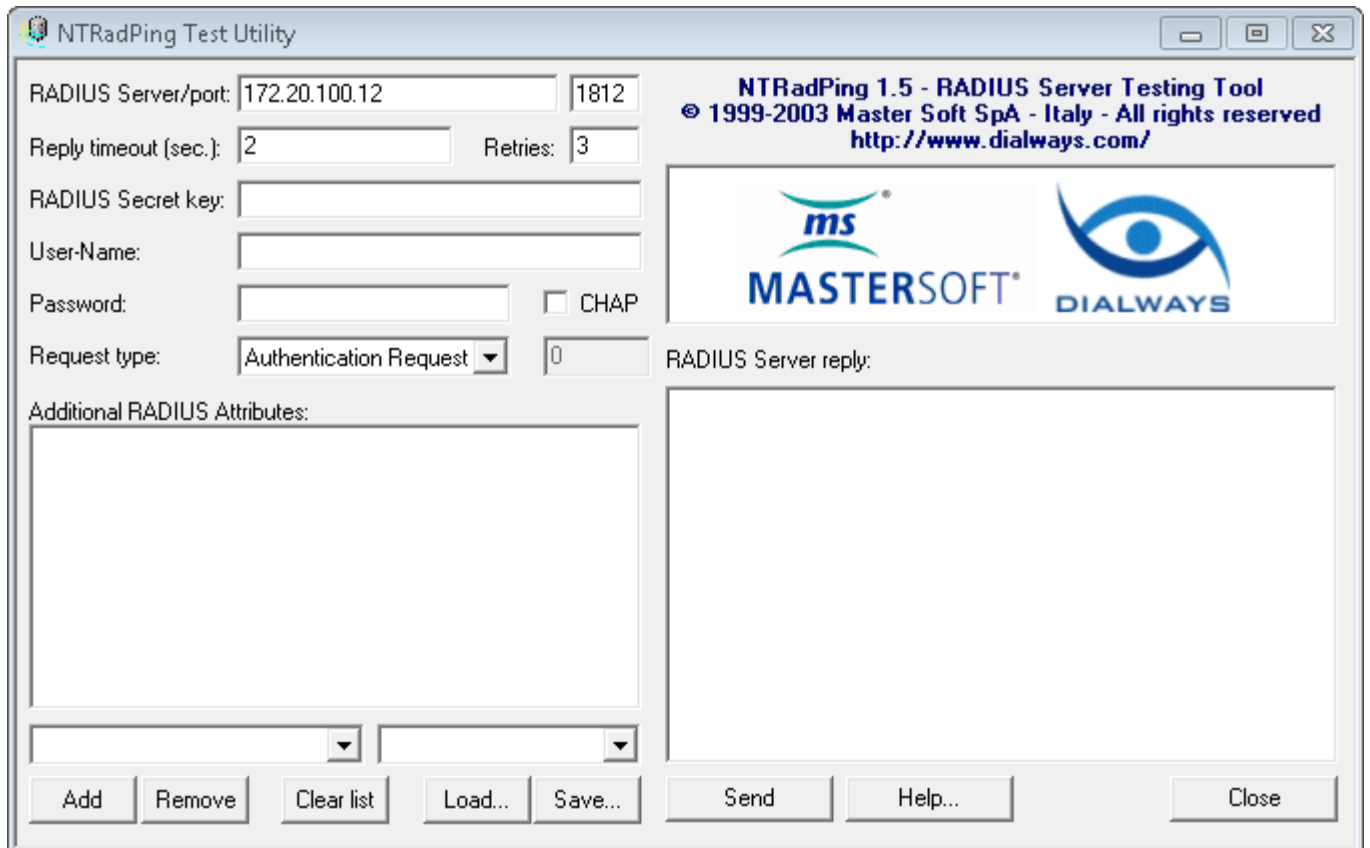


5.3. Other Available Diagnostic Tools

<http://www.serverwatch.com/sreviews/article.php/3935211/5-Free-RADIUS-Testing-and-Monitoring-Tools.htm>
The URL above has links to several tools to assist with RADIUS management.

5.4. NTRadPing

Your mileage may vary, but the most useful one appeared to be NTRadPing.





6. Appendix A: Example Errors

Several common misconfiguration have been tested, with the resulting errors and symptoms described in this Section.

6.1. Client Side Errors

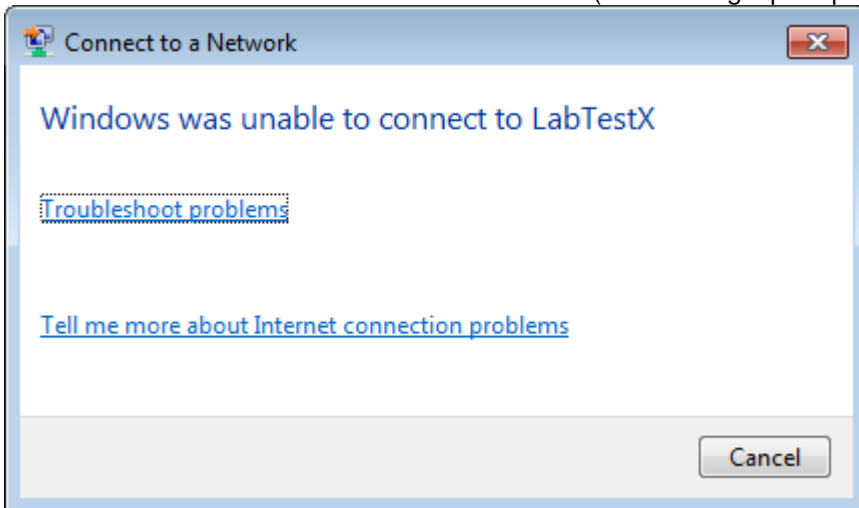
6.1.1. Incorrect Username

6.1.1.1. Scenario

The user logs in from the client with the incorrect username.

6.1.1.2. Symptoms

The user will see this window on the client device (after the login prompt appears several times):



The Windows Event Log shows Event ID 6273, with Reason Code 8: The specified user account does not exist.

Authentication Details:	
Connection Request Policy Name:	Secure Wireless Connections (from wizard)
Network Policy Name:	-
Authentication Provider:	Windows
Authentication Server:	LABserver.hpn.demo
Authentication Type:	EAP
EAP Type:	-
Account Session Identifier:	34363531316464362D3030303030303037
Logging Results:	Accounting information was written to the local log file.
Reason Code:	8
Reason:	The specified user account does not exist.



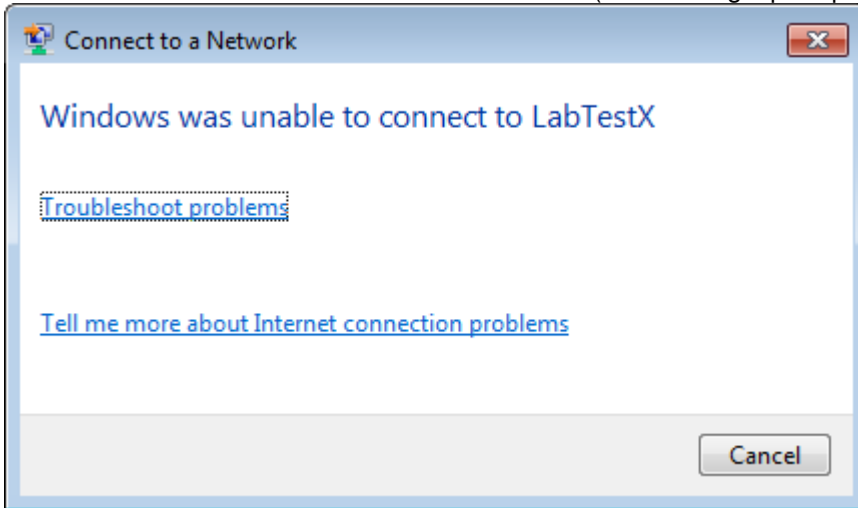
6.1.2. Incorrect Windows Domain

6.1.2.1. Scenario

The user logs in from the client with the incorrect domain name specified as part of the username. This may also occur if the authentication mode has not been set to user.

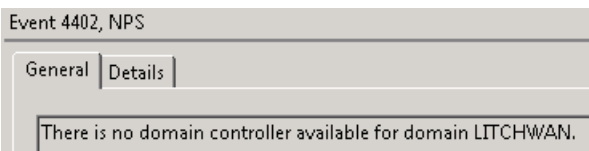
6.1.2.2. Symptoms

The user will see this window on the client device (after the login prompt appears several times):



The Windows Event Log shows Event ID 4402, with Reason Code 7: The specified domain does not exist.

Level	Date and Time	Source	Event ID	Category
Information	9/08/2012 12:05:01 AM	Microsoft Windows secur...	6273	Network Policy Server
Error	9/08/2012 12:05:01 AM	NPS	4402	None



Authentication Details:

Connection Request Policy Name:	Secure Wireless Connections (from wizard)
Network Policy Name:	-
Authentication Provider:	Windows
Authentication Server:	LABserver.hpn.demo
Authentication Type:	EAP
EAP Type:	-
Account Session Identifier:	34363531316464362D3030303030303038
Logging Results:	Accounting information was written to the local log file.
Reason Code:	7
Reason:	The specified domain does not exist.



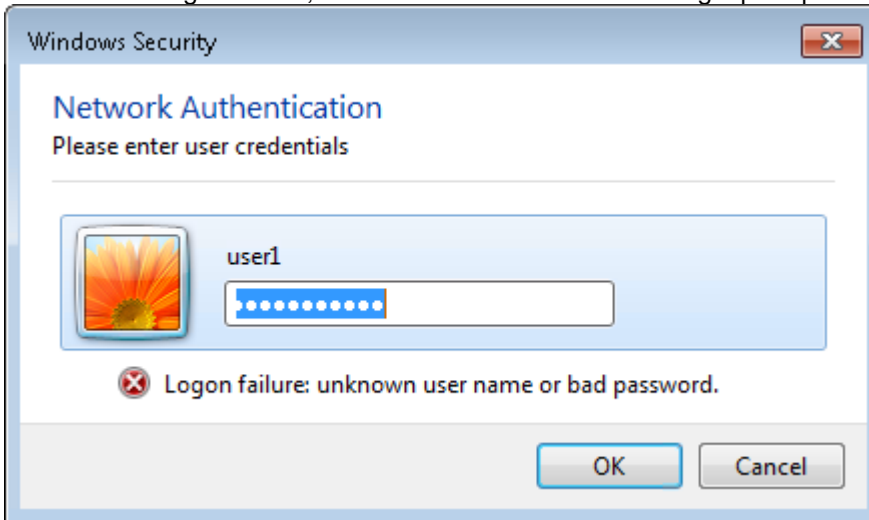
6.1.3. Incorrect Password

6.1.3.1. Scenario

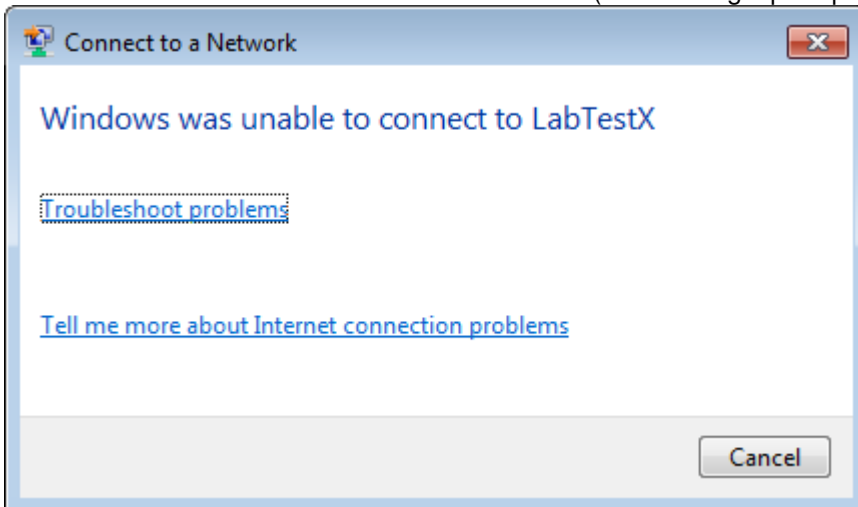
The user logs in from the client with the correct username but incorrect password.

6.1.3.2. Symptoms

After the first login screen, the user will see this modified login prompt:



The user will see this window on the client device (after the login prompt appears several times):



The Windows Event Log shows Event ID 6273, with Reason Code 16: Authentication failed due to a user credentials mismatch.

Authentication Details:

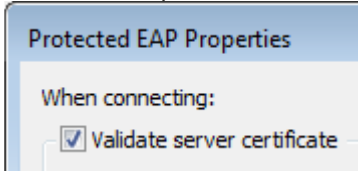
Connection Request Policy Name:	Secure Wireless Connections (from wizard)
Network Policy Name:	Secure Wireless Connections (from wizard)
Authentication Provider:	Windows
Authentication Server:	LABserver.hpn.demo
Authentication Type:	PEAP
EAP Type:	Microsoft: Secured password (EAP-MSCHAP v2)
Account Session Identifier:	30333637383034352D3030303030303035
Logging Results:	Accounting information was written to the local log file.
Reason Code:	16
Reason:	Authentication failed due to a user credentials mismatch. Either the user name provided does not map to an existing user account or the password was incorrect.



6.1.4. Server Certificate Required

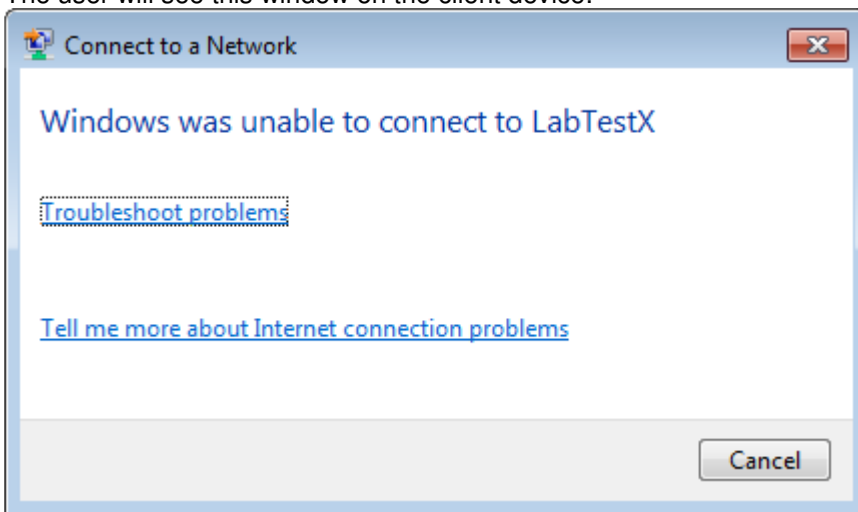
6.1.4.1. Scenario

The wireless profile on the Windows client is misconfigured with the “Validate server certificate” option enabled.

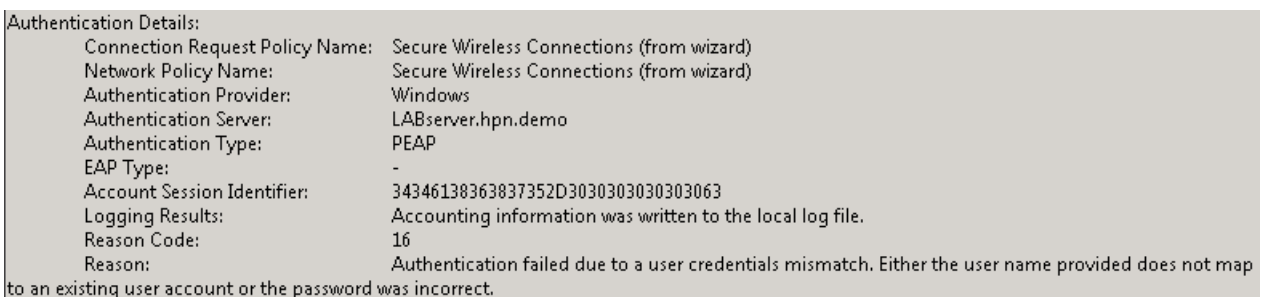


6.1.4.2. Symptoms

The user will see this window on the client device:



The Windows Event Log shows Event ID 6273, with Reason Code 16: Authentication failed due to a user credentials mismatch.

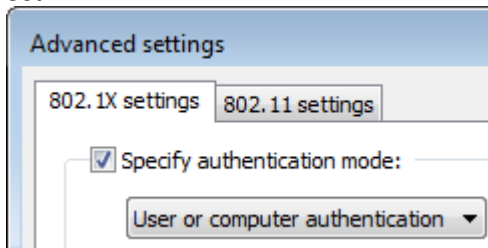




6.1.5. Username Setting not Specified

6.1.5.1. Scenario

The wireless profile on the Windows client is misconfigured with the “Specify Authentication Mode” option not set.



6.1.5.2. Symptoms

Initially fails with the Windows Event Log showing 2 x Event ID 6273 errors (trying local machine name), but then prompts for username and works OK.

6.1.6. Server Certificate Required and Username Setting

6.1.6.1. Scenario

The wireless profile on the Windows client is misconfigured with the “Validate server certificate” option enabled (Section 6.1.4), and the username setting is missing (Section **Error! Reference source not found.**).

6.1.6.2. Symptoms

The Windows Event Log shows 2 x Event ID 6273 errors (trying local machine name), but even after the client prompts for the username/password, another Event ID 6273 is logged.



6.1.7. Wireless Profile with TKIP or WPA

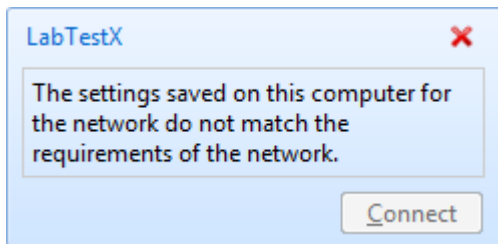
6.1.7.1. Scenario

The wireless profile on the Windows client is misconfigured with properties such as TKIP or WPA-Enterprise (AES).

6.1.7.2. Symptoms

On the client you will see errors similar to these when viewing the available wireless connections list:

LabTestX



Note that WPA-Enterprise didn't work even with "WPA or WPA2" specified in the VSC. Even when the VSC was set to just WPA, the client still shows the red X. However, when the VSC was set to "WPA (TKIP)", and the client's wireless profile set to WPA/TKIP, it works OK.



6.2. Server Side Errors

6.2.1. Invalid NAS Port Type

6.2.1.1. Scenario

The NPS Network policy has an incorrect NAS Port Type specified. In this example it is set to Ethernet only.

Condition	Value
NAS Port Type	Ethernet

6.2.1.2. Symptoms

The client fails to connect.

The Windows Event Log shows Event ID 6273, with Reason Code 65.

Information 9/08/2012 12:34:29 AM Microsoft Windows secur... 6273 Network Policy Server

Authentication Details:

Connection Request Policy Name: Secure Wireless Connections (from wizard)
Network Policy Name: Connections to other access servers
Authentication Provider: Windows
Authentication Server: LABserver.hpn.demo
Authentication Type: EAP
EAP Type: -
Account Session Identifier: 34346138363837352D3030303030303131
Logging Results: Accounting information was written to the local log file.
Reason Code: 65
Reason: The Network Access Permission setting in the dial-in properties of the user account in Active Directory

is set to Deny access to the user. To change the Network Access Permission setting to either Allow access or Control access through NPS Network Policy, obtain the properties of the user account in Active Directory Users and Computers, click the Dial-in tab, and change Network Access Permission.



6.2.2. Incorrect EAP

6.2.2.1. Scenario

The EAP type is removed from the NPS Network Policy Constraints.

6.2.2.2. Symptoms

The client fails to connect.

The Windows Event Log shows Event ID 6273, with Reason Code 66: ... authentication method that is not enabled...