Hewlett-Packard
MSM Example Configurations

Contributors:

Graham Brown,

Fotios Kotsiopoulos,

Richard Litchfield,

Elissa McCormick,

HP Networking Solution Architects

Hewlett-Packard Australia Limited

Document Date: 27-May-11

Document Version: 2.40b

Distribution List

From	Date	Phone/Fax/Email
Elissa McCormick		
Graham Brown		
Richard Litchfield		
Fotios Kotsiopoulos		

Version History

Ver. No.	Ver. Date	Revised By	Description	Filename
0.92	15-12-09	Elissa McCormick	Initial draft	MSM Example Configurations
0.93	12-01-10	Graham Brown	Updates to initial draft	
0.94	20-01-10	Fotios Kotsiopoulos	Appendix A	
0 95	28-01-10	Graham Brown	Updates	
1.00	28-01-10	Elissa McCormick	Final Edit	
2.00	16-02-2011	Elissa McCormick	Updates on version1.0	
2.25	7-03-2011	Richard Litchfield	Screenshots	
2.40	28-04-2011	Elissa McCormick	Final Edits	

Proprietary Notice

Table of Contents

1 Introduction

1.1 Purpose

This document has been reviewed to incorporate additional functionality associated with the release of 5.x firmware. This functionality includes Teaming, Network profiles.

The purpose of this document is to provide HPN resellers and customers with some verified deployment examples to assist with the initial design, configuration and integration of their HP MSM wireless networks into their existing routed switch networks. There are many ways to deploy a HP wireless network. This document covers some of the more common deployment scenarios, being trusted employees/students/teachers; guests and contractors along with devices such as WiFi capable phones and i-devices.

This document assumes there are existing VLANs, security policies and IP addressing schemas in place for existing wired clients. When adding wireless capabilities to the network it is recommended that additional VLANs, IP addressing and security policies also be applied. As this document is provided as a guide only, it is not possible to take into account installation specific security policies or requirements. It is the responsibility of the user of this document to modify the configuration examples to suit the site specific security requirements. It is also the responsibility of the user to thoroughly test the conformance of the configuration to those security policies. Hewlett-Packard shall not be held liable for security breaches through the use of this material.

This document is not designed to replace the official Network training available from Hewlett Packard. For a full listing of all courses available and Professional Accreditations visit http://h17007.www1.hp.com/us/en/training/index.aspx.

In this document we create Wireless VLANs for Teachers, Students, Guests and contractors, additional DHCP scopes have been added for the various networks.

1.2 Related Documents

Date/Version	Author	Document
13/10/2009	HPN	Upstream Proxy Explained
7/10/2009	HPN	Upstream_proxy.cfg
April 2010	HPN	HPN MSM7xx Controllers Management and Configuration Guide version 5.4.0
April 2010	HPN	Installation and Getting Started Guide for the HP ProCurve MSM765 Controller version 5.4.0
Jan 2007	Colubris	Deploying Voice over WiFi

1.3 Equipment Details

Controller/AP	MAC Address/IP Address	Firmware Details
765zl Controller	Internet Port IP:192.168.1.20	5.5.0.0
765zl Controller	Internet Port IP:192.168.1.21	5.5.0.0
MSM422 Radio	Radio 1:00-03-52-b3-dd-70 Radio 2: 00-03-52-b3-dd-70 IP:10.20.30.105	As the APs were configured for controlled mode they received their firmware from the controller, hence the firmware revision was the same as the controller.
MSM410 Radio	IP: 10.20.30.101	As the APs were configured for controlled mode they received their firmware from the controller, hence the firmware revision was the same as the controller.

Infrastructure	IP Address	Firmware Details
2910al	192.168.1.3/24	K15.02
5406zl switch	192.168.1.2/24	K15.02
8606zl switch	192.168.1.1/24	K15.02
DHCP/DNS/Active Directory/radius	192.168.1.10/24	Windows 2008SP2

1.4 Definitions and Abbreviations

HP	Hewlett Packard
AAA	Authentication Authorization and Accounting (RADIUS Server Functions)
AP	Access Point
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DR	Disaster Recovery
GMS	Guest Management Software (previously called the Visitor Management Tool or VMT)
HPGM	HP Global Method (Project Management)
LLDP	Link Layer Discovery Protocol-Media Endpoint Discovery
MSM	MultiService Mobility
NIC	Network Interface Card
OS	Operating System
PCM+	ProCurve Manager Plus
PoE	Power over Ethernet
QoS	Quality of Service
RFI	Request for Information
SOE	Standard Operating Environment
TLV	Type Length Variable
TNC	Trusted Network Computing
VLAN	Virtual Local Area Network
VSC	Virtual Service Community
WDS	Wireless Distribution System
WLAN	Wireless Local Area Network

When reading this document or other MSM related documents it is important to keep in mind the following definitions.

Trusted Network	With respect to MSM controllers the “Trusted” network is the “Internet” port.
Untrusted Network	With respect to MSM controllers the “Un-trusted” network is the “LAN” port.

2 Design

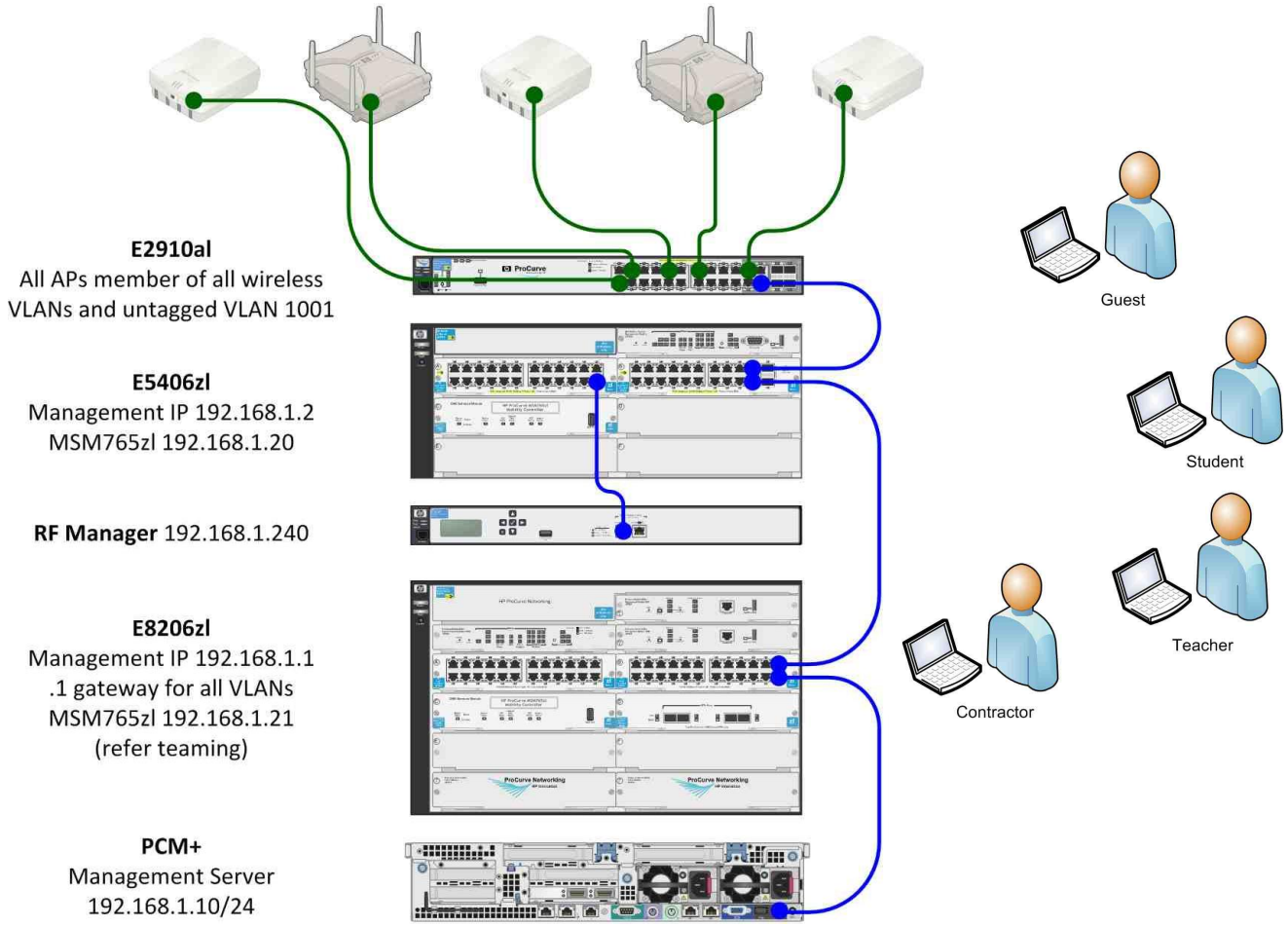
The following MSM deployment examples are based upon a school scenario; however this scenario can be easily replicated to suite corporate environments.

Tabled below are the various examples discussed within this document along with a network diagram and switch configuration

User Group Name	VLAN	Subnet	Security	Authentication
Infrastructure	1001	192.168.1.x/24		
Wired Students	120	10.20.120.x/24		
Wireless Students	121	10.20.121.x/24	Dynamic WPA2	802.1x
Wired Teachers	130	10.20.130.x/24		
Wireless Teachers	131	10.20.131.x/24	Dynamic WPA2	Active Directory
Wired Guest	110	10.20.110.x/24		
Wireless Guest	111	10.20.111.x/24	No security	HTML/Radius
Contractor	50	10.20.50.x/24	WPA Pre-shared Key	HTML/Active Directory

As standard practice the management VLAN should be secure

2.1 Network Diagram



VLANs:
50 Contractors – 10.20.50.x
110 wired Guest – 10.20.110.x
111 Wireless Guests – 10.20.111.x
120 Wired Students – 10.20.120.x
121 Wireless Students - 10.20.121.x
130 Wired Teachers – 10.20.130.x
131 Wireless Teachers 10.20.131.x
1001 Infrastructure/management 192.168.1.x

2.2 Switch Configurations

2.2.1 8206zl Switch Configuration

Below is the switch configuration file used for these wireless examples. Key points to note are in red text.

```
hostname "CORP_8206_1"
time timezone 600
time daylight-time-rule Southern-Hemisphere Time needs to be set as AD and controller must be synchronised
module 1 type J9308A
module 2 type J9309A
module 3 type J9154A
module 4 type J8707A
module 5 type J9154A
module 6 type J9308A
interface B1
   name "Connection to 5400zl"
exit
interface D4
   name "Connection to 8206zl"
exit
ip routing
vlan 1
   name "DEFAULT_VLAN"
   untagged A1-A24,B1-B3,C2,D1-D4,F1-F24
   no ip address
   tagged C1
   no untagged B4,E1-E2
   exit
vlan 1001
   name "infrastructure" VLAN contains DHCP/DNS server, MSM Controller Internet port and MSM APs
   untagged E1
   ip address 192.168.1.1 255.255.255.0
   tagged B1,D4,F20
   exit
vlan 110
   name "wired guest"
   ip address 10.20.110.2 255.255.255.0
   tagged B1,D4,F20
   exit
vlan 111
   name "wireless-guest" No Helper address required as controller providing IP addresses
    ip address 10.20.111.1 255.255.255.0
   tagged B1,D4,E1,F20
   exit
vlan 120
   name "wired student"
   ip address 10.20.120.2 255.255.255.0
   tagged B1,D4,F20
   exit
vlan 121
   name "wireless student"
   ip helper-address 192.168.1.10
   ip address 10.20.121.1 255.255.255.0
   tagged B1,D4,F20
   exit
vlan 130
```

```
  name "wired Teacher"
  ip address 10.20.130.2 255.255.255.0
  tagged B1,D4,F20
  exit
vlan 131
  name "wireless teacher"
  ip address 10.20.131.1 255.255.255.0
  tagged B1,D4,F20
  exit
vlan 50
  name "contractors"                    No Helper address required as controller providing IP addresses
  ip address 10.20.50.1 255.255.255.0
  tagged B1,D4,F20
  exit
vlan 200
  name "telephony"
  qos dscp 101110                       QoS required to support Voice traffic
  ip helper-address 192.168.1.10
  ip address 10.20.200.1 255.255.255.0
  tagged B1,D4,F20
  voice
  exit
vlan 2200
  name "MSM765LANPORT" Null VLAN for the LAN port required for teaming
  untagged C2
  no ip address
  exit

qos type-of-service diff-services
timesync sntp
sntp unicast
sntp server priority 1 192.168.1.10
snmp-server community "public" unrestricted
snmp-server host 192.168.1.10 community "public"
```

2.2.2 5406zl Switch Configuration

The MSM765zl Controller resides in slot C.

```
; J8697A Configuration Editor; Created on release #K.15.02.0005

hostname "CORP_5406"
time timezone 600
time daylight-time-rule Southern-Hemisphere
fastboot
ip access-list extended "100"            Access list to control access to switch Management Plane
 4 deny tcp 0.0.0.0 255.255.255.255 eq 23 10.20.30.252
 10 deny tcp 0.0.0.0 255.255.255.255 eq 80 10.20.30.252
 20 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
 exit
interface C1
   ip access-group "100" in
module 1 type J9307A
module 2 type J9308A
module 3 type J9154A
module 4 type J8702A
module 5 type J9309A
vlan 1
   name "DEFAULT_VLAN"
   untagged A1-A20,A22-A23,B2-B14,B16-B18,B21-B24,D1-D24,E1-E4,Trk1
   no ip address
   no untagged A21,B1,B15,B19,C2
vlan 2200
   name "MSM765LANPORT" Null VLAN for the LAN port
   untagged C2
   tagged D21
   no ip address
   exit
vlan 1001
   name "infrastructure"
   ip address 192.168.1.2/24
   untagged A21,B1,B15,B19,C1
   tagged A1,D21,D23
   no ip address
   exit
vlan 200
   name "voice"
   tagged D21,D23
   voice
   no ip address
   exit
vlan 120
   name "wired Student"
   tagged D21,D23
   no ip address
   exit
vlan 121
   name "wireless student"
   tagged D21,D23
   no ip address
   exit
vlan 130
   name "wired teacher"
```

```
   tagged D21,D23
   no ip address
   exit
vlan 131
   name "wireless teacher"
   tagged D21,D23
   no ip address
   exit
vlan 110
   name "wired guest"
   tagged D21,D23
   no ip address
   exit
vlan 50
   name "contractor"
   tagged C1,D21,D23
   no ip address
   exit
vlan 111
   name "wireless guest"
   tagged C1,D21,D23
   no ip address
   exit
qos type-of-service diff-services  switch will honour incoming diffServ values
timesync sntp
sntp unicast
sntp server priority 1 10.1.20.250
snmp-server community "public" unrestricted
snmp-server host 192.168.10 community "public"
```

2.2.3 2910al Switch Configuration

The access points reside on ports 21-23 and receive power from this switch.

```
; J9146A Configuration Editor; Created on release #W.14.38

hostname "Corp_2910al"
module 1 type J9146A
module 2 type J9008A
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-16,24-A2
   no ip address
   no untagged 17-23
   exit
vlan 1001
   name "infrastructure"
   ip address 192.168.1.4/24
   untagged 17-23
   tagged 24
   no ip address
   exit
vlan 111
   name "wireless guest"
   tagged 21-24
   no ip address
   exit
vlan 120
   name "wired student"
   tagged 24
   no ip address
   exit
vlan 121
   name "wireless student"     Access point tagged in this Vlan
   tagged 21-24
   no ip address
   exit
vlan 130
   name "wired teacher"
   tagged 24
   no ip address
   exit
vlan 50
   name "contractor"
   tagged 21-24            Access point tagged in these VLANs
   no ip address
   exit
vlan 200
   name "voice"
   tagged 21-24            Access point tagged in these VLANs
   qos dscp 46
   voice
   no ip address
   exit
snmp-server community "public" unrestricted
snmp-server host 192.168.1.10 "public"
spanning-tree
```

3 General Configuration

3.1 Start up

When using the appliance the LAN port is assigned an IP address 192.168.1.1. Thus access to the controllers web interface is available immediately. The MSM765zl module requires some additional configuration as an IP address needs to be configured on the LAN port (#2) or Internet Port(#1), this is done via the switch. For details on configuring IP addresses please refer to the “HP MSM765zl Mobility Controller Installation and Getting Started Guide” which can be downloaded from http://www.hp.com/rnd/support/manuals/mscseries.htm.

4 Controller MSM765zl

Refer to the “HP MSM765zl Mobility Controller Installation and Getting Started Guide” to configure the internal uplinks and assign default IP address 192.168.1.1/24 the LAN port. Once complete you will be able to access the controller via the web interface. As part of the initial setup you will be prompted to change the admin password and country code. The steps below discuss the other options to enable/configure on the Services Controller prior to configuring any VSCs

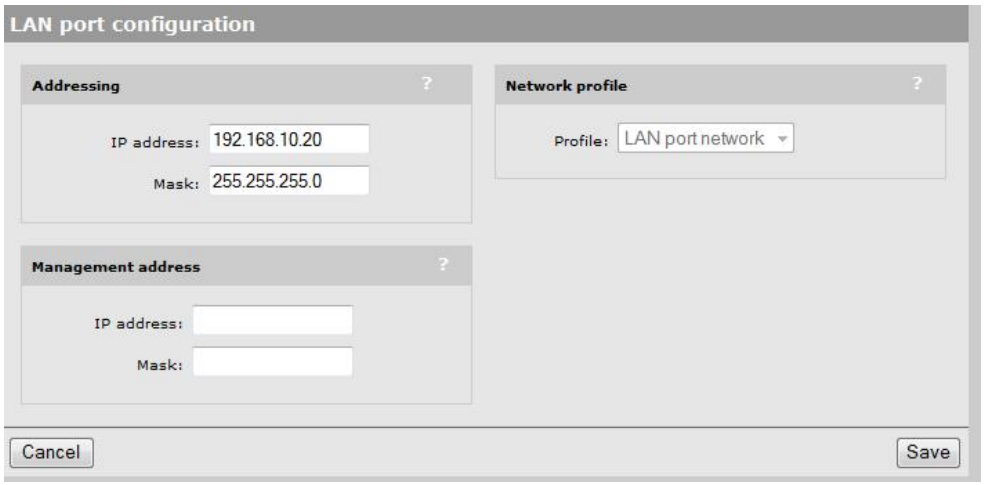
Note MSM Access Points also default to the 192.168.1.1 address if they cannot find a controller, or receive an IP address from the controller or another source. Therefore it is recommended at this early stage of configuration that any MSM APs are either powered down or not connected to the network.

4.1 Services Controller Configuration

In this configuration we are using 192.168.1.x for the Infrastructure Network, which is the “Trusted Network” hence we are required to change the LAN Port’s IP address to 192.168.10.20 (being a separate network)

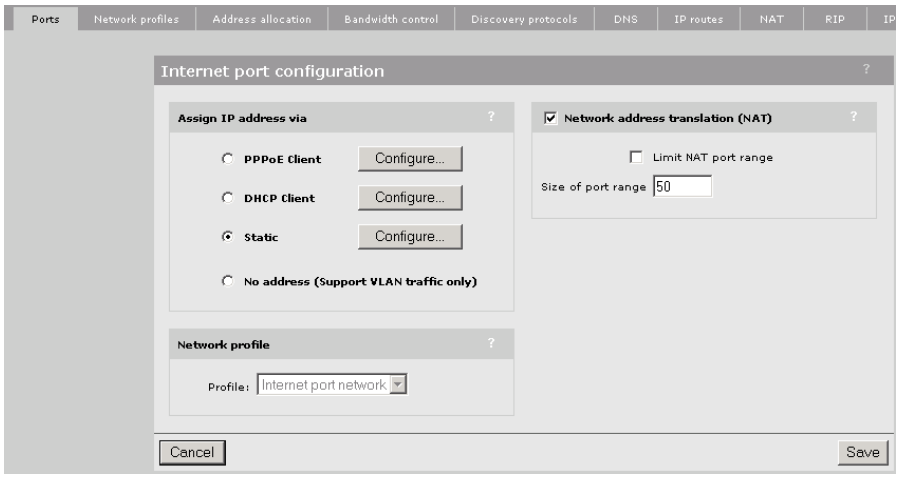
4.1.1 LAN Port Configuration

Network | Ports | LAN Port

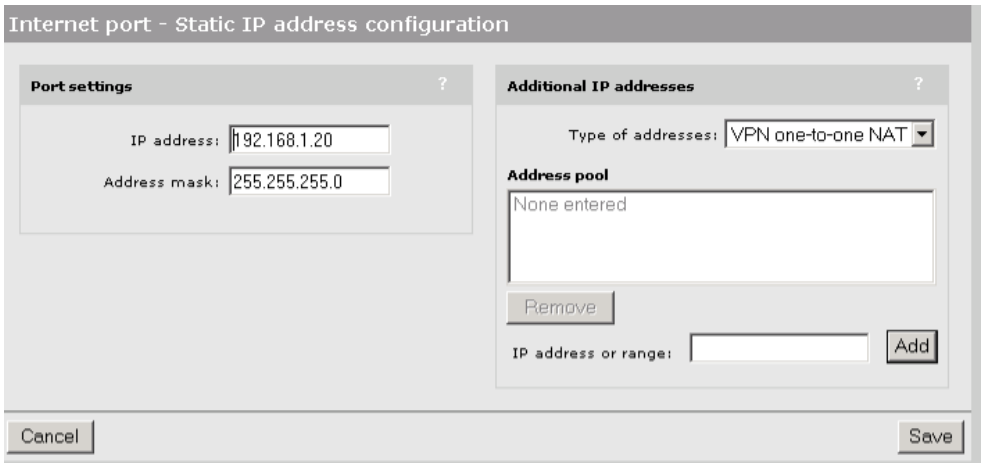


4.1.2 Internet Port Configuration

Network | Ports | Internet Port

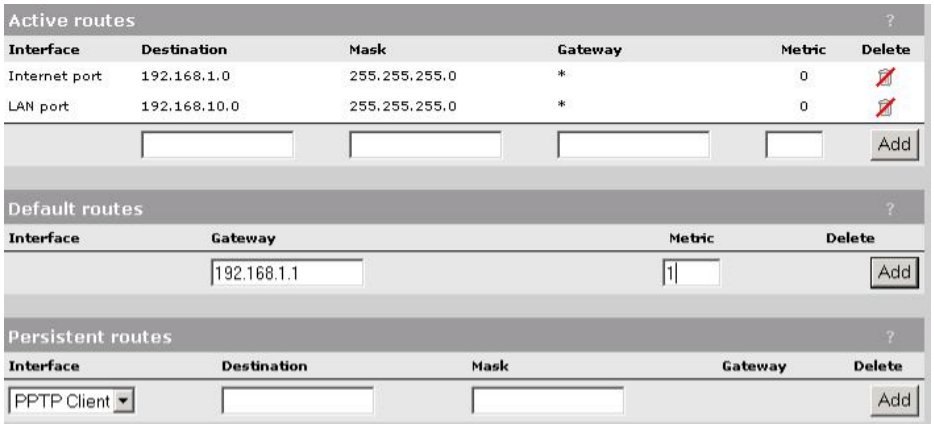


Assign a Static IP address to the Internet port and check NAT (we will be using NAT for Guest Access). In the screen shot below the Internet Port is assigned an IP address in the 192.168.1.x range. Once the Internet port has an IP address you can now manage the controller via this interface.



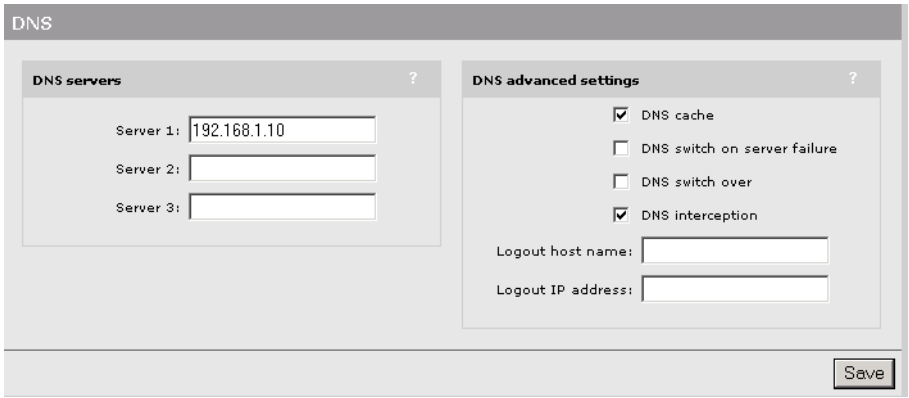
Network | IP Route

Assign a default gateway for the Internet port. Here the default gateway on the switch for VLAN 1001 is being used 192.168.1.1/24



Network | DNS

Add DNS Server



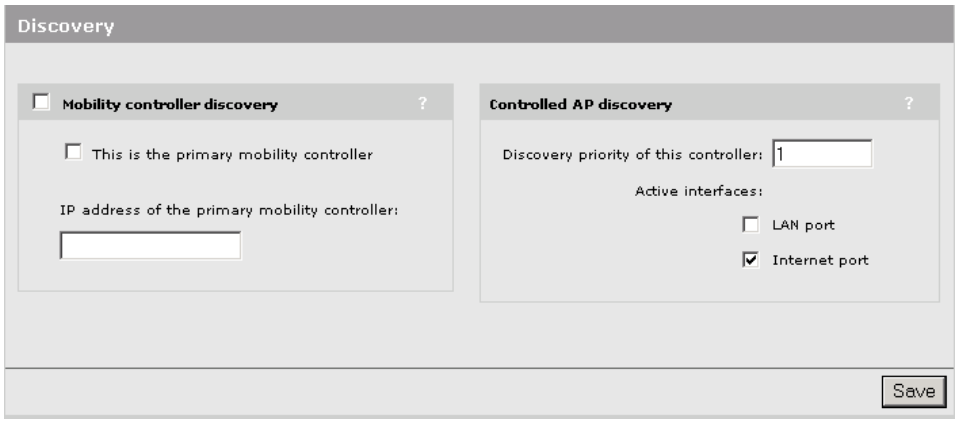
4.2 Management Configuration

4.2.1 Device Discovery

Service Controller | Management | Device Discovery

Because these examples are using the “trusted” (Internet) port ensure the Internet port is checked listening for join requests from APs on this port. Both ports are checked by default.

Uncheck LAN port. Leave all others as default

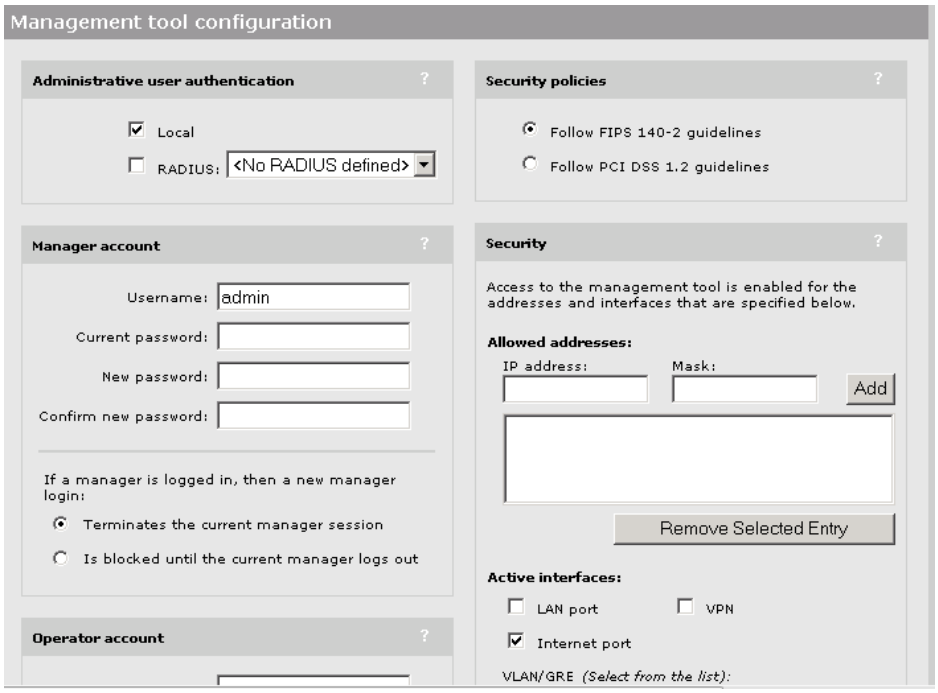


4.2.2 Service Controller | Management

The following screens covers off configuring the Controller to participate in your Network Management Domain. In the example provided we are using SNMP v2.

Service Controller | Management | Management Tool

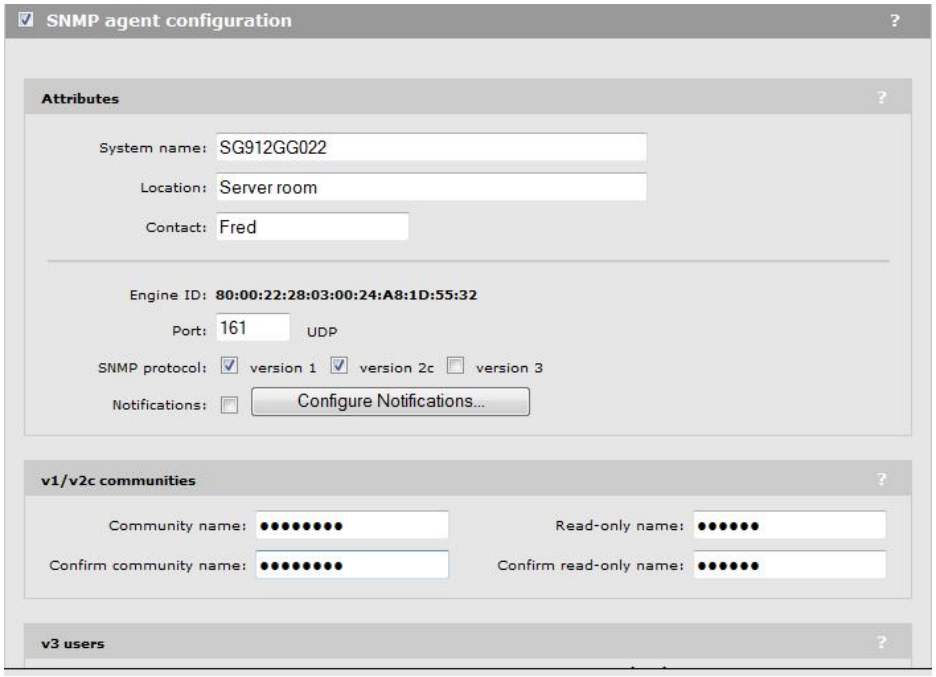
To assist in securing access to the management interface, the Internet port should be checked and LAN port unchecked.



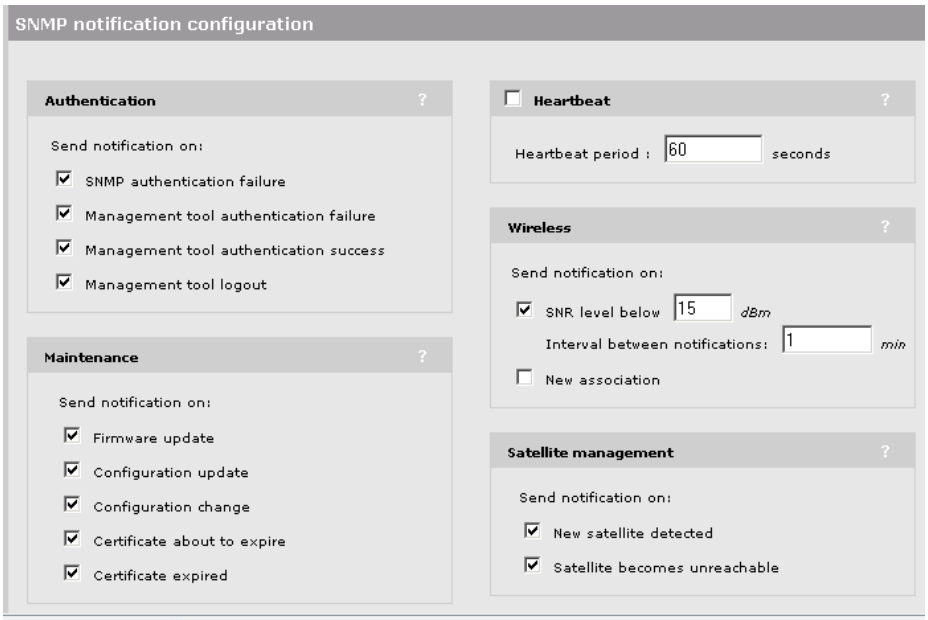
Service Controller | Management | SNMP

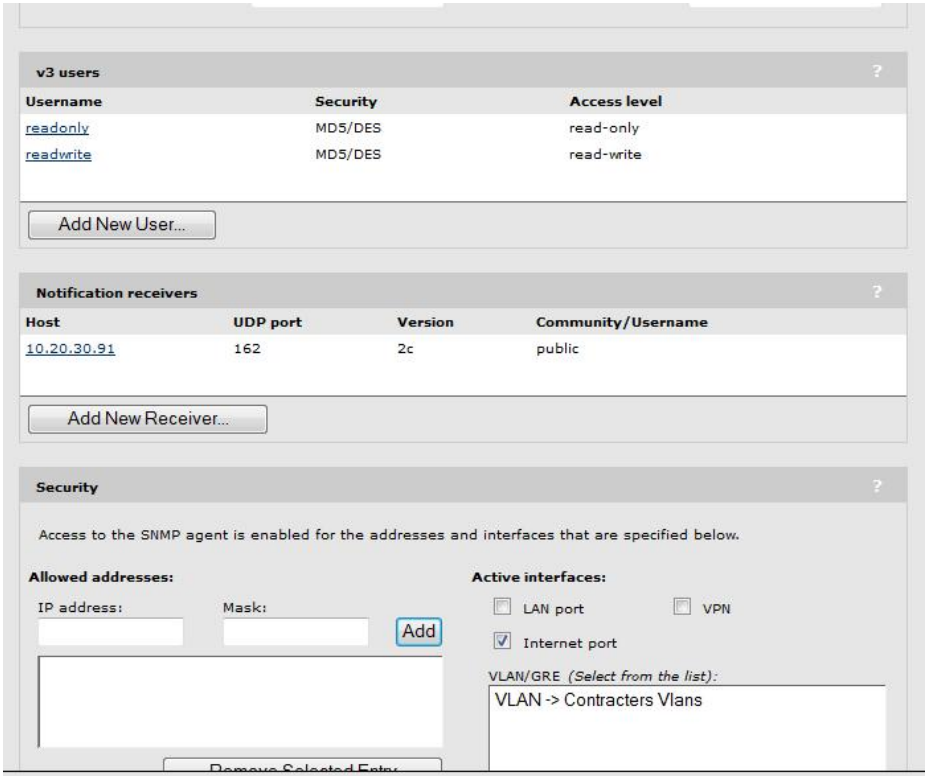
To enable PCM to manage the controller and radio information to be passed into PMM the following SNMP variables need to be configured:

- Device location
- Community strings
- Notification Receiver (PCM+ Server)
- Active Interface – ensure Internet port is checked and uncheck LAN port (LAN port is considered untrusted).



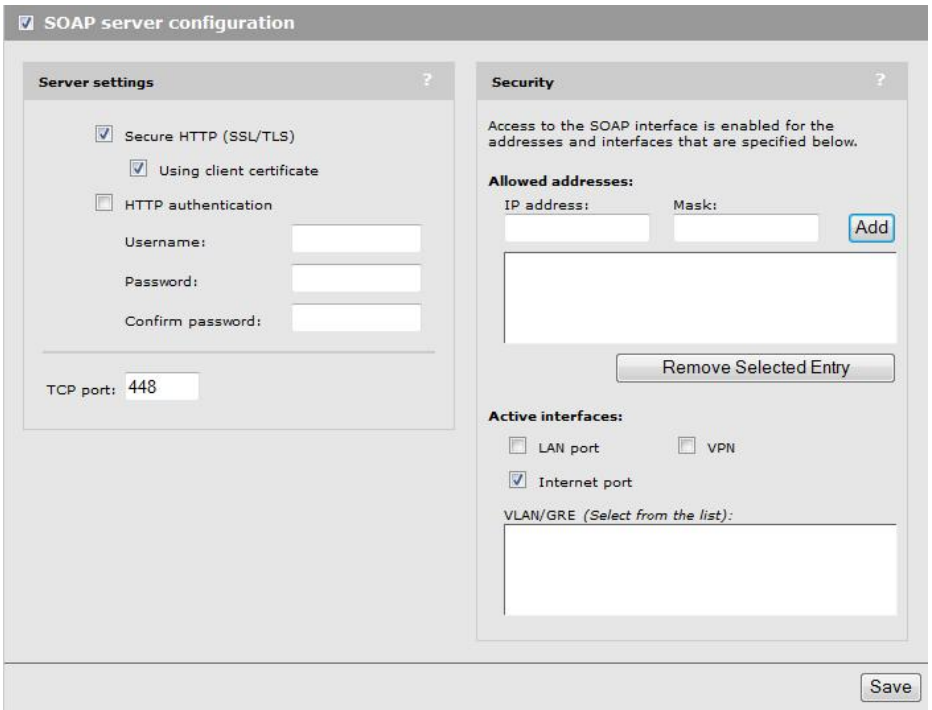
You have the option to customise the notifications sent to the SNMP manager by selecting “Configure notifications” as shown in the example screen shot below.





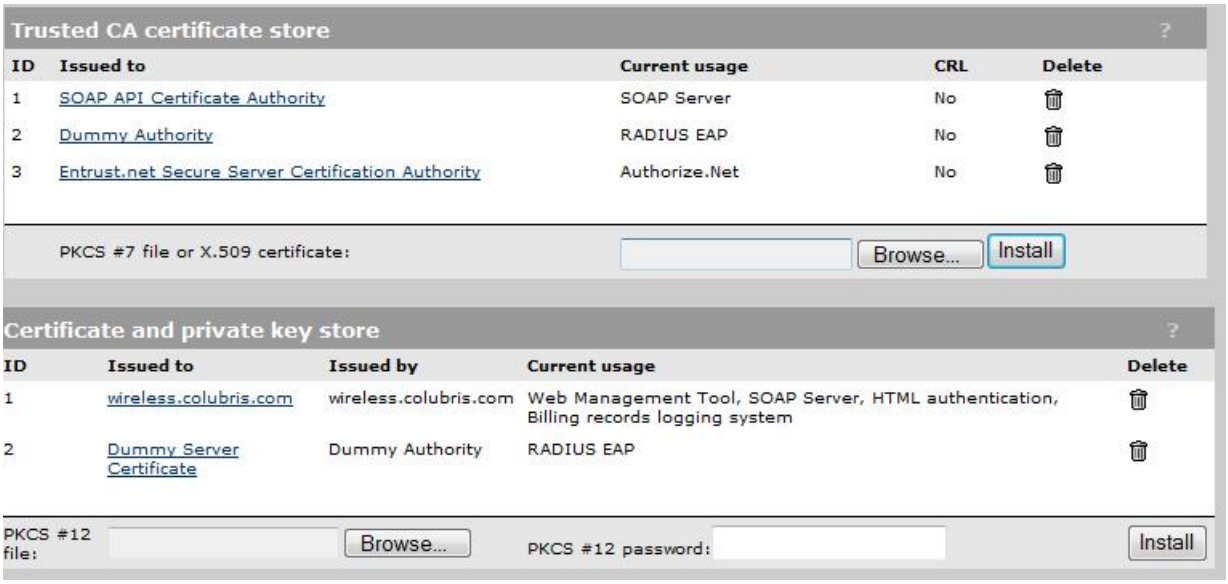
Service Controller | Management | SOAP

The SOAP server configuration is required to enable the MSM APs to send statistics back to PMM and enable the Guest Management Software (GMS) to operate. Because the Internet Port is the trusted port, it is checked and LAN port should be unchecked.



Service Controller – Security-Certificate Stores

The final step to configuring the SOAP server is to ensure the SOAP API Certificate Authority



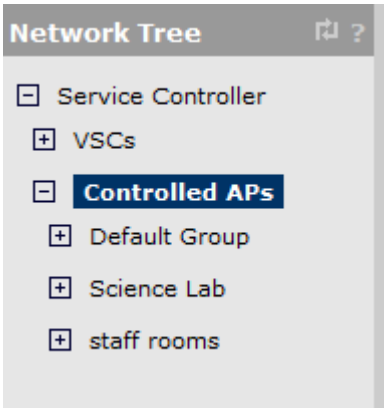
The SOAP protocol is outside the boundaries of this document, for further information there are many tutorials that can be found on the Internet.

5 Access Point Provisioning

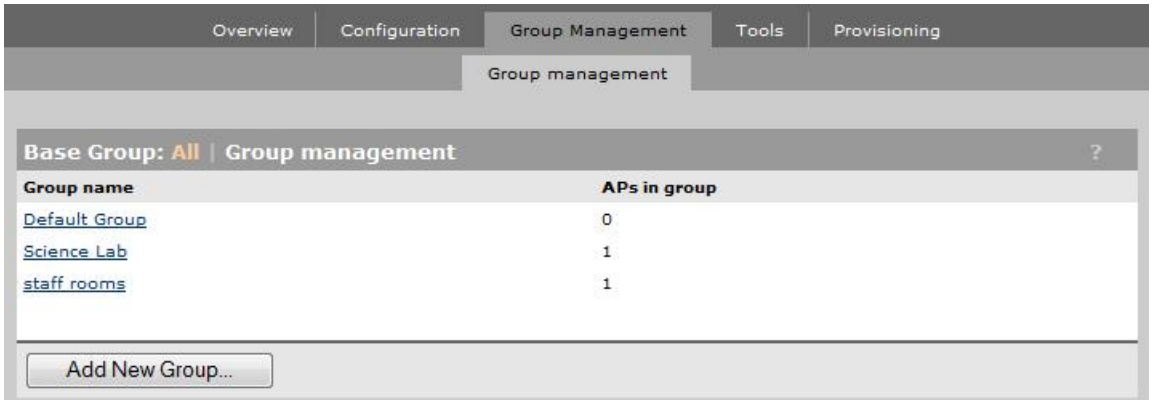
The MSM solution enables administrators to create custom groups for the Access points. These groups can be based upon location, function or access point type for example. When an AP connects to the network and is provided with an IP address by the DHCP server it is automatically placed into the Default Group. In the example provided the Default Group is being uses as a “holding” place for new APs. The following groups were created to house the MSM422 and MSM410 Access points.

In the example provided two groups have created as shown below. (These can be modified as appropriate to suit the environment.)

- Science Lab
- Staff rooms

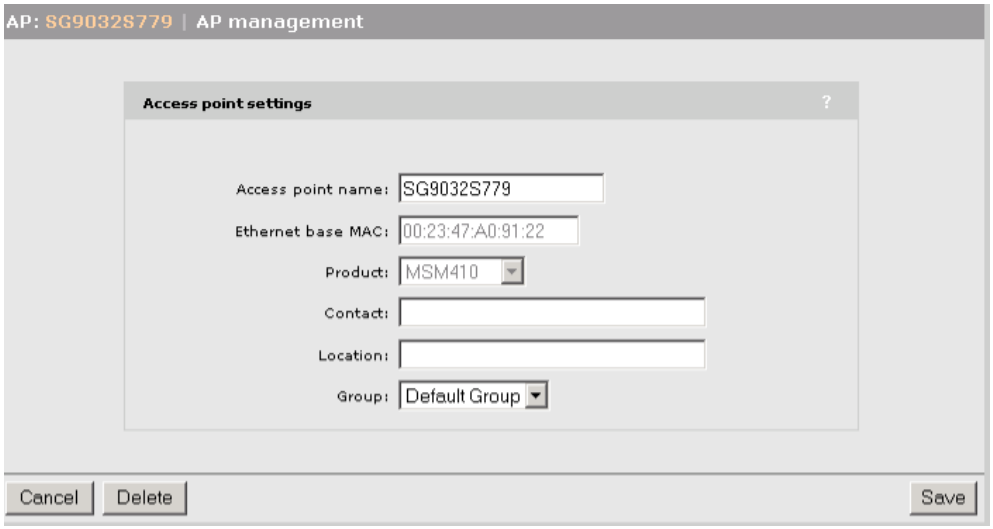


Controlled APs | Group Management | Group Management
Add the Science Lab and Staff Rooms

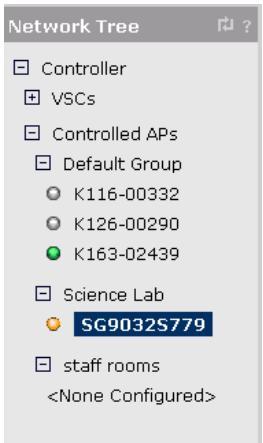


AP | Device Management

Once the Groups have been created the Access points can either be “Dragged and Dropped” into the appropriate group or select the Access Point, Device Management then select the appropriate Group.

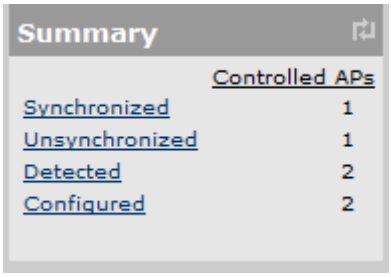


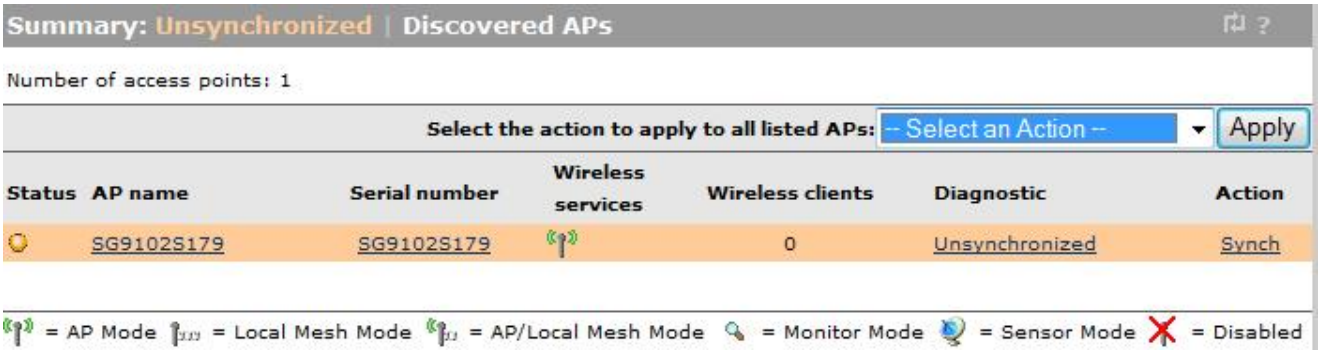
In this example, the MSM410 has been moved into group “Science Lab” and the MSM422 moved into group “staff rooms”.



Note the icon next to the AP has turned amber in colour, this signifies the AP is unsynchronized. Meaning the AP requires synchronization to pick-up the last configuration changes.

Once the move has been completed the Access Points will require Synchronising. This process is required whenever there is a change to the Radio (ie channels, auto power, etc) or binding/unbinding of VSCs and some changes within the VSC. The screen shot below depicts this:





6 Wireless_Students VSC

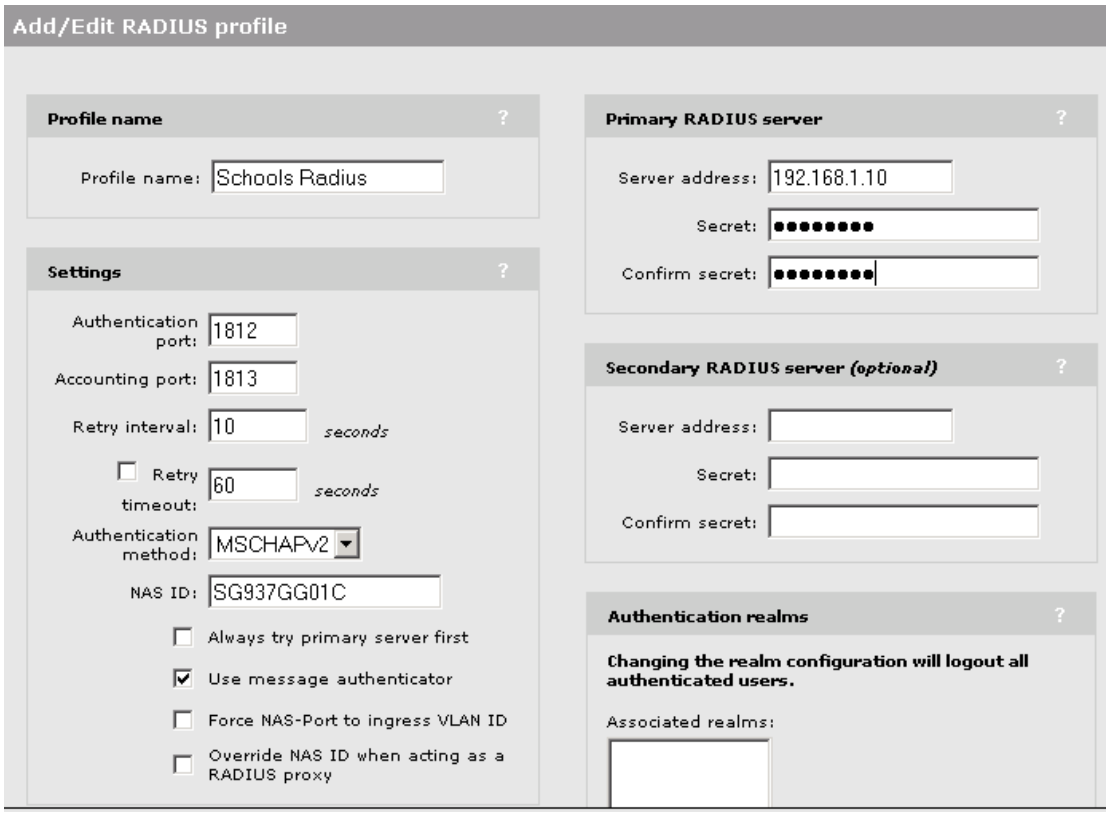
Students are considered “trusted” network connections and so they will use 802.1x for authentication. ALL traffic from the VSC will be passed directly onto the network from the AP. As the APs will be facilitating the Radius authentication they need to be defined as Radius Clients and should have a static IP address or ensure the DHCP assigns a preconfigured IP address to each AP.

This scenario leverages existing Radius, certificates and Active Directory infrastructure and assumes appropriate client configuration. Please refer to Section 9 for MS NPS and AD configuration.

6.1 Radius Configuration

Service Controller | Authentication | Radius Profiles

The first step is to create a Radius Profile pointing to the existing NAP/IAS/Radius Server.
An account will need to be created on the Radius Server for the controller. All other items are default.



Once complete, the Wireless Student VSC can be created.

6.2 Network Profiles

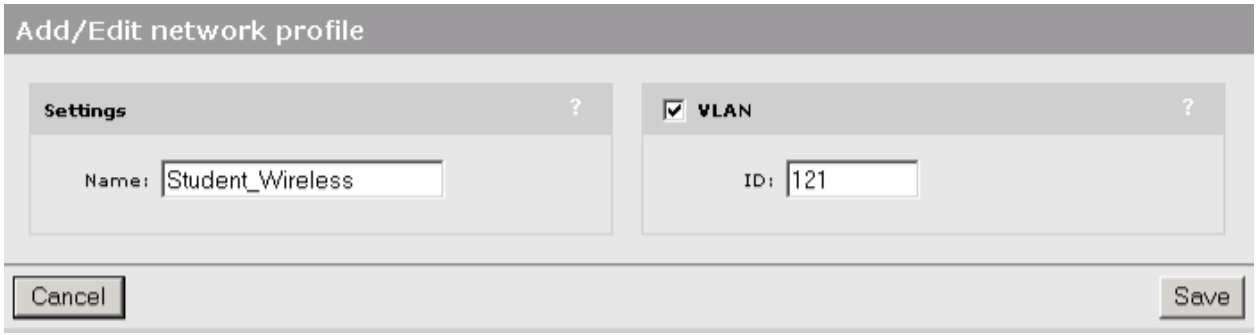
Network Profiles are new to version 5.4. A network profile is used to associate a friendly name with a network definition. It is designed to make it easy to configure the same settings in multiple places on the controller. For example, if you define a profile with the VLAN 10, that profile can be used to:

- Configure VLAN 10 on the controller's Internet or LAN port using the Controller >> Network > Ports page.
- Configure VLAN 10 as the egress network for a group of APs when binding them to a VSC using the Controlled APs > [group] >> VSC bindings page.
- Configure VLAN 10 as the home network for an AP using the Controlled APs >> Configuration > Home network page

Whenever traffic is being handed off to the network from the AP (ie non access controlled VSC, therefore the controller is not seeing any traffic from this VSC) the VSC needs to be assigned a VLAN. On the switch the port connecting the AP must be tagged for the same VLAN.

For the Wireless_Students VSC a Network Profile for VLAN 121 is created. The next step is to bind this profile to a VSC.

Controller | Network | Network Profiles

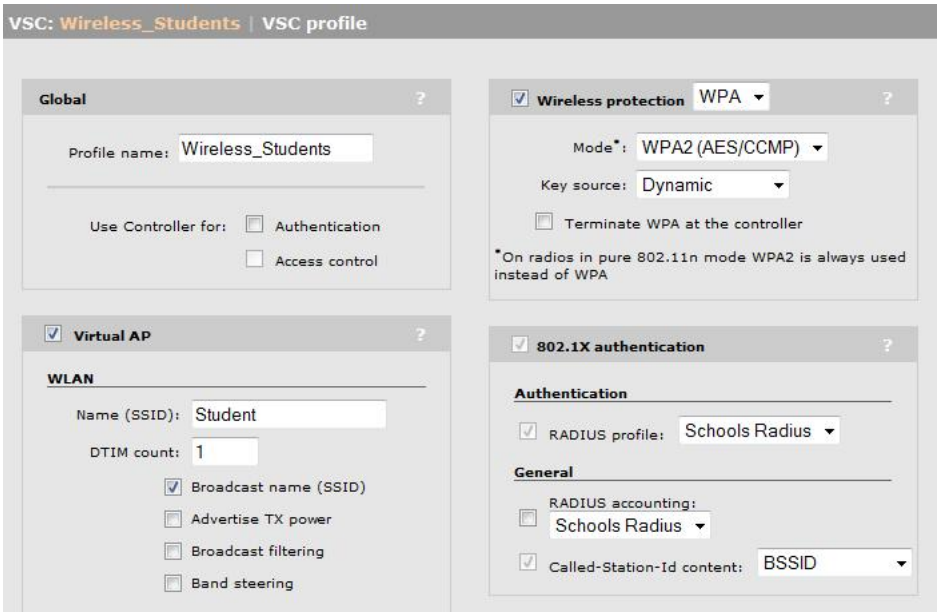


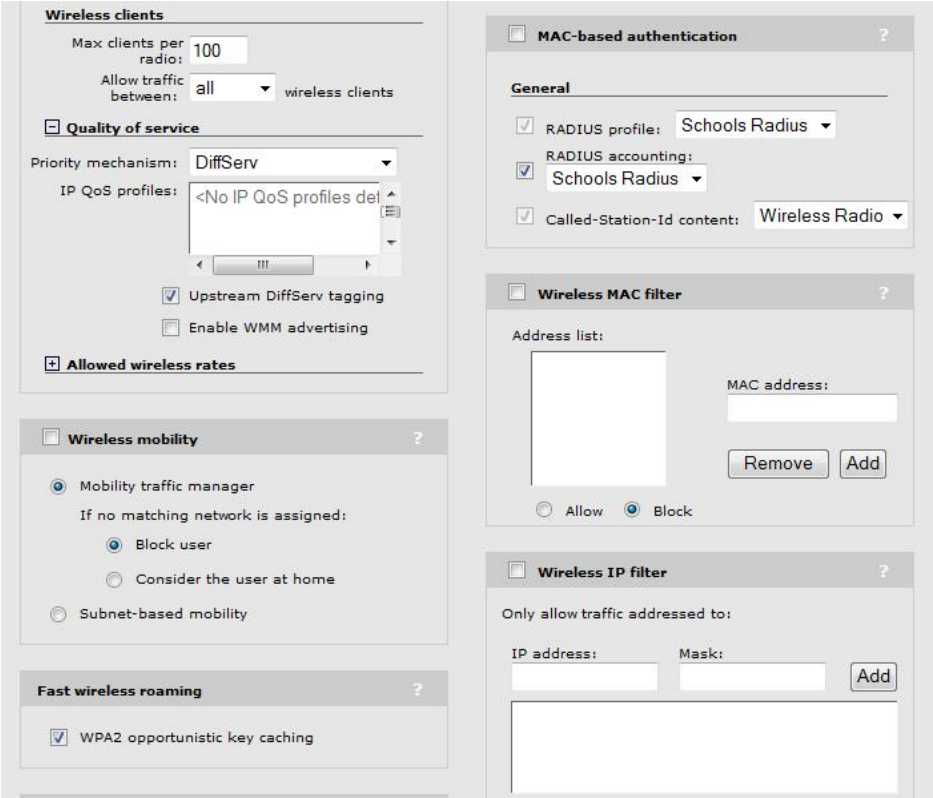
6.3 Wireless_Student VSC Configuration

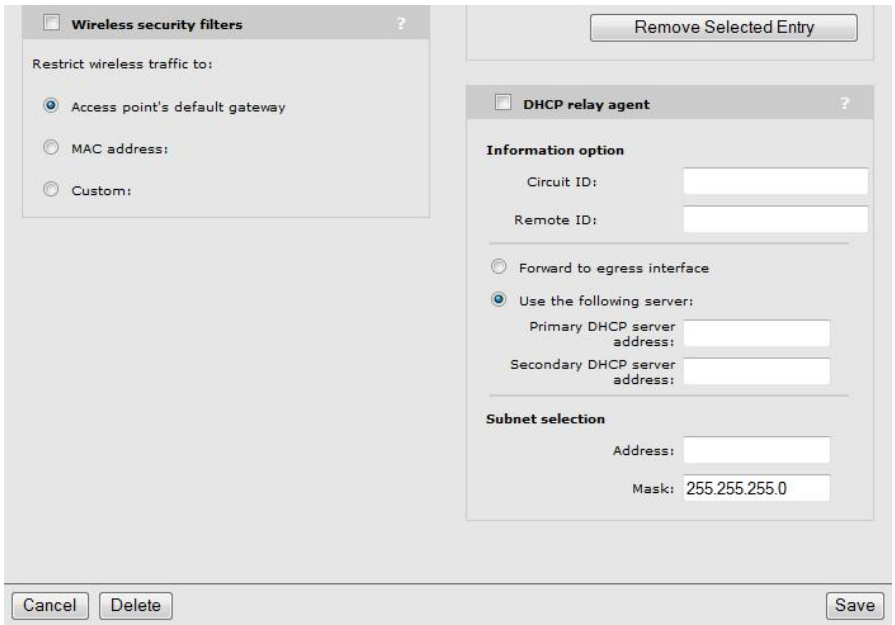
VSC | Add New VSC Profile

Key points to note:

1. Both Access Control and Authentication are UNCHECKED
2. Client traffic is not being tunnelled
3. Wireless Security Filters is unchecked
4. WPA2 AES encryption with Dynamic keys
5. 802.1x is checked, under authentication select Radius Profile then select the profile you have just created.
6. Uncheck WMM advertising
7. Uncheck Wireless Security Filters –In this case the network will apply any ACLs/traffic control mechanisms







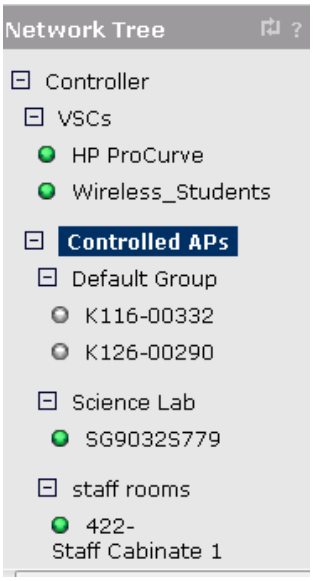
You will notice an option to terminate the WPA at the controller within the WPA settings; this feature is intended for low throughput applications, such as supporting point of sale (POS) terminals that require end-to-end encryption to meet security criteria such as that specified by PCI DSS. Please refer the user manual for details instructions and design configurations.

We have left the maximum clients per radio as default. When configuring this option consideration must be taken as to application and client throughput requirement. Due to the diversity of applications and throughput requirements connection we are not prescribing limits per AP within this guide.

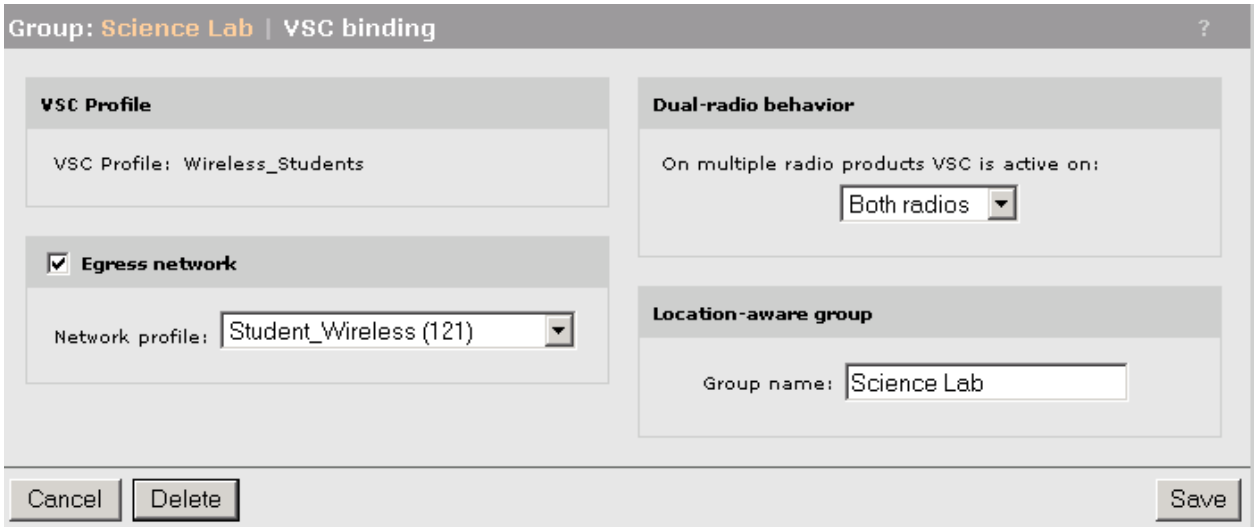
6.4 VSC Binding

Radio Group | VSC Bindings

The screen shot below shows the current Radio Groups. In this example we are going to activate this VSC on all radios in the “Science Lab”



When binding the Profile to the VSC, the Egress Network option is checked to ensure traffic is handed off at the AP in VLAN 121. This VSC will be active on Both Radios (you can select either radio 1 or 2) and it will be applied to all radios within the “Science Lab” location. Repeat this process to advertise this VSC in the Staff Room.



Key point to note:
The SSID Wireless_Students will not be broadcast until the VSC is bound to the appropriate AP Groups. In this scenario the VSC Binding is also used to inform the AP which VLAN to egress the student traffic onto.

Remember to Synchronise the APs

Upon successful authentication the client will receive an IP address in the 10.20.121.x subnet from the enterprise DHCP server.

To recap, the client will receive an IP address in the 10.20.121.x subnet because the Student VSC binding uses egress VLAN 121, which is tagged on the switch port that the AP is connected to. On the routing (core) switch this VLAN is configured with an “IP helper-address” pointing to the enterprise DHCP server. Refer to the switch configuration in Section 2.2.

7 Wireless_Teachers VSC

In this scenario we are treating the teachers slightly differently. The controller will proxy authentication requests directly to Active Directory and upon successful authentication the following traffic will be passed from the AP directly onto the network in VLAN 131. It should be noted when using the controller as a proxy, it becomes a single point of failure. There are a number of steps involved in setting up this configuration as follows:

7.1 Network Profile

Service Controller | Network | Network Profiles

The VLAN 131 needs to be defined

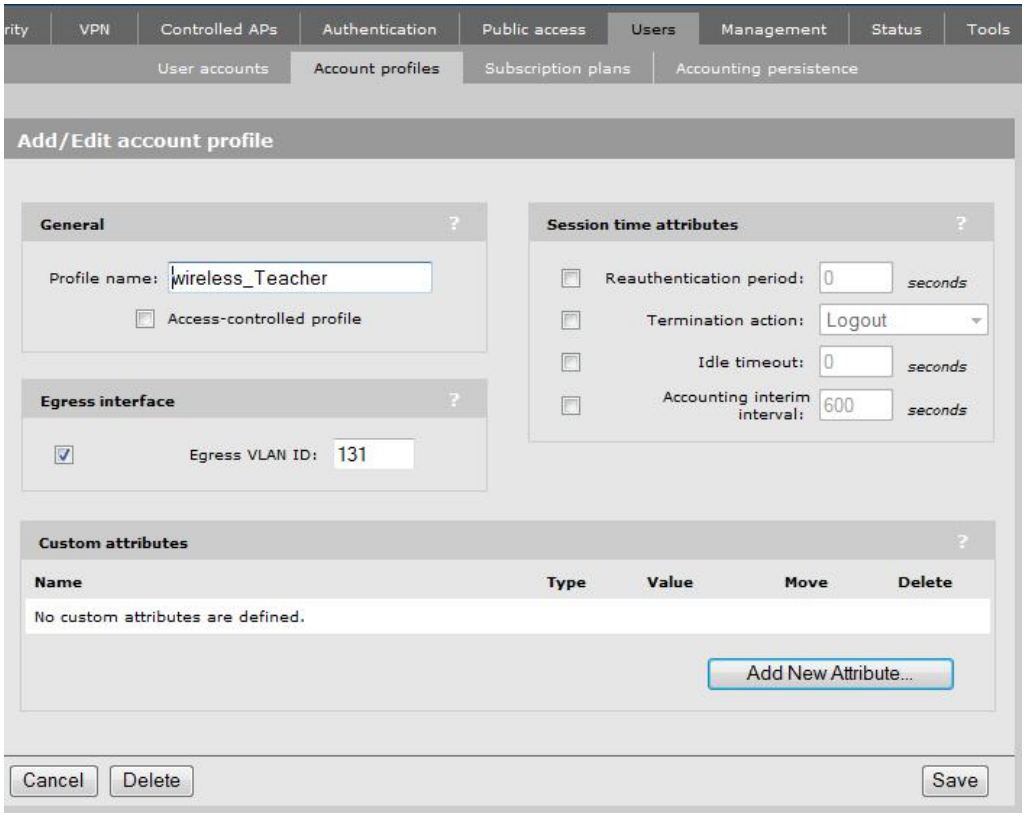
7.2 Account Profile

The Account profile will be used to tell the AP to use VLAN 131 as the Egress VLAN for all data traffic; remembering that the controller is only being used to assist with authentication. The data will be passed off onto the network from the AP into VLAN 131.

Service Controller | Users | Account Profiles

Key points to note:

1. Ensure Access-Controlled Profile is UNCHECKED
2. Check Egress VLAN ID and use the VLAN created on the switch for Wireless_Teachers (131)



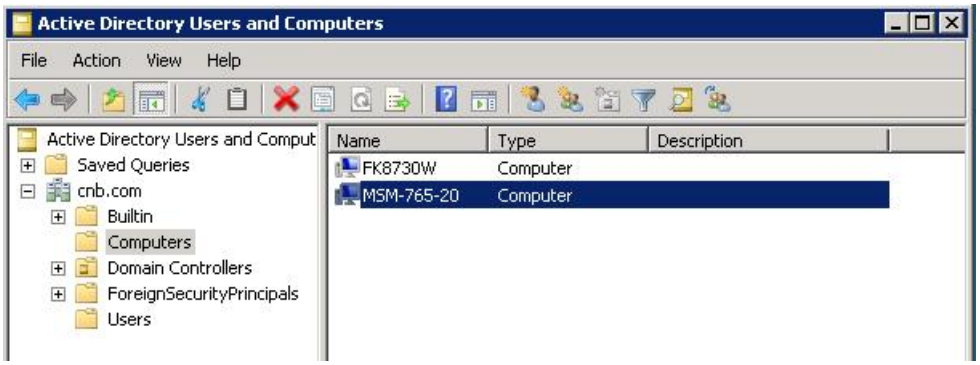
7.3 Active Directory Configuration

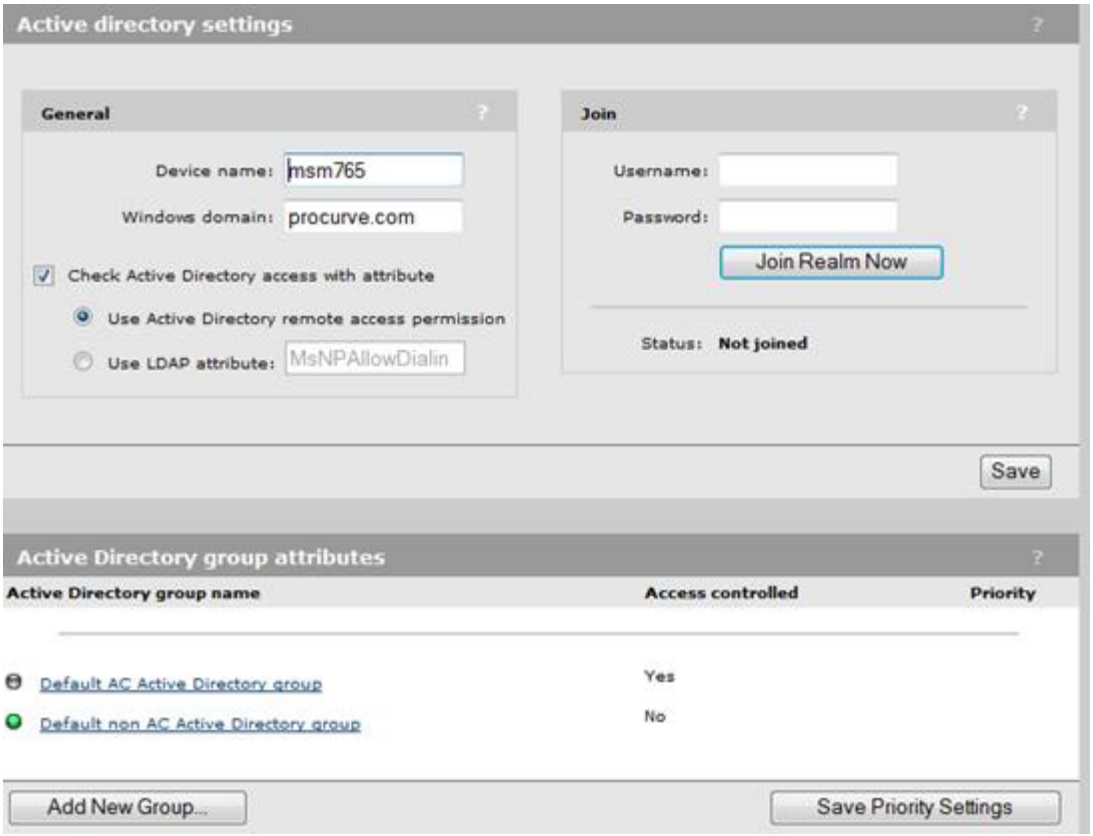
This step involves configuring the interface into AD to enable the controller to “proxy” the teacher’s authentication requests. Assigning a device name and specifying the domain are the parameters required to create a “device” account in the AD Domain for the controller. Using the Domain Administrators account (or account with device creation privileges) Join the Domain (Join Realm Now). Upon successfully joining the domain the status will change to “Joined”. The “Check Active Directory Access with Attribute looks for dial-in permissions on the user account. This type of authentication requires any client computers to be part of the domain.

Service Controller | Authentication | Active Directory

Key Points to note:

1. If using an MSM 765 you will need to ensure the switch and AD Domain have their times synchronised as the MSM765 receives its time from the switch. It is recommended you use SNTP and timeserver(s).
2. If you receive a “Domain not found” message check your DNS.

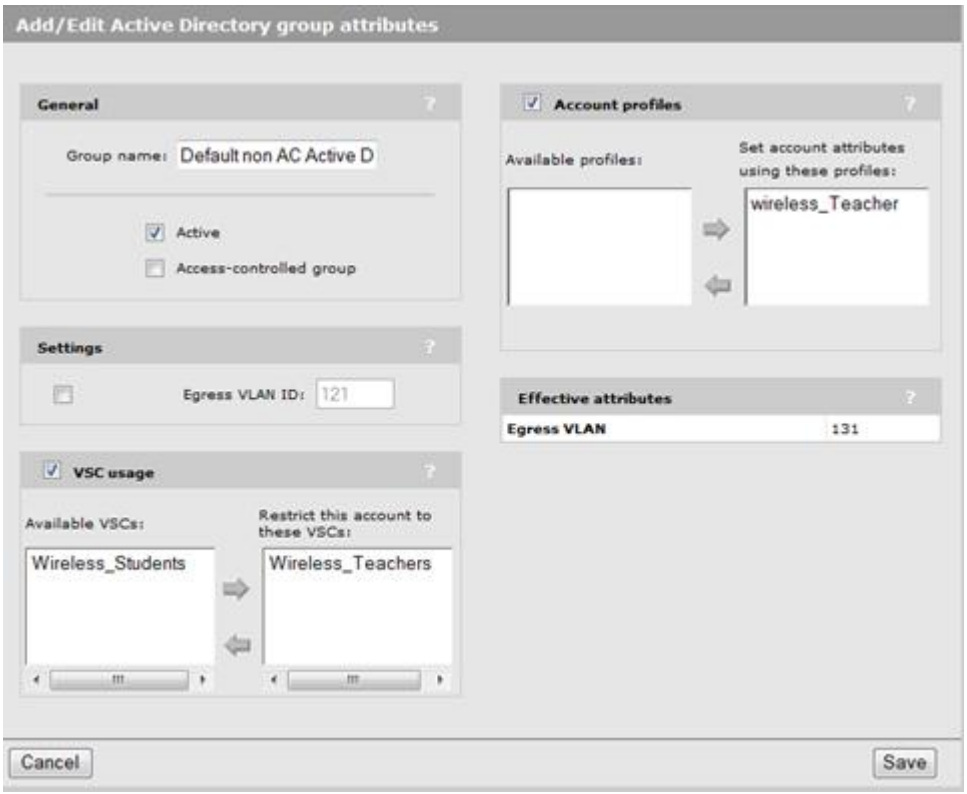




The next step is to edit the Active Directory Group Attributes. In this example we are using the Default non AC Active Directory Group – meaning it does not check for any group or OU membership as part of the authentication process.

Key points to note:

1. Only Teachers are using this means of authentication, therefore VSC Usage is Checked and Wireless_Teachers VSC is selected.
2. We are using an Account Profile Wireless_Teacher previously created to specify the egress VLAN (note effective attributes). You could also specify the egress VLAN ID under settings noting any Account profiles will take precedence.



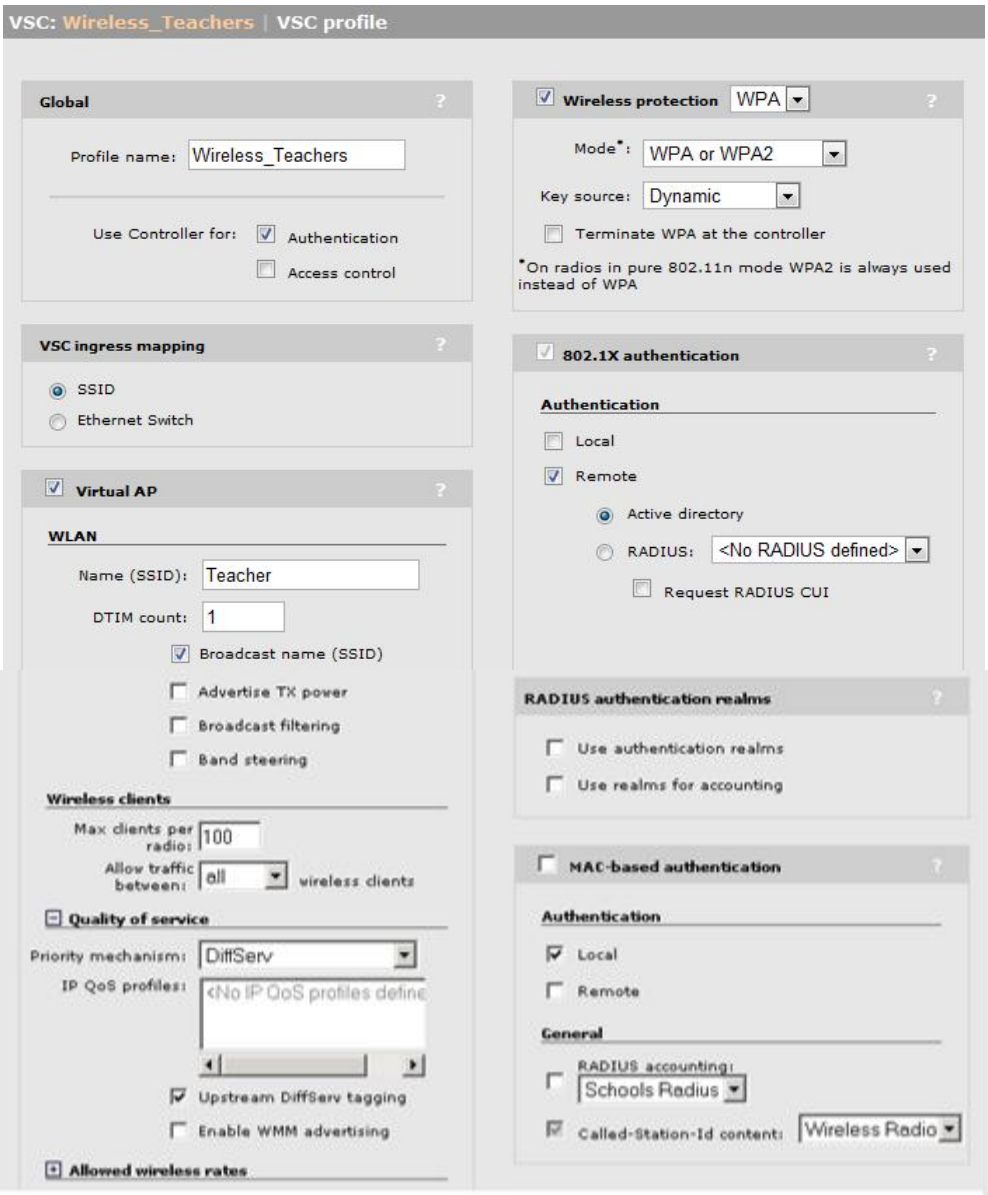
7.4 Wireless_Teachers VSC Configuration

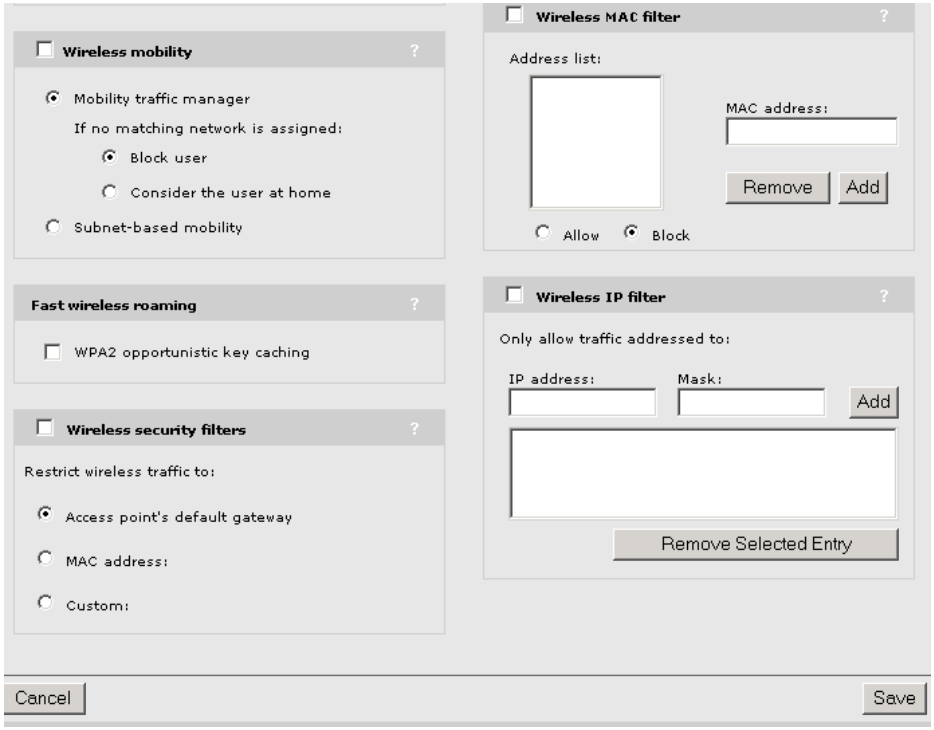
The VSC "Wireless_Teachers" was created, this VSC uses the Service Controller for Authentication but not Access Control and the client traffic is not being tunnelled. In this scenario we are using WPA with dynamic keys using WPA/WPA2 with dynamic keys, selecting Dynamic keys automatically checks 802.1x authentication as we are using RADIUS between the client and AP and the controller initiates an LDAP connection back to the Active Directory server.

VSC | Add New VSC Profile

Key Points to note:

1. Checking the Remote option in the 802,1X authentication box reveals the Active Directory option.
2. Uncheck WMM advertising.



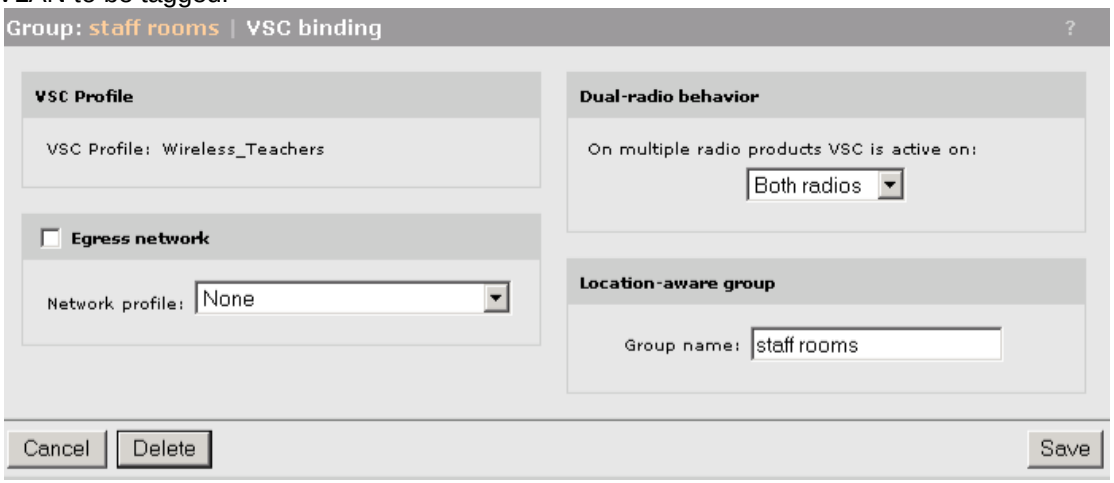


7.5 VSC Binding

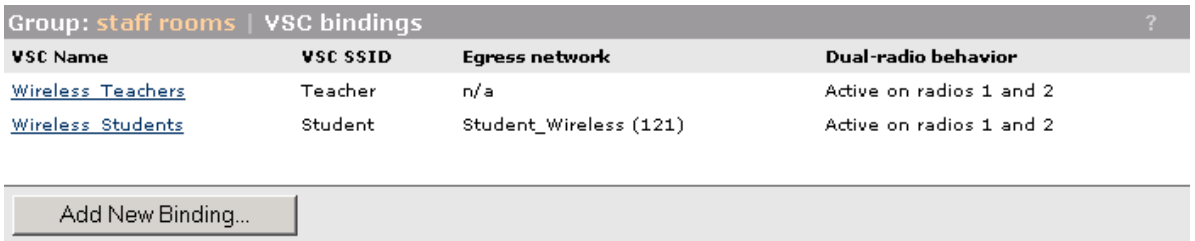
The VSC then needs to be bound to the appropriate Access point groups in order to have the AP broadcast the SSID.

Access point Group | VSC Bindings

Key point to note:
"Use Egress VLAN" is UNCHECKED and no network profile has been assigned as the egress VLAN has been specified in the account profile and the MSM AP will pick it up from the account profile – it does not need to be added here. The switch does need to be configured for this VLAN and the port connecting the AP requires this VLAN to be tagged.



The screen shot below illustrates the current bindings for staff Room Access Point Group – note the Wireless Teacher VSC does not have an egress VLAN nominated.



Remember to Synchronise the APs

Upon successful authentication the client will receive an IP address in the 10.20.131.x subnet. Again the routing switch has been configured with an "IP Helper-address" point to the DHCP server, which is configured with the corresponding scope.

8 Guest Access

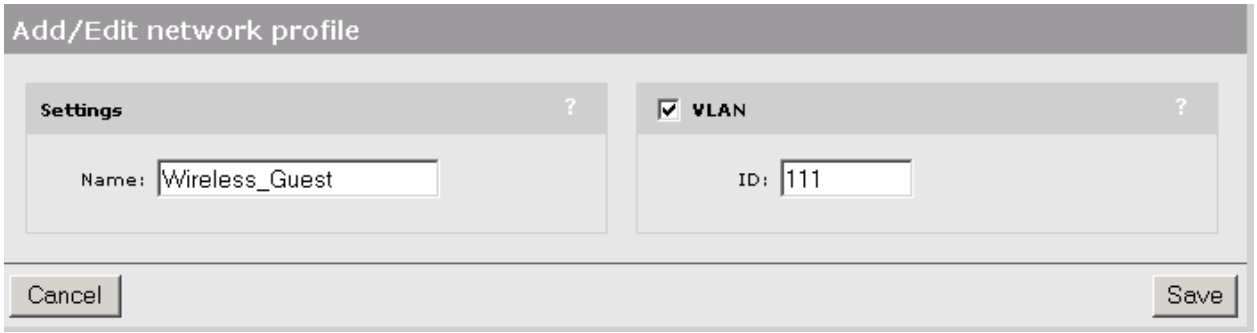
When providing Guest Access we want to shield the internal/corporate network as much as possible. The controller is providing DHCP and DNS services, NAT. The Guest traffic will be NAT'd from the controllers IP Address Range to a real IP address 10.20.111.200 within the Guest VLAN.

This particular example provides the frame work for the HPN Guest Management Software (please refer to http://www.hp.com/rnd/support/manuals/guestman.htm for instructions on this product).

8.1 Network Profiles

Create a network profile for the Guest VLAN.

Service Controller | Network | Network Profiles



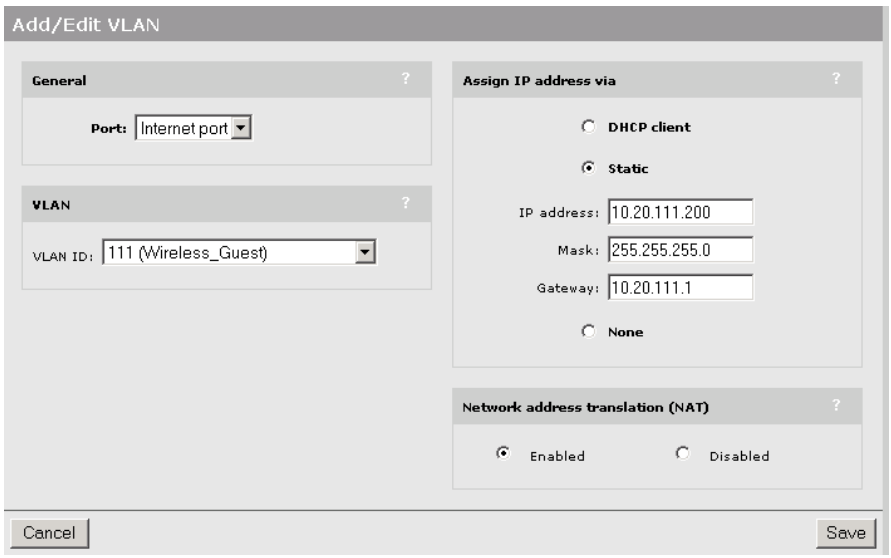
8.2 Port Configuration

The Guest VLAN ID 111 needs to be added to the controller with a static IP address of 10.20.111.200, it will use the switch IP address for VLAN 111 as the default Gateway.

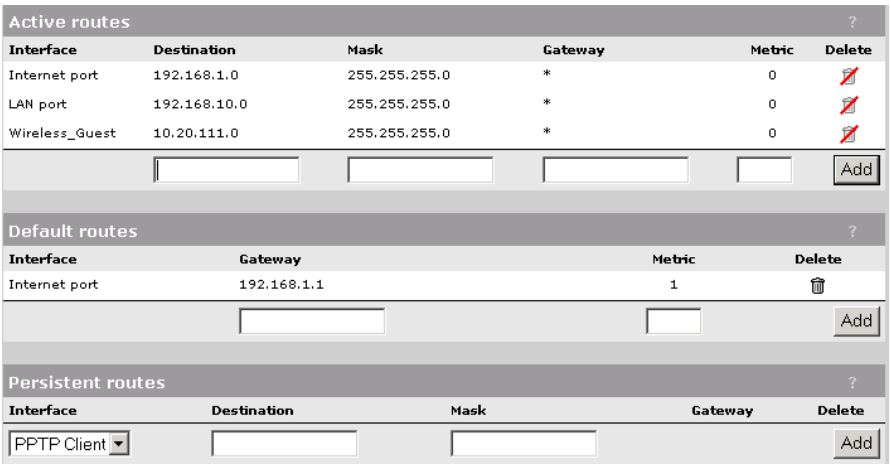
Network | Ports

Key Point to note

1. Ensure NAT is enabled



Upon creating the VLAN on the controller the controller will automatically add a route to its table.



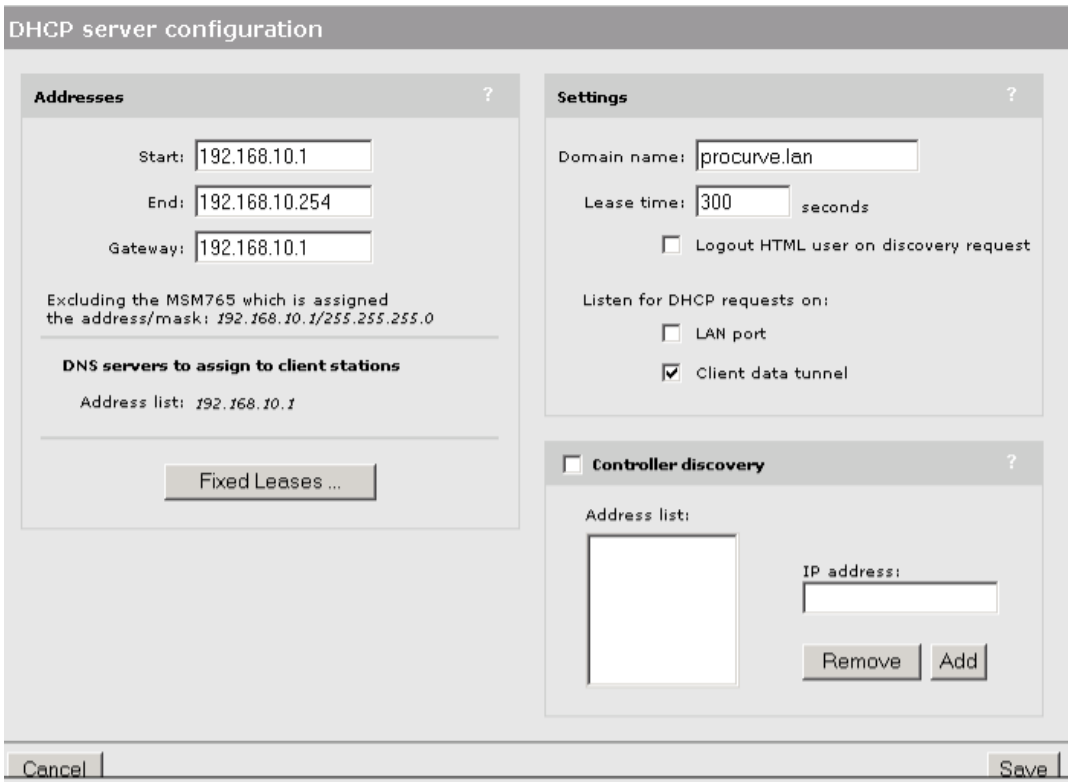
8.3 DHCP Server

The local DHCP server will be used to provide Guests with and IP address. This IP address range is outside the current internal scopes. The screen shot below illustrates the IP address scheme to be used for Guests and Domain Name

Service Controller | Network | Address Allocation

Key point to note:

Listen for the DCHP requests on Client Data tunnel is checked, if this is not checked the guests will not receive an IP address.



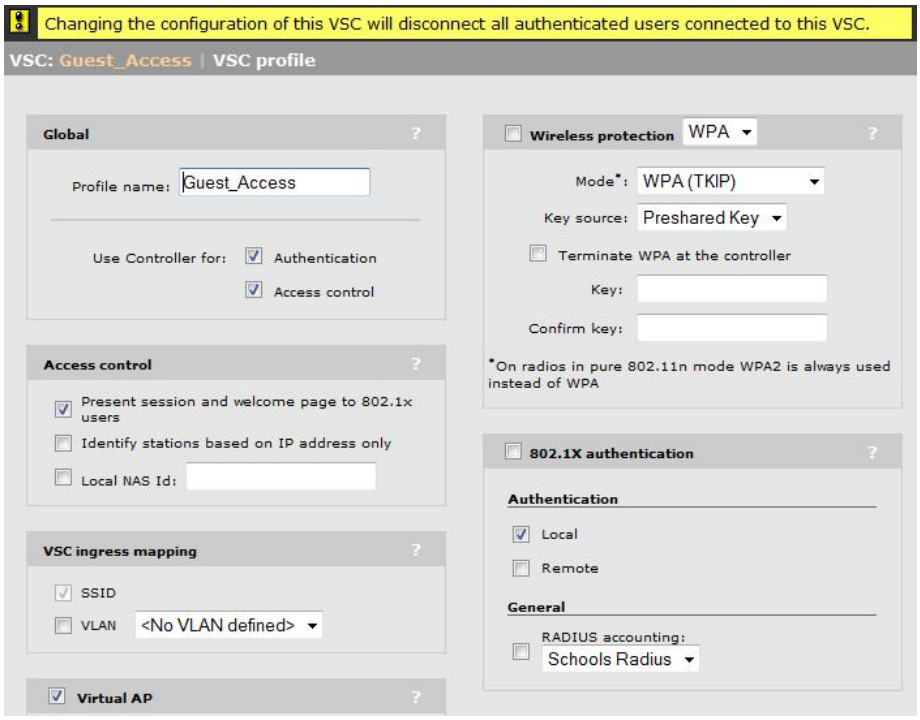
8.4 Guest_VSC Configuration

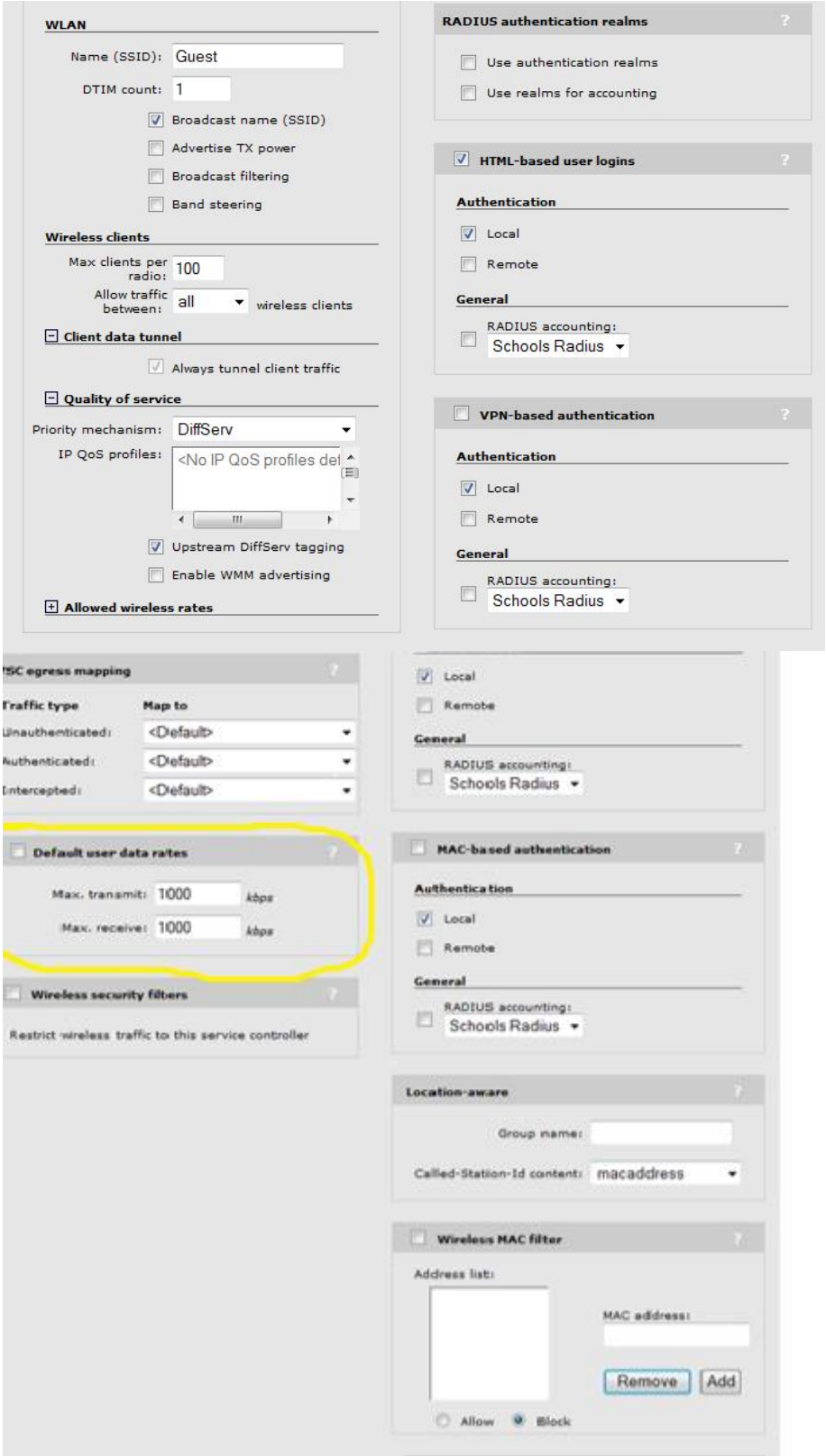
The Guest VSC is using the service controller for both Authentication and Access Control. In this scenario we are not using any wireless protection, the use of wireless protection for guest traffic will be dependent upon the particular site security policies. HTML login is checked and as we will create local accounts on the controller.

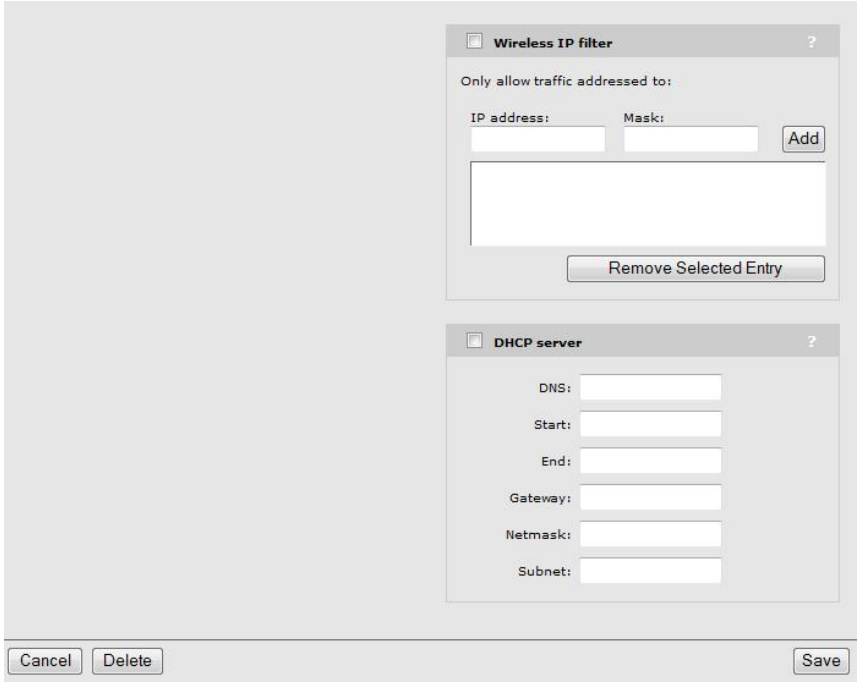
VSCs – Add New VSC profile.

Key points to note

1. Client Data Tunnel – always tunnel client traffic is checked. This creates a tunnel between the AP and controller and all Guest traffic traverses this tunnel.
2. Ensure WMM is unchecked







As this is an access controlled VSC, it is the most configurable type of VSC. As shown above, Default user data rates can be applied to limit upload/download bandwidth, users logins to the network can be controlled based upon the wireless AP to which a user is connected via the location-aware feature.

8.5 Creating Local User Accounts

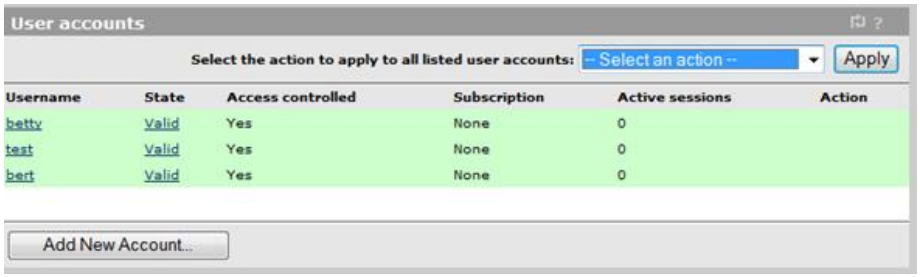
Below is an example of local account. These accounts can also be created using the Guest Management Software (GMS), which is designed for use by non-technical receptionists/front desk staff. This is a very simple Guest account, additional parameters can be applied through the use of Account Profiles.

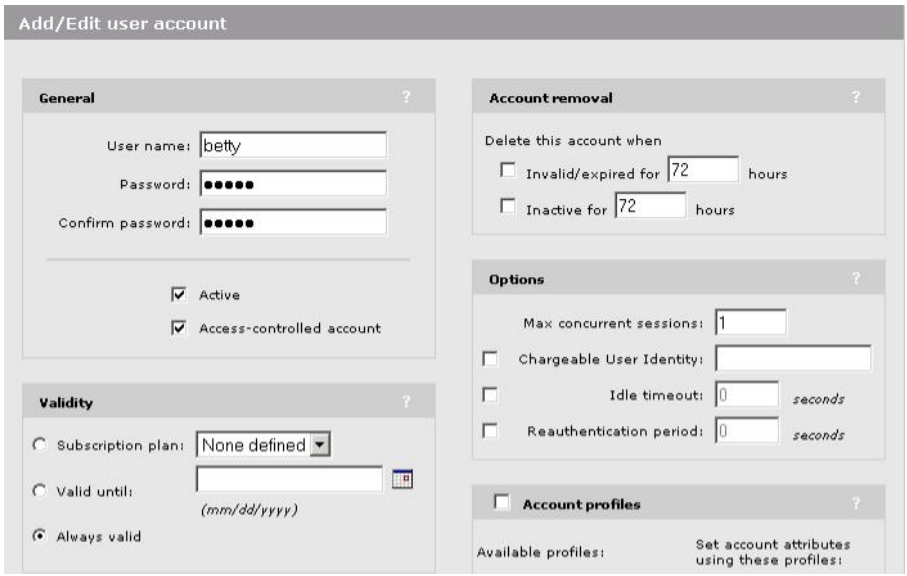
Service Controller | Users | User Accounts

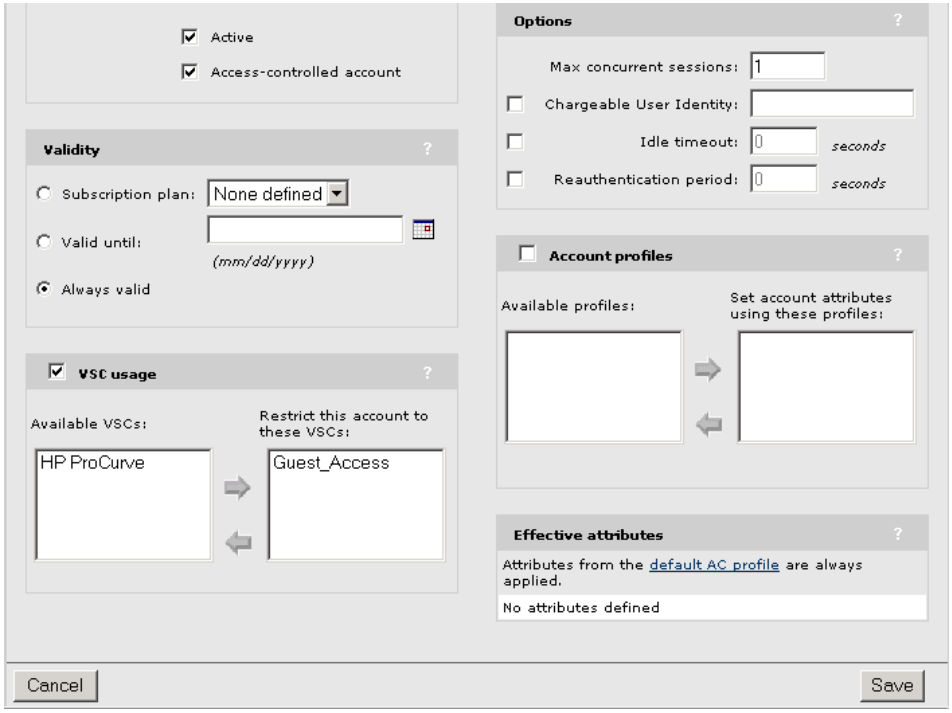
Key points to note:

1. The account is both Active and Access Controlled
2. The account is restricted to the Guest VSC

Select Add New Account



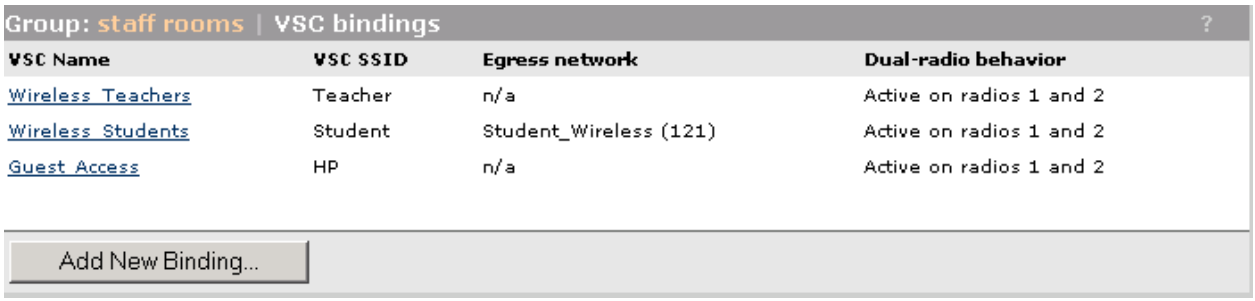




8.6 VSC Binding

Because the VLAN has been defined on the controller, the binding in this instance will be used to broadcast the Guest SSID from nominated Access point groups.

Access point Group | VSC Binding



Group: staff rooms | VSC bindings

VSC Name	VSC SSID	Egress network	Dual-radio behavior
Wireless_Teachers	Teacher	n/a	Active on radios 1 and 2
Wireless_Students	Student	Student_Wireless (121)	Active on radios 1 and 2
Guest_Access	HP	n/a	Active on radios 1 and 2

Add New Binding...

9 Appendix A: Windows Server 2008 NPS Configuration

In Windows Server 2008, Network Policy Server (NPS) replaces the Internet Authentication Service (IAS) component of Windows Server 2003.

NPS is the Microsoft implementation of the Remote Authentication Dial-In User Service (RADIUS) protocol, and can be configured to act as a RADIUS server or RADIUS proxy, providing centralized network access management. NPS can also be configured as a Network Access Protection (NAP) policy server. When NAP is deployed, NPS acts as a NAP policy server, performing client health checks against configured health policies.

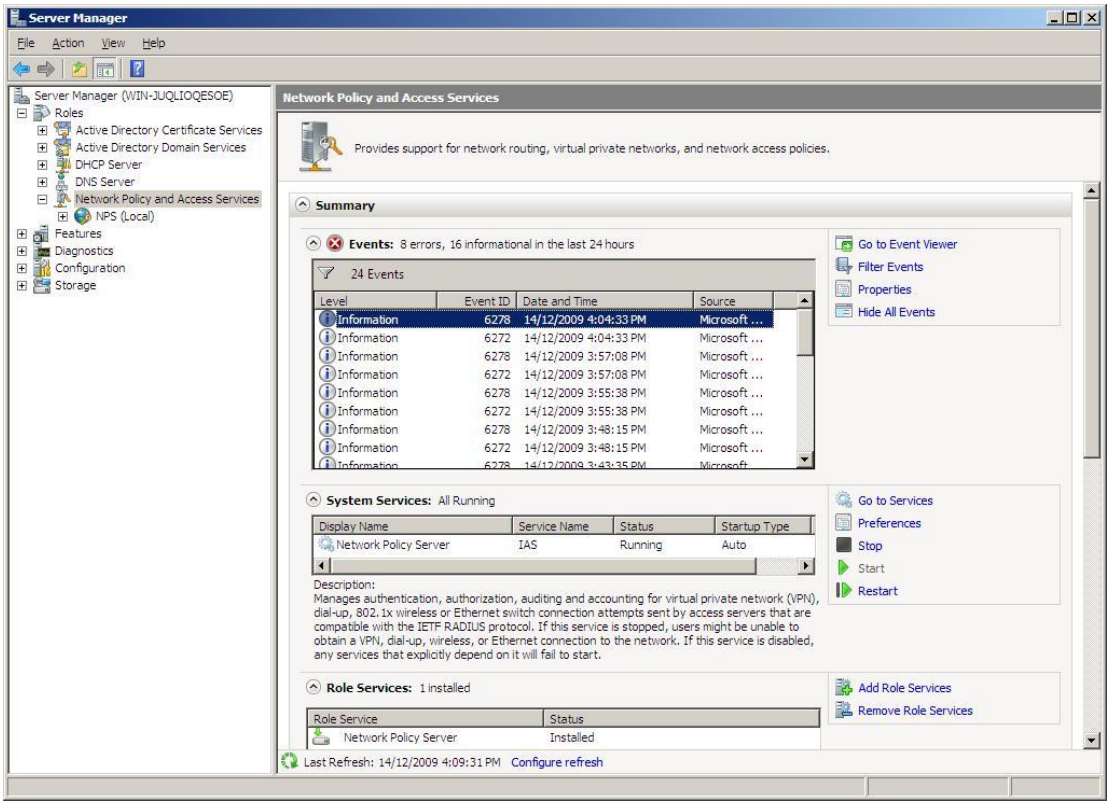
In this guide, NPS will be configured as a RADIUS server for 802.1X wireless/wired connections. Active Directory Certificate Services should already be configured and running.

9.1 Installing NPS

To complete this procedure, you must be a member of the Administrators group.

- Click **Start**, and then click **Server Manager**. In the left pane of Server Manager, click **Roles**, and in the details pane, in **Roles Summary**, click **Add Roles**. The Add Roles Wizard opens.
- In **Select Server Roles**, in **Roles**, select **Network Policy and Access Services**, and then click **Next**.
- In **Network Policy and Access Services**, click **Next**.
- In **Select Role Services**, in **Role Services**, select **Network Policy Server**, and then click **Next**.
- In **Confirm Installation Selections**, click **Install**.
- In **Installation Results**, review your installation results, and then click **Close**.

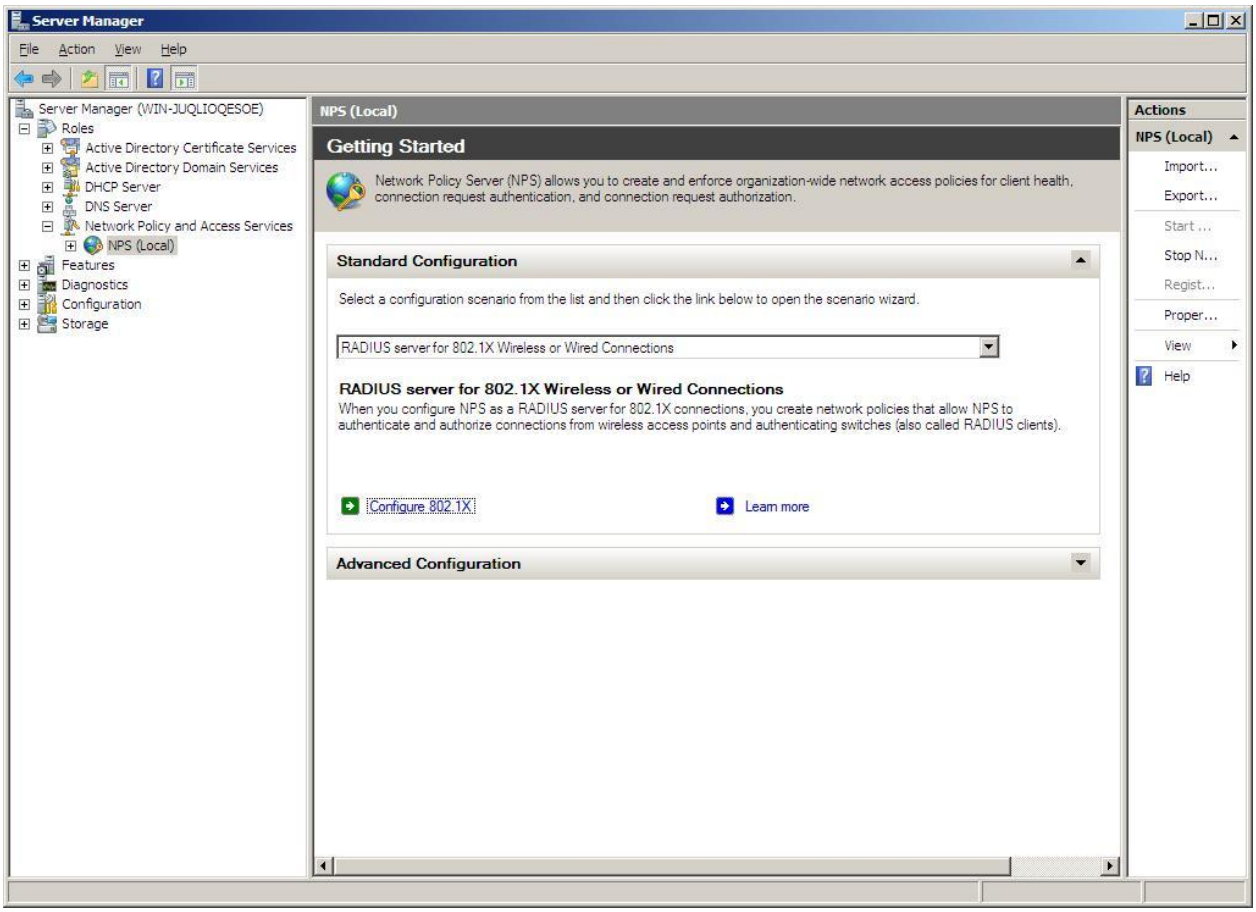
To confirm that NPS has been installed, start **Server Manager** and in the left frame under **Roles** select **Network Policy and Access Services**. Under **System Services**, the **Network Policy Server** should be in the running state.



9.2 Configuring NPS

To configure NPS, start the Network Policy Server by clicking Start | All Programs | Administrative Tools | Network Policy Server.

Under **Standard Configuration**, use the drop down list to select **RADIUS server for 802.1X Wireless or Wired Connections**.



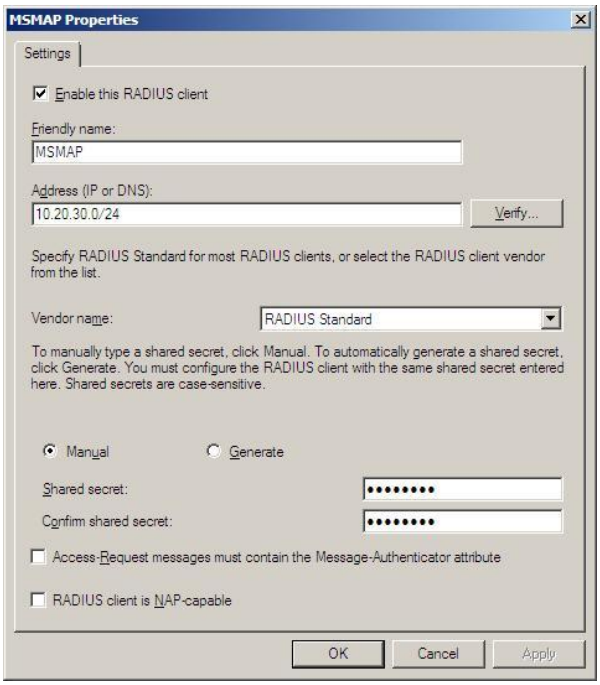
Click on **Configure 802.1X** and under **Type of 802.1X connections** select **Secure Wireless Connections**. In this example, the policy name used is also *Secure Wireless Connections*.

We then need to specify the wireless access points as RADIUS clients. NPS provides different functionality depending on the edition of Windows Server 2008 that you install.

With NPS in Windows Server 2008 Standard Edition, you can configure a maximum of 50 RADIUS clients and a maximum of 2 remote RADIUS server groups. You can define a RADIUS client by using a fully qualified domain name or an IP address, but you cannot define groups of RADIUS clients by specifying an IP address range.

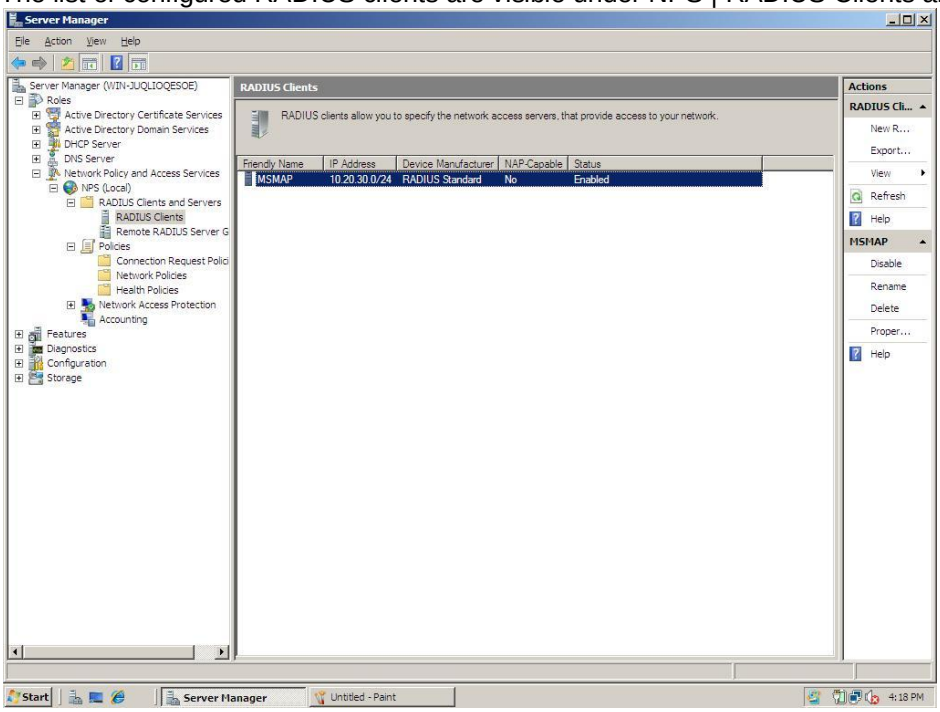
Windows Server 2008 Enterprise Edition allows an unlimited number of RADIUS clients that can be entered as a single RADIUS client using an IP subnet.

In this example, we configure a single RADIUS client for all of the HP ProCurve MSM wireless access points assigned with IP addresses in subnet 10.20.30.0/24.

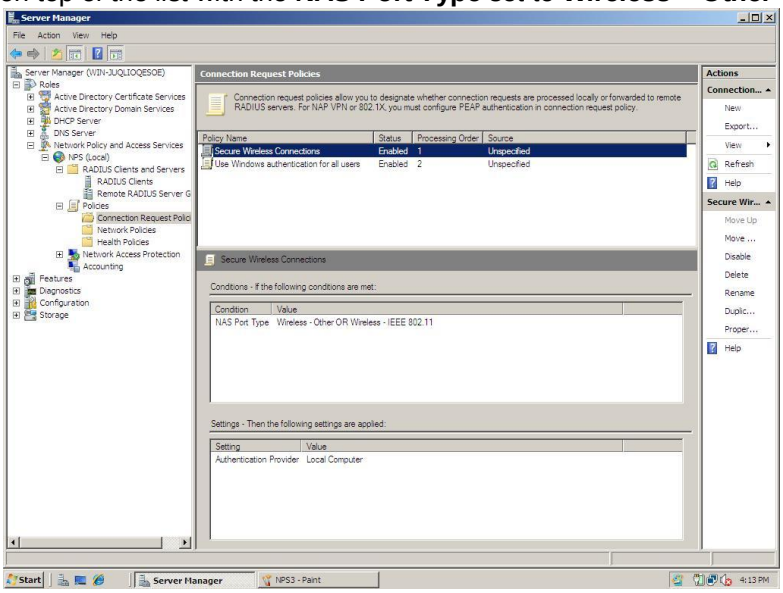


Take note of the RADIUS Client Shared Secret as it needs to be identical to the one configured on the HP ProCurve MSM7xx series controller used.

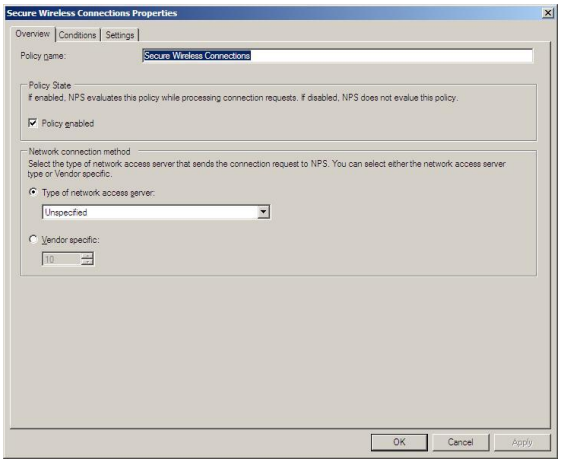
The list of configured RADIUS clients are visible under NPS | RADIUS Clients and Servers | RADIUS Clients.

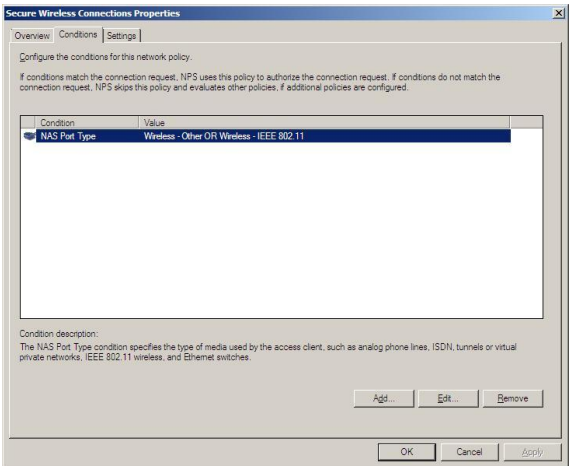


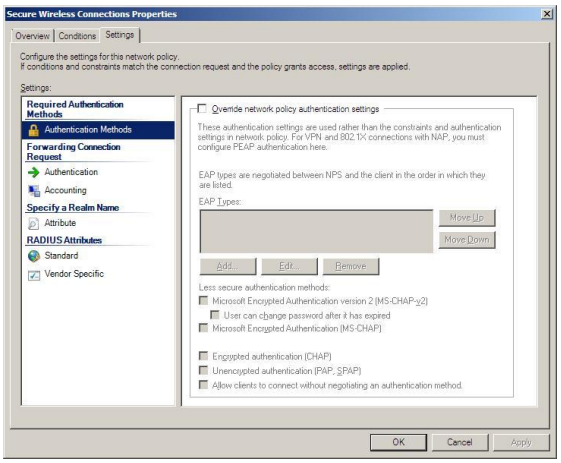
Under NPS | Policies | Connection Request Policies, ensure that the **Secure Wireless Connections** policy is on top of the list with the **NAS Port Type** set to **Wireless – Other OR Wireless – IEEE 802.11**.



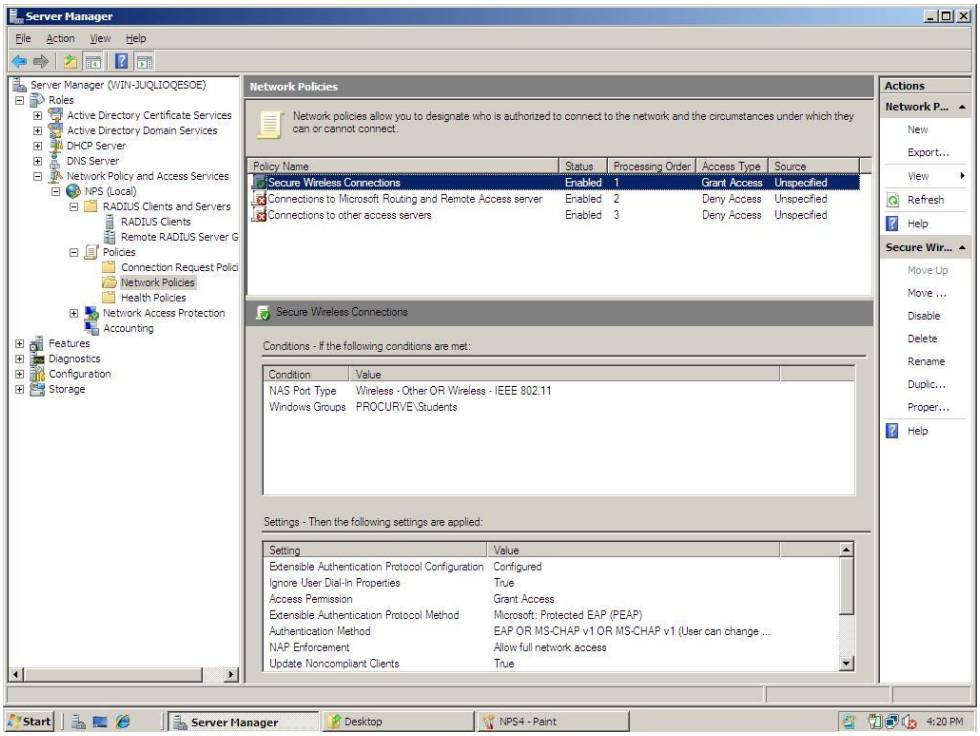
Double click on Secure Wireless Connections to view the policy properties. The following default parameters are shown.





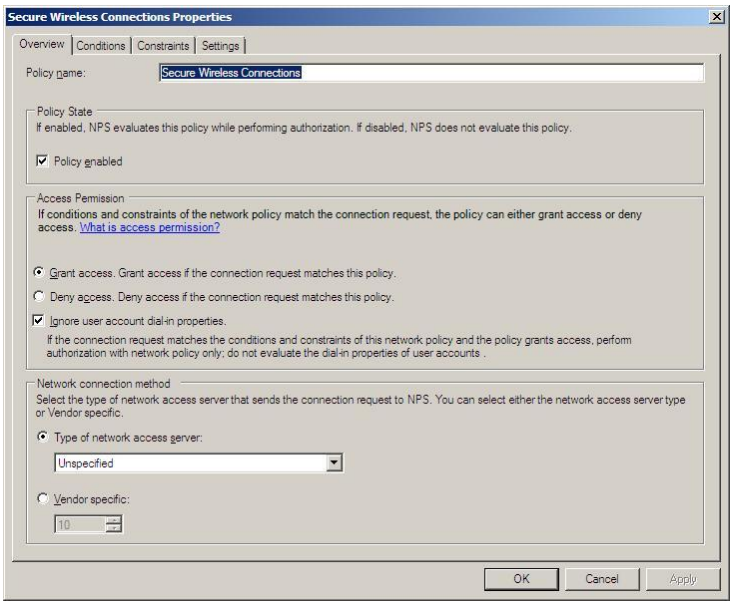


Under **Network Policies**, move up the **Secure Wireless Connections** policy to the top of the list.



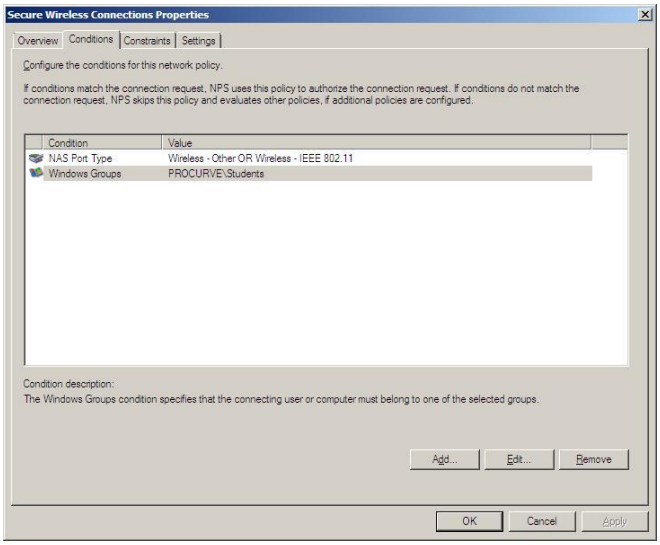
Configure the Network Policy to include the relevant Windows Group, Authentication Method and VLAN attribute.

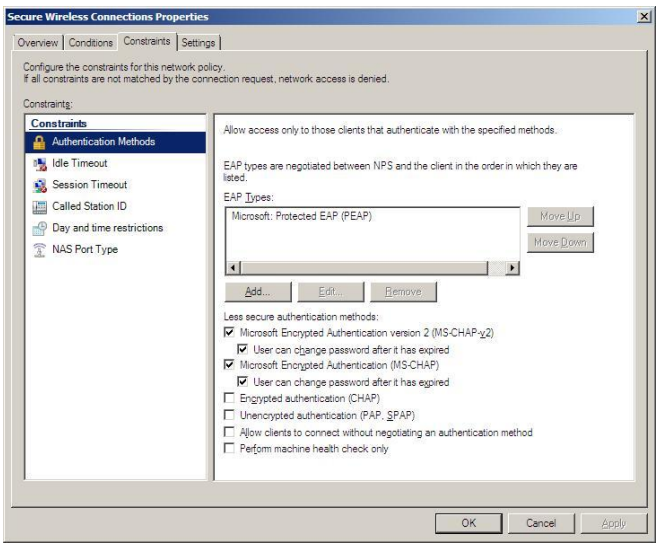
In this example, we're providing secure wireless access for students that are members of the Windows Group **PROCURVE\Students**. Double click on the **Secure Wireless Connections** policy to view/configure the policy properties.



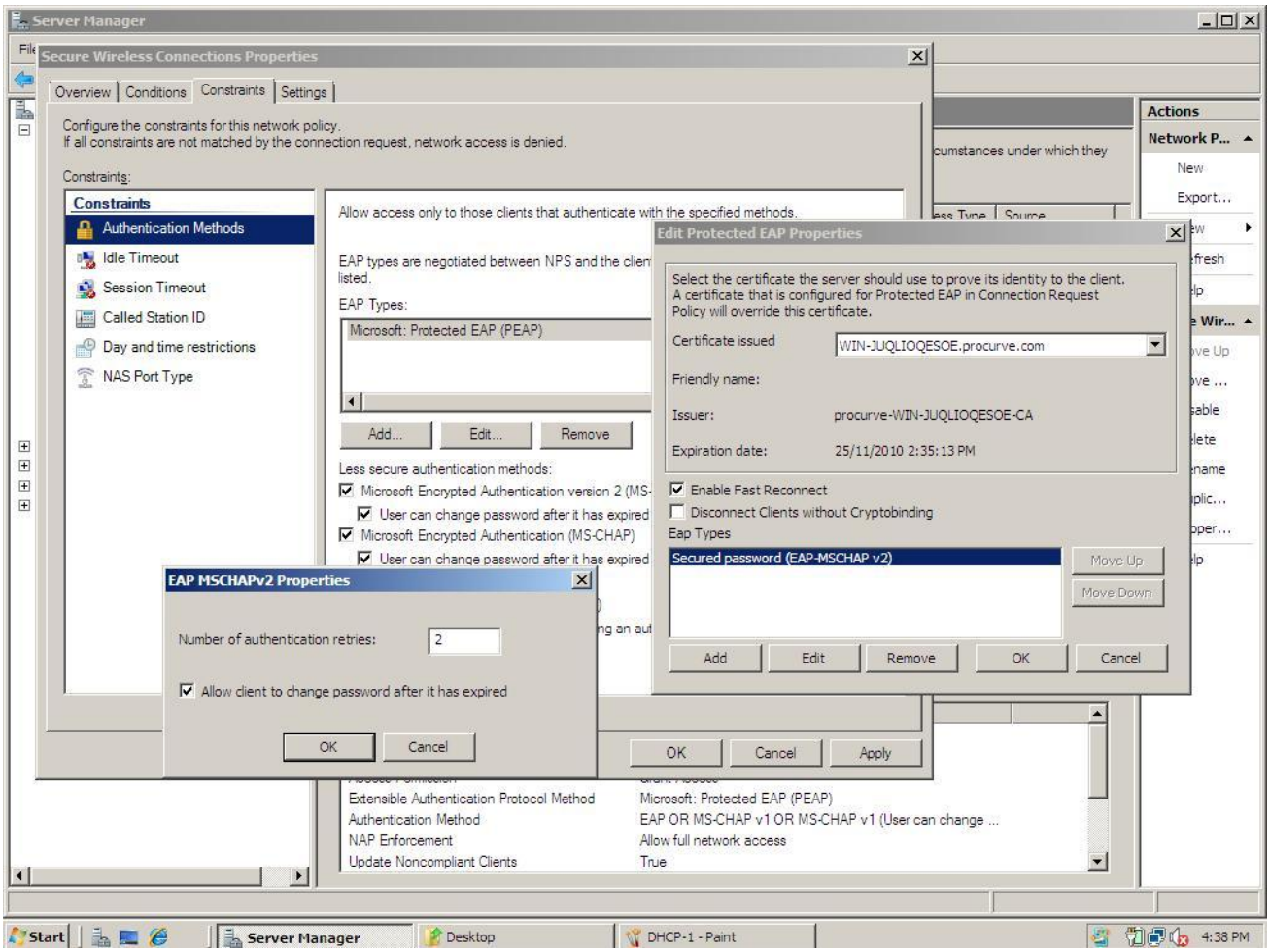
Ensure that the policy is enabled and that access is granted when the connection request matches this policy.

Click on the **Conditions** tab to configure the appropriate Windows Groups and Authentication Methods.



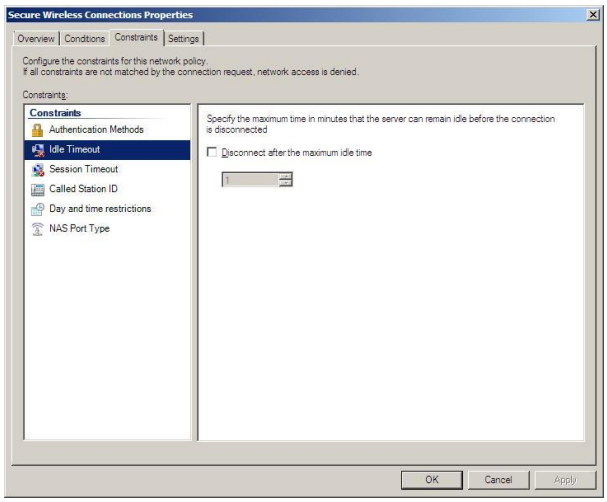


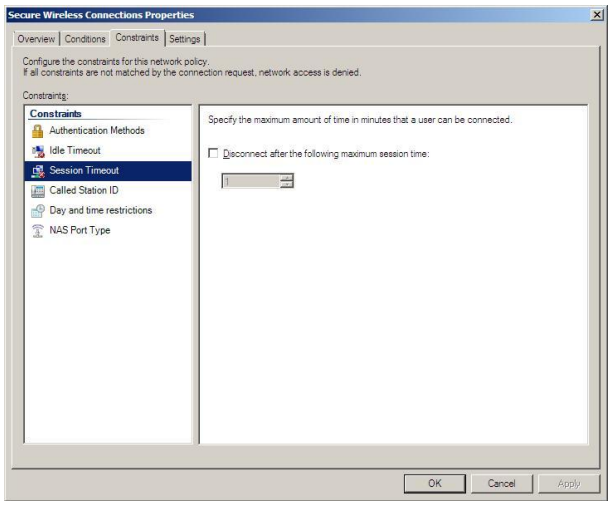
In the above example, students that are members of the Windows Group **PROCURVE\Students** need to authenticate using Microsoft PEAP. Note; you will get an error message if you do not have “Active Directory Certificate Services” already running. Installing Certificate Services at this point will require a reboot of the server.

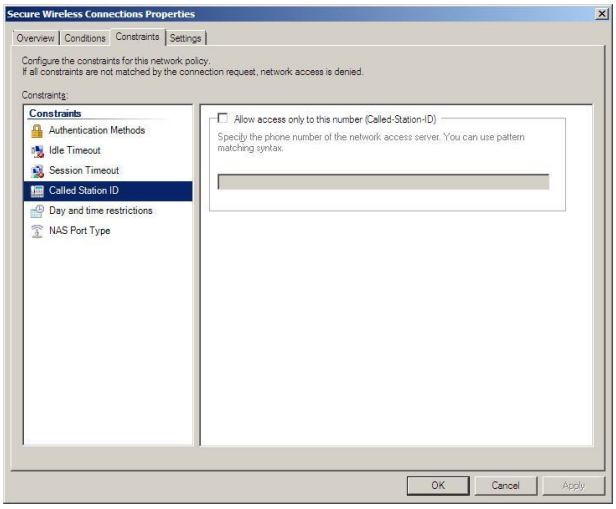


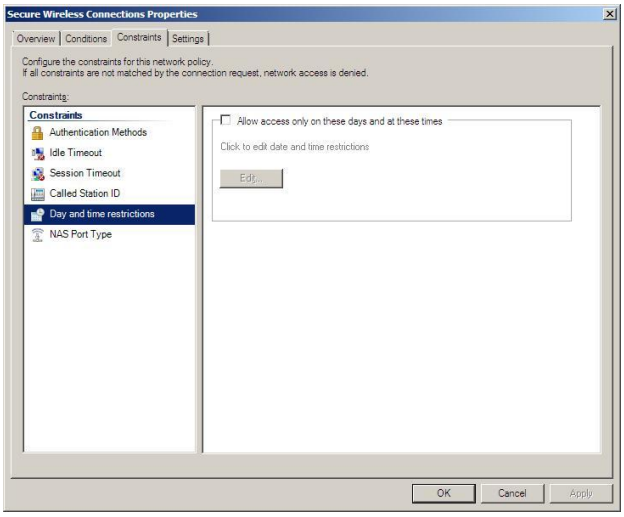
Check that the correct certificate is being used for MS PEAP.

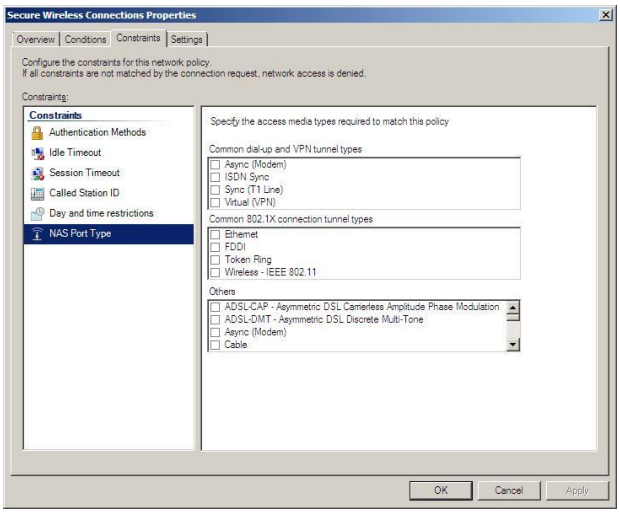
For testing purposes, do not change the following default parameters.











Students should now be able to authenticate via NPS using 802.1X with Microsoft PEAP.

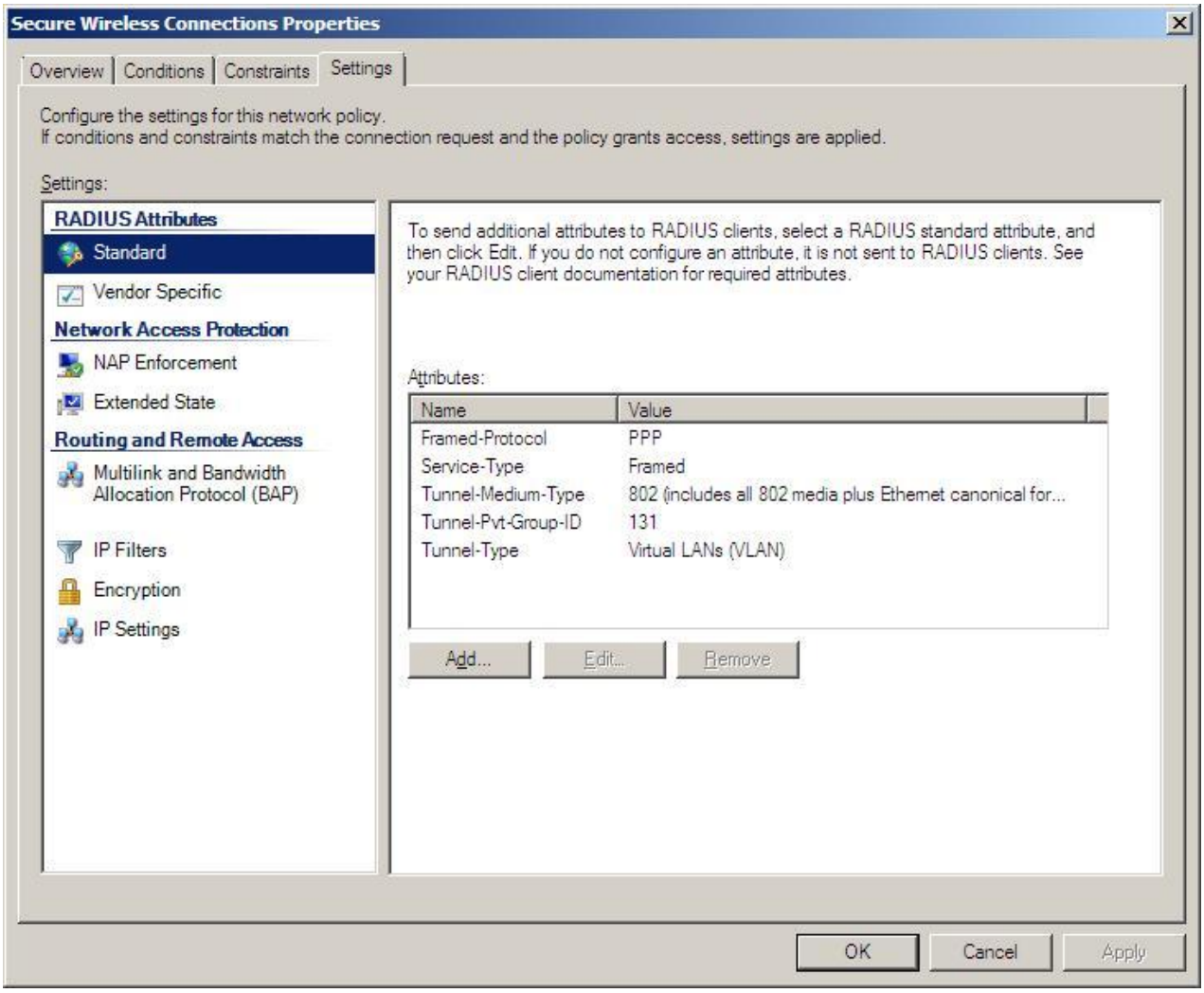
9.3 Dynamic VLANs using NPS

The Student VSC binding on page 22 of this guide lists an Egress VLAN ID of 121. Therefore, students that successfully authenticate will be placed in VLAN 121 and obtain an IP address via DHCP in subnet 10.20.121.x/24.

When using VSC bindings to assign VLAN ID's, a separate VSC is required for each VLAN. While this may be acceptable for small size networks, larger environments would benefit from dynamically assigning the VLAN ID using NPS RADIUS attributes. This allows the use of the same SSID (one VSC) for multiple VLANs.

Important Note: RADIUS assigned VLAN ID's overwrite the Egress VLAN ID specified within the VSC binding!

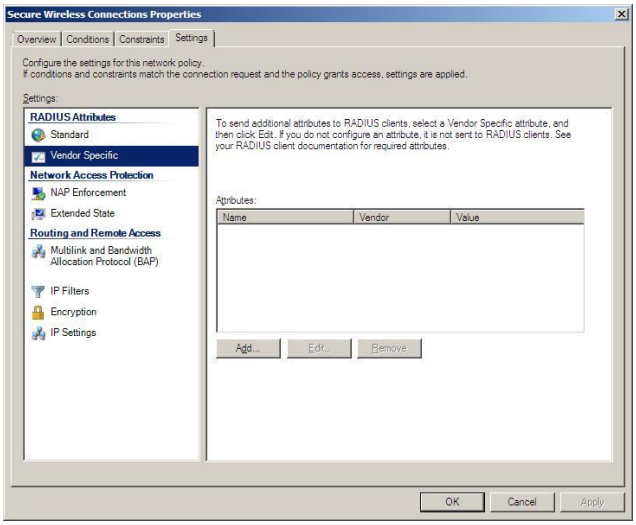
In the following example, authenticated wireless students will be placed in VLAN 131, dynamically assigned by NPS using a RADIUS attribute, overwriting VLAN 121 specified in the VSC Student binding.

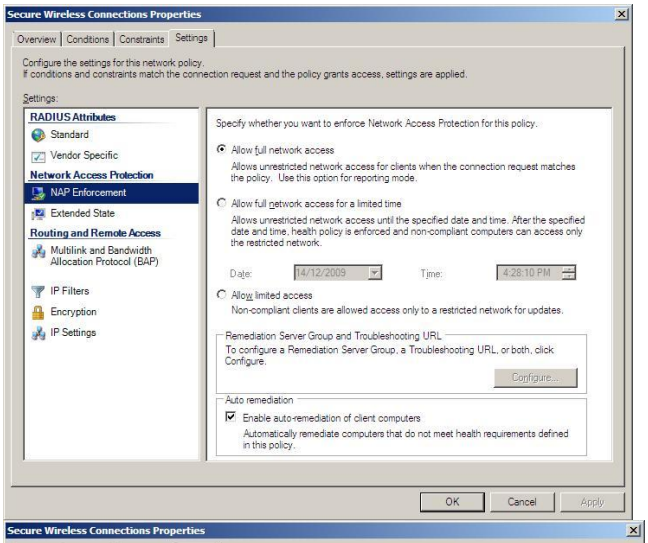


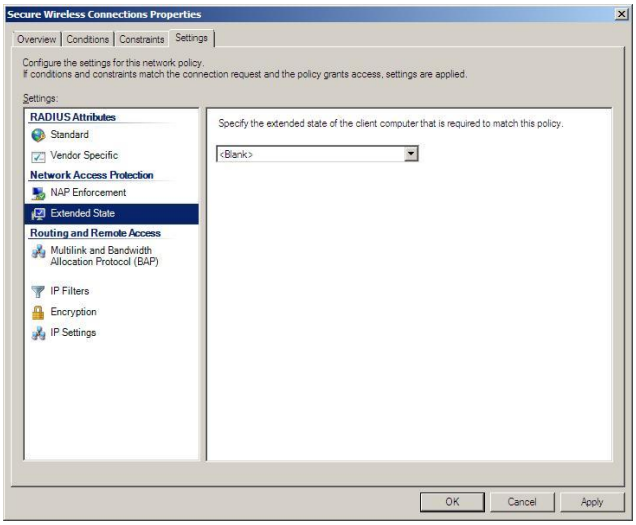
The following three RADIUS Attributes are required for dynamic VLAN assignment via NPS:

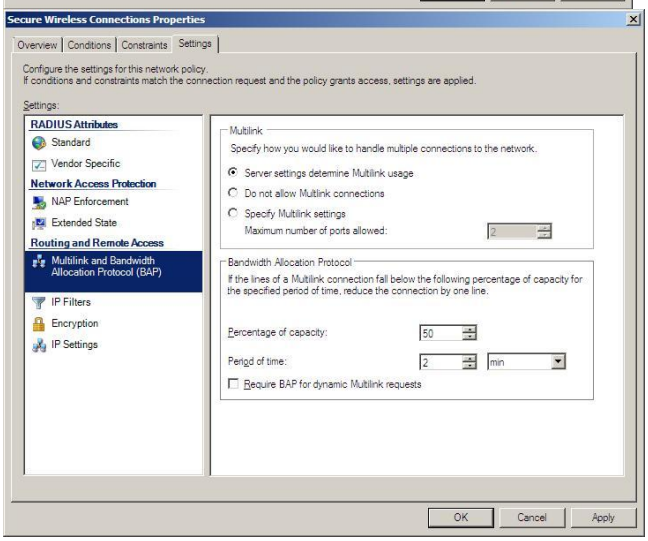
- **Tunnel-Medium-Type**.
- **Tunnel-Pvt-Group-ID**. *This integer represents the VLANID to which group members will be assigned.*
- **Tunnel-Type**. Select Virtual LANs (VLAN).

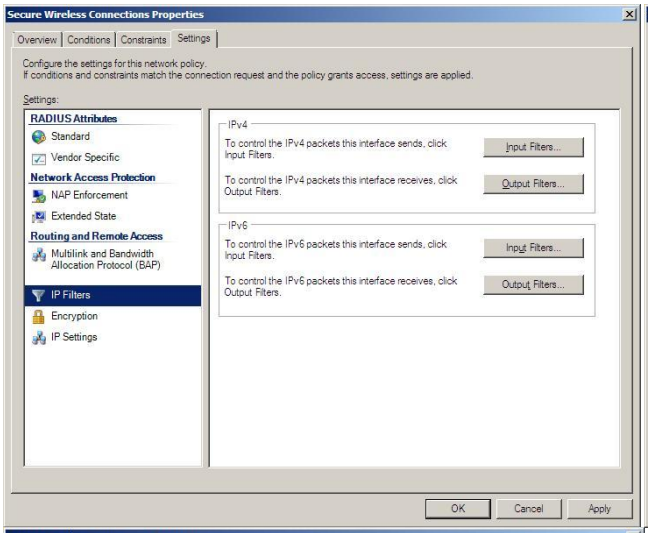
For testing purposes, do not change the following default parameters.

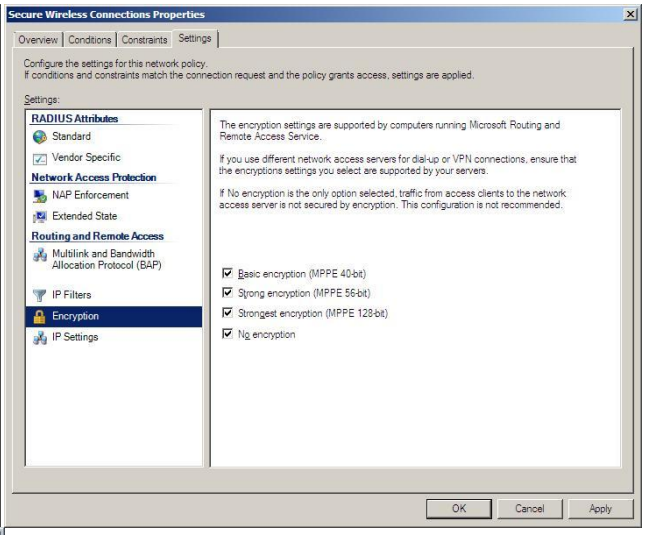


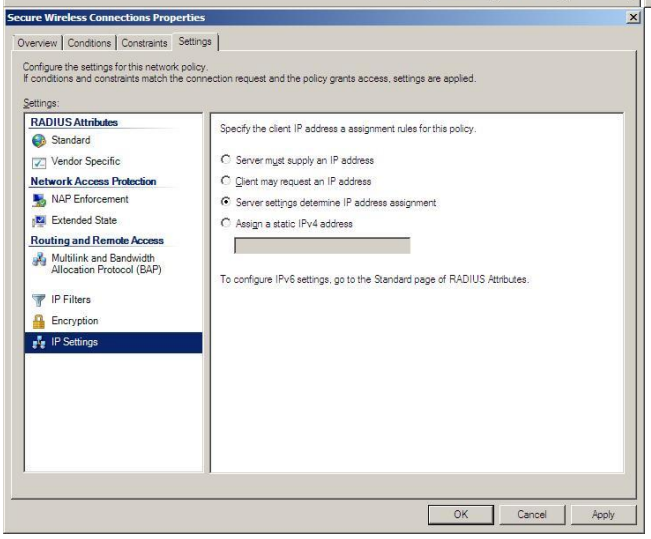






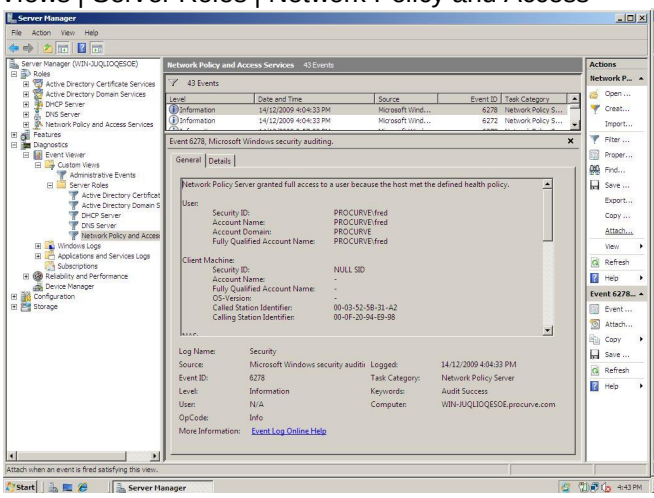


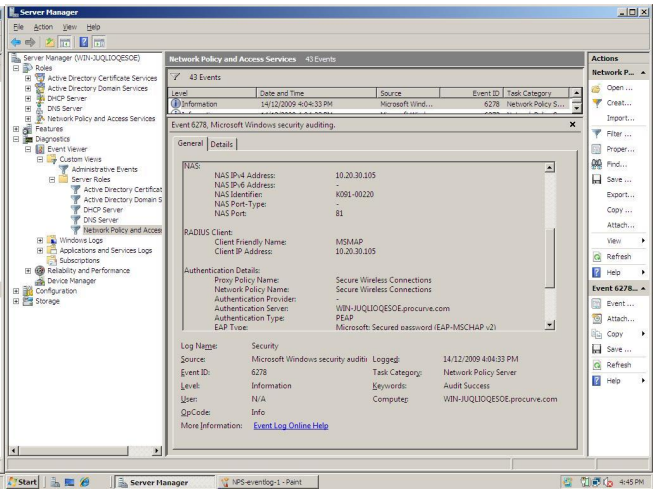




9.4 NPS Logs

To ensure that NPS is operating successfully, you may review the NPS logs under Event Viewer | Custom Views | Server Roles | Network Policy and Access

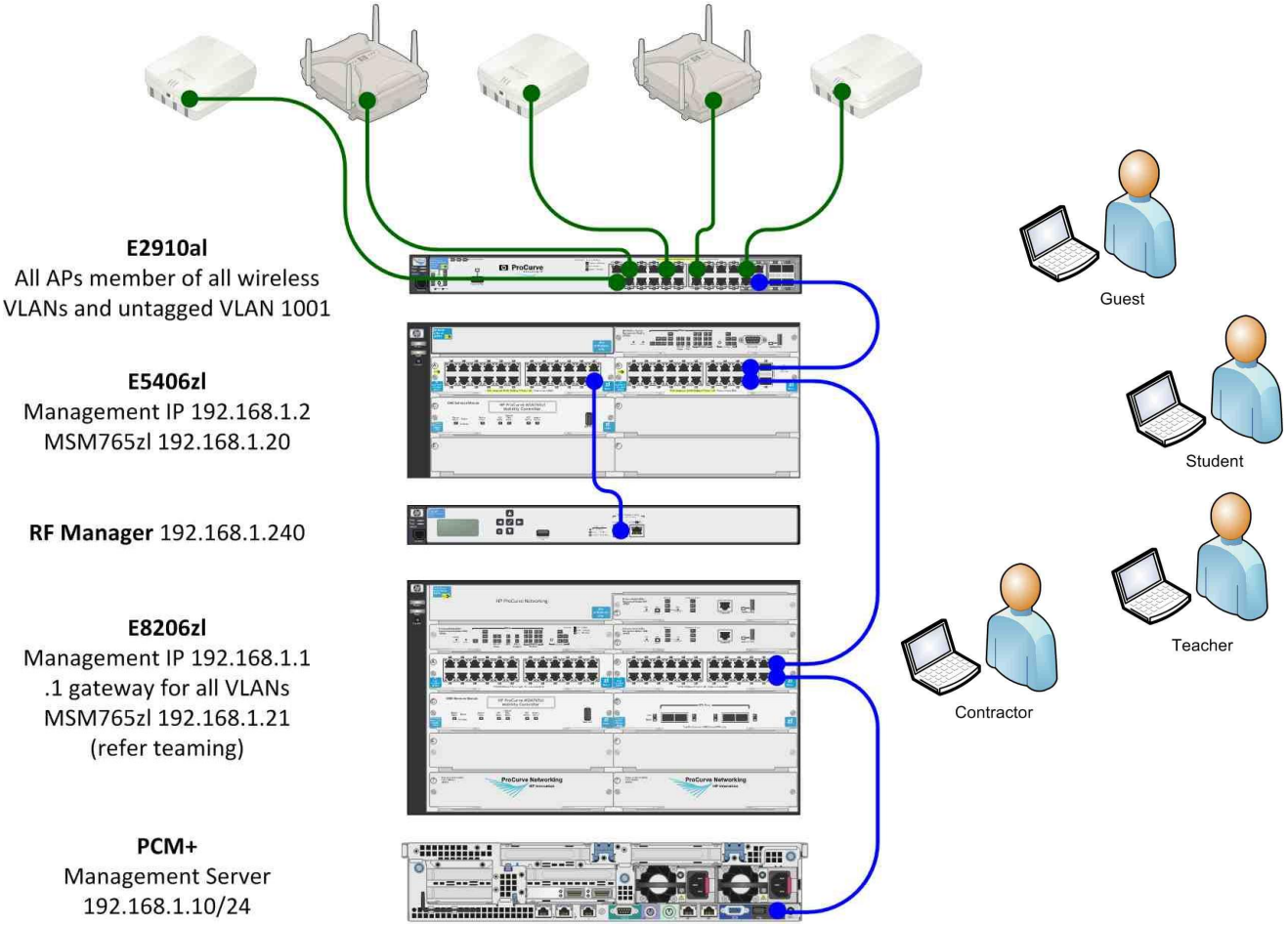




10 Appendix B: Example Contractor Configuration

The contractor configuration has been included as an Appendix as the results from the Authentication process when using AD groups was not as expected.

This configuration simulates a corporate environment whereupon the contractor is considered more trusted than a guest, however not as trusted as an employee as such the corporate infrastructure (AD) will be leveraged to provide authentication whilst the controller will act as the interface between the corporate network and contactor clients. The controller will provide DHCP and DNS services on behalf of the clients.



VLANs:

50 Contractors – 10.20.50.x
110 wired Guest – 10.20.110.x
111 Wireless Guests – 10.20.111.x
120 Wired Students – 10.20.120.x
121 Wireless Students - 10.20.121.x
130 Wired Teachers – 10.20.130.x
131 Wireless Teachers 10.20.131.x
1001 Infrastructure/management 192.168.1.x

10.1 Switch Configuration

A VLAN was added to the switch for the contractors, the only port tagged in the contractors VLAN was the controller's Internet port. The VLAN was given an IP address as the controller will be routing traffic to this interface to facilitate access to corporate resources.

```
vlan 50
 name "contractors"
 ip address 10.20.50.252 255.255.255.0
 tagged C1
 exit
```

In addition the following route was added to enable the return path for corporate traffic pointing to the controller's Internet port.

```
ip route 10.20.5.0 255.255.255.0 10.20.50.200
```

It is important to note that we have assumed access to network resources is controlled by ACLs on the switch. Every site will have their own policies with respect to contractor access, ranging from no restrictions to limited access, again it is up to each site to determine the required restrictions and implement them as per their security policy.

10.2 Controller Configuration

10.2.1 Service Controller Parameters

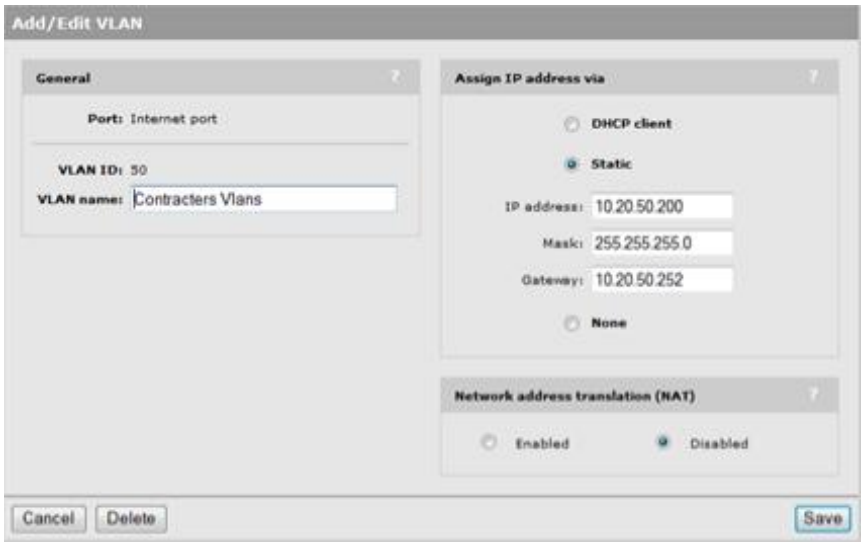
Service Controller | Network | Network Profile

Service Controller | Network | Ports

Assign the previously created Network Profile (VLAN 50) to a VLAN Interface and assign it an IP address within the 10.20.50.x range and point it's default gateway to the VLAN 50 interface on the switch.

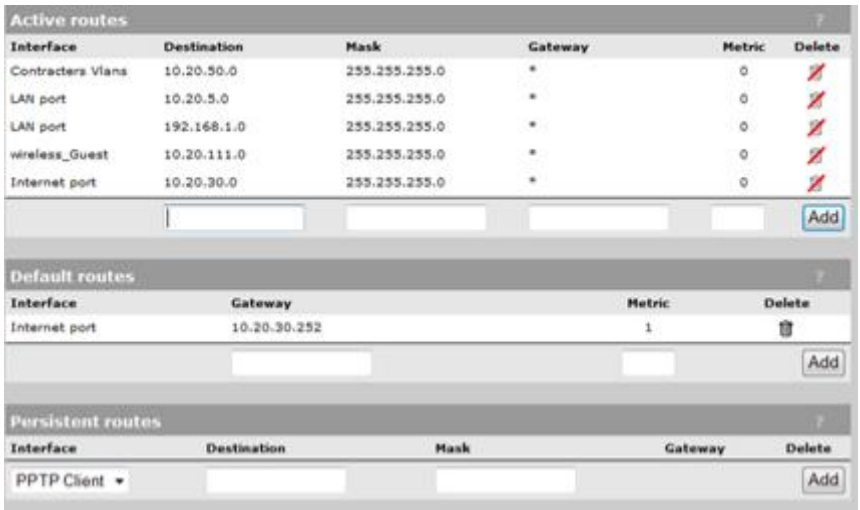
Key point to note:

1. Select Internet Port
2. Ensure NAT is Disabled



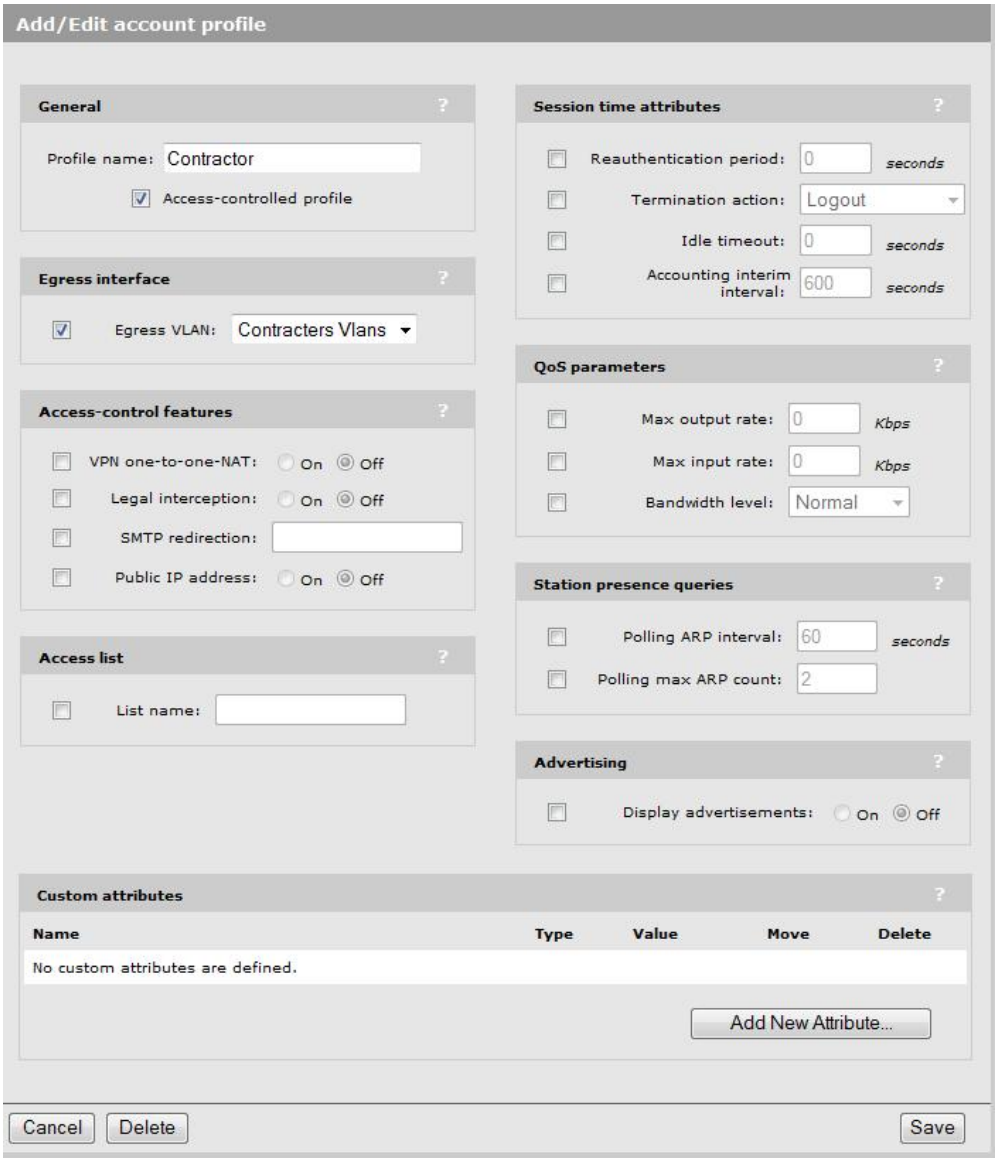
Once the VLAN has been created there will be a route added to the 10.20.50.x VLAN to the controllers routing table.

Network | IP Routes



Service Controller | Users | Account Profile

To ensure controller traffic is placed into VLAN 50, an account profile is created. This profile will then be assigned to the Active Directory Group attributes (to be defined later). The only changes required on this page for this example configuration are – check “Egress VLAN” and select “Contractors VLAN” from the drop down box.



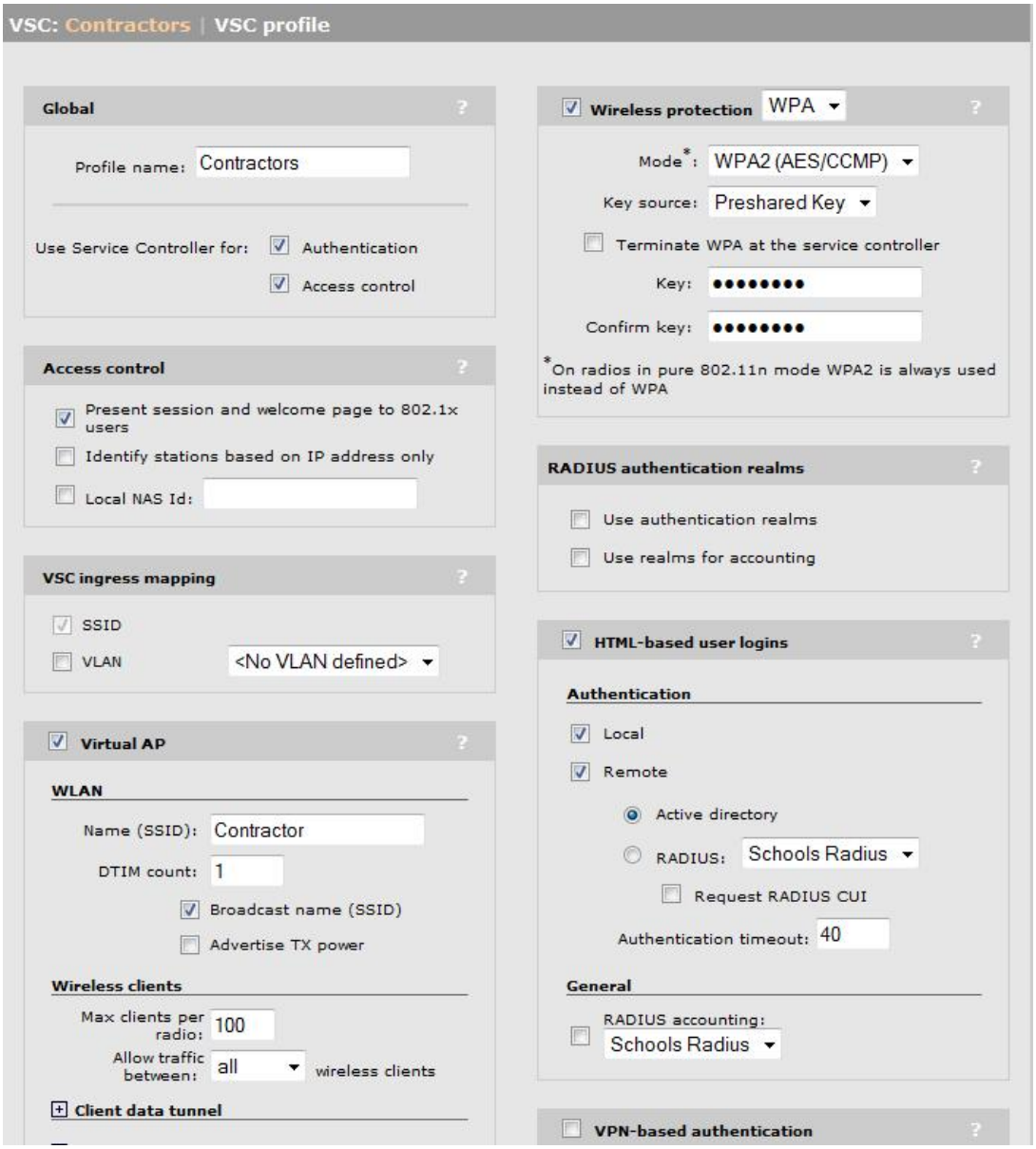
10.2.2 Contractors VSC

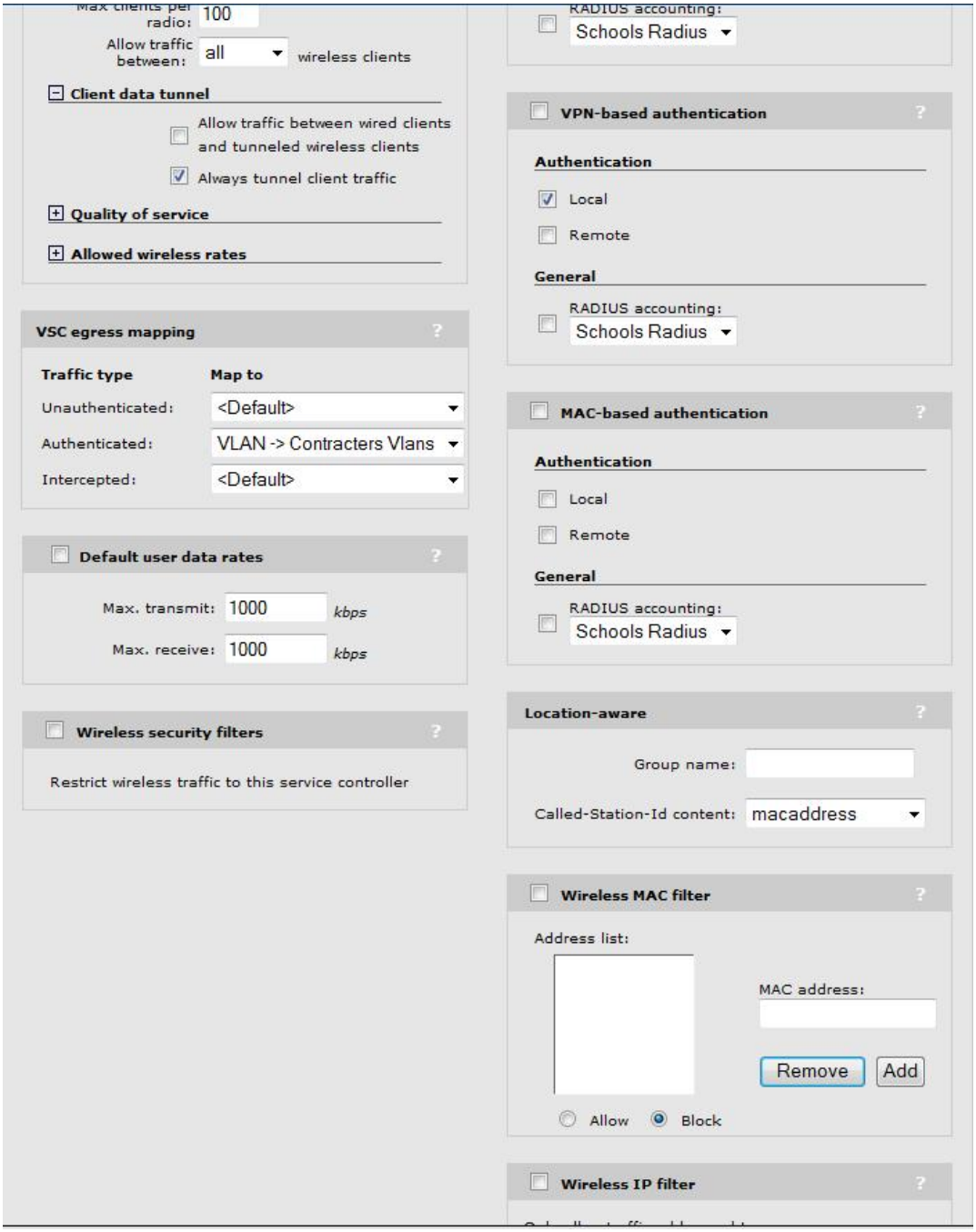
The Contractor VSC is leveraging the controller for both authentication and access control.

Data is encrypted using WAP2 with pre-shared keys, HTML logins are checked to enforce authentication prior to accessing the wireless network.

Some key points to note regarding on the screen shot below are

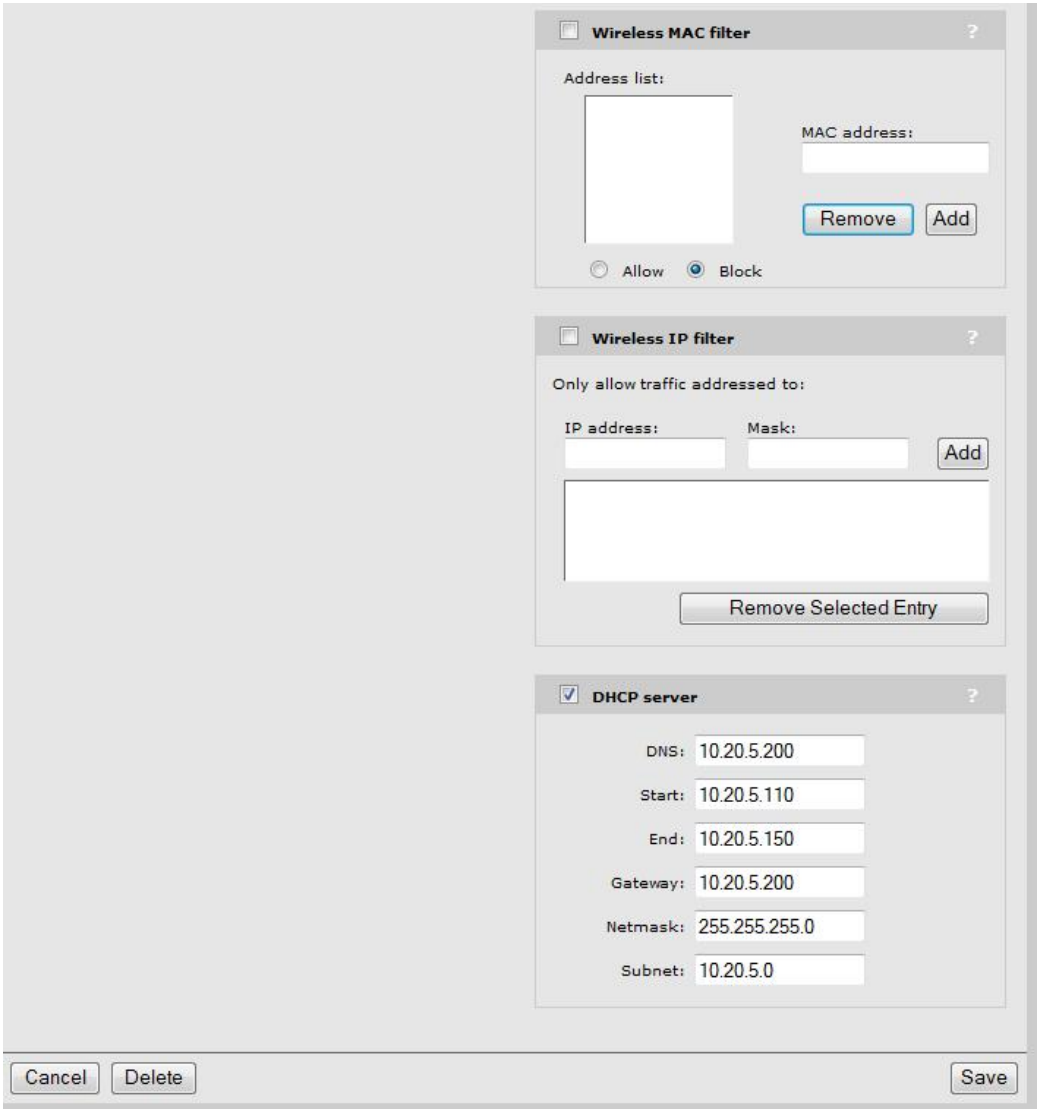
1. Both local and remote authentication has been checked along with Active Directory. Checking Active Directory forces the controller to proxy authentication requests to AD, if the account exists and correct credentials are entered the user will receive a “successful login” message.
2. Checking “local” under authentication forces the controller to provide and IP address to the client.
3. Checking “remote” forces the controller to establish a connection with the AD server.





Key points to note on this screen are:

1. Ensure "Always Tunnel Client Traffic" is checked. Checking this feature forces the controller to establish a tunnel between traffic from the AP and the Internet port thus hiding the contractor traffic from the corporate network.
2. Uncheck Wireless security filters
3. Uncheck WMM



Key points to note on screen shot above are:

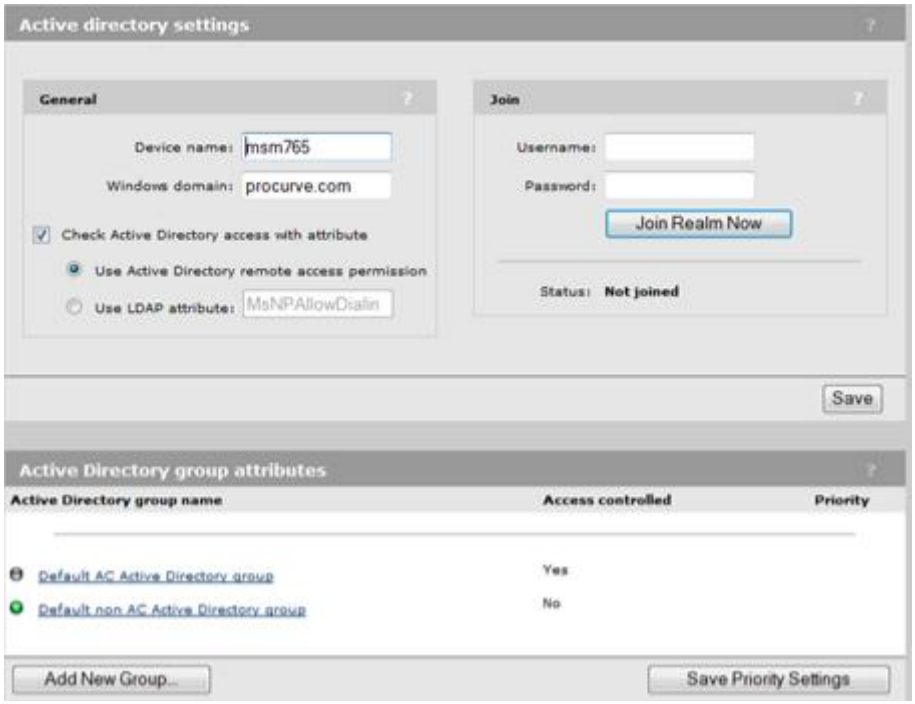
1. The 10.20.5.x subnet does not exist anywhere on the corporate network
2. The DNS and Gateway addresses MUST be the same, this forces the controller to reference its DNS setting (refer page x)
3. The DNS server 10.20.5.200 does not exist

10.2.3 Active Directory Configuration

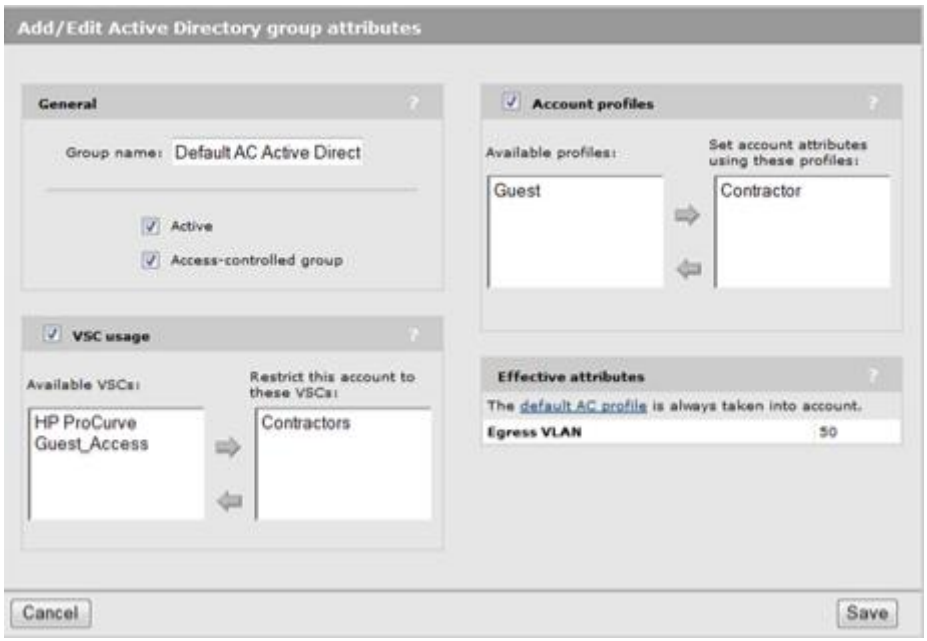
Service Controller | Authentication | Active Directory

We will leverage what has been setup in teacher's VSC and extend it to contractors. As a recap the following has already been completed

1. The Controller has successfully joined the domain and the status is joined (ignore status below) using the Administrator password with a device name of MSM765
2. The Non AC Active Directory Group is currently active for teachers we are now going to configure and active the Default AC Active Directory Group

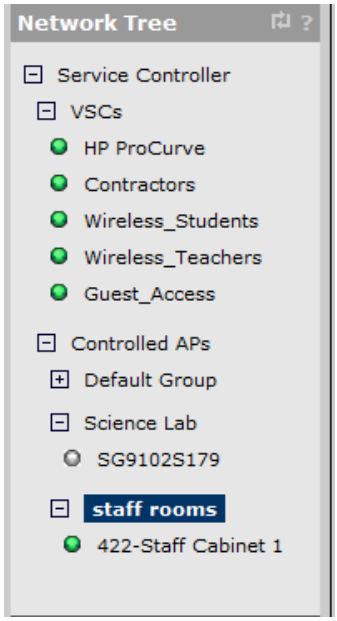


Within the group attributes we are restricting usage to the Contractors VSC and are using the Contractor Account profile to ensure traffic egresses onto VLAN 50.



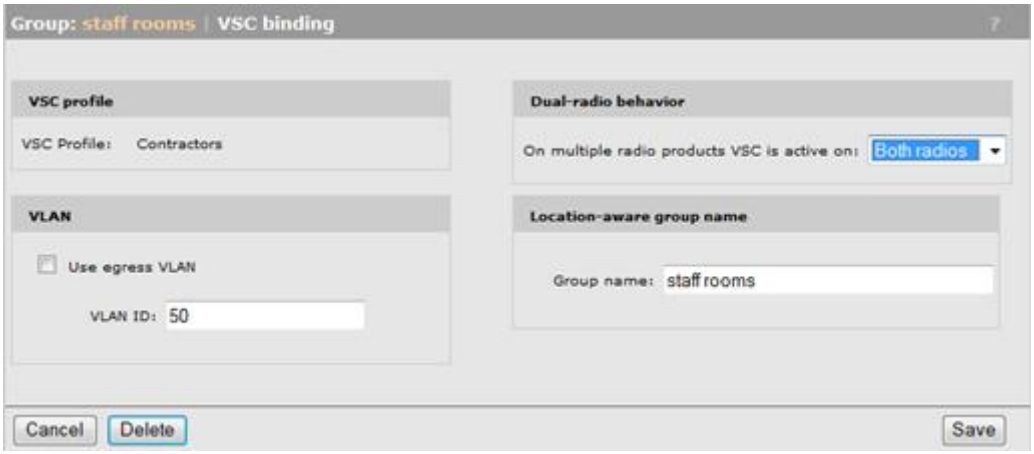
10.2.4 VSC Binding

The last step before synchronising the MSMAPs is to bind the VSC to the appropriate MSM AP Groups



Select the appropriate Group that will advertise the Contractor SSID. In this case we will activate the Contractor VSC on all Access points in the “Staff Room” location

VSC bindings | VSC Binding



Remember to Synchronise the APs

11 Appendix C: Voice over WLAN Configuration

To carry voice across a WLAN requires careful planning and complete understand of the WiFi devices capabilities. Unlike TCP traffic which can tolerate lost/delayed packet, telephony traffic does not therefore careful site planning and RF management is required. HPN recommend site surveys are conducted to ensure complete signal coverage and strength.

In addition the telephony traffic being delay sensitive must be prioritised over any existing data traffic and where possible egress onto the network from the AP. The QoS policies configured within the VSC must align with the network infrastructure to ensure appropriate end-to –end prioritisation.

The following example provides a guide how to configure a Voice over WLAN VSC, the variables shown are examples only and must be reviewed/customised for each Voice over WLAN deployment

11.1 Network Profile

Define a profile for the voice VLAN (VLAN 200).

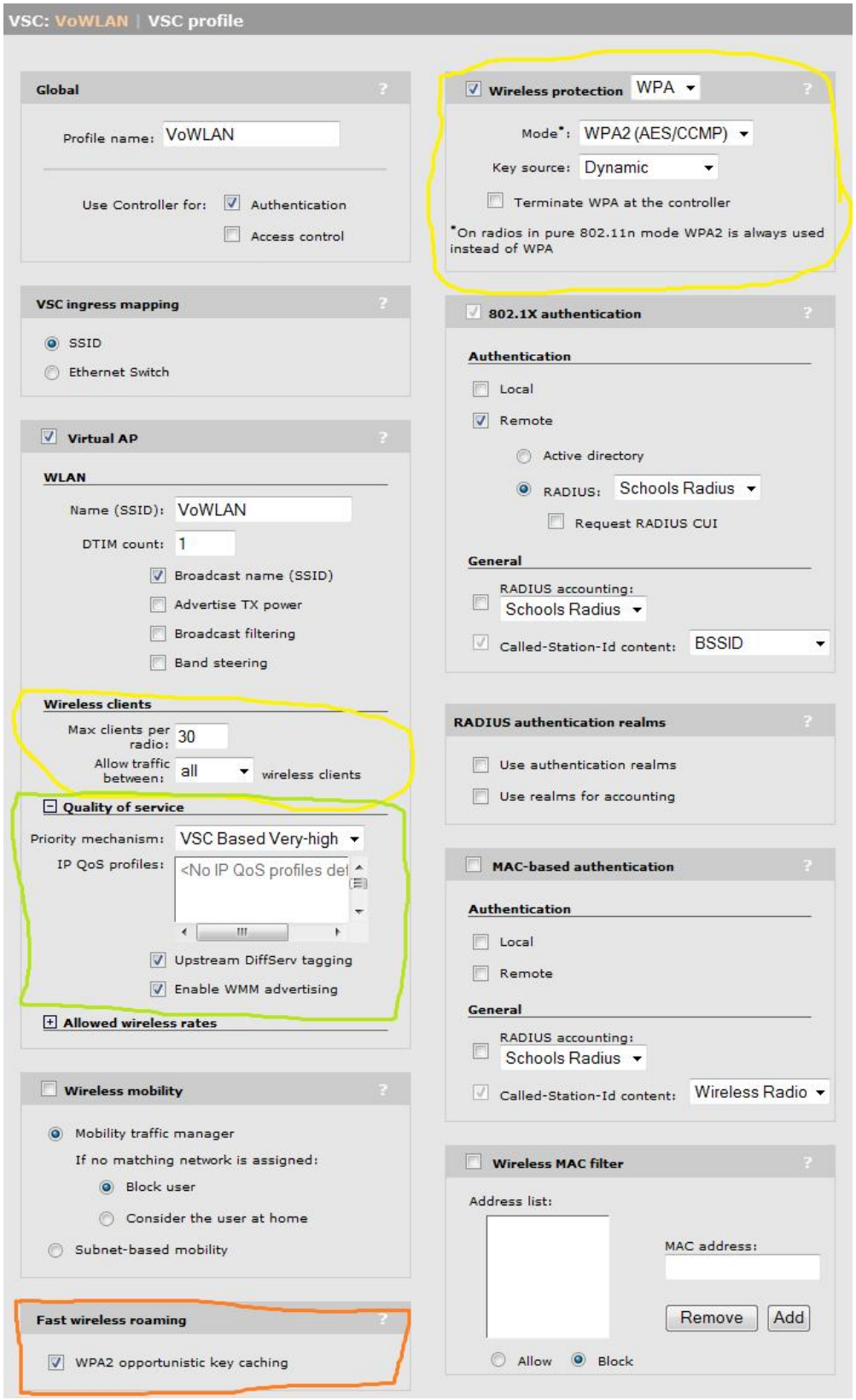
Service Controller | Network | Network Profiles

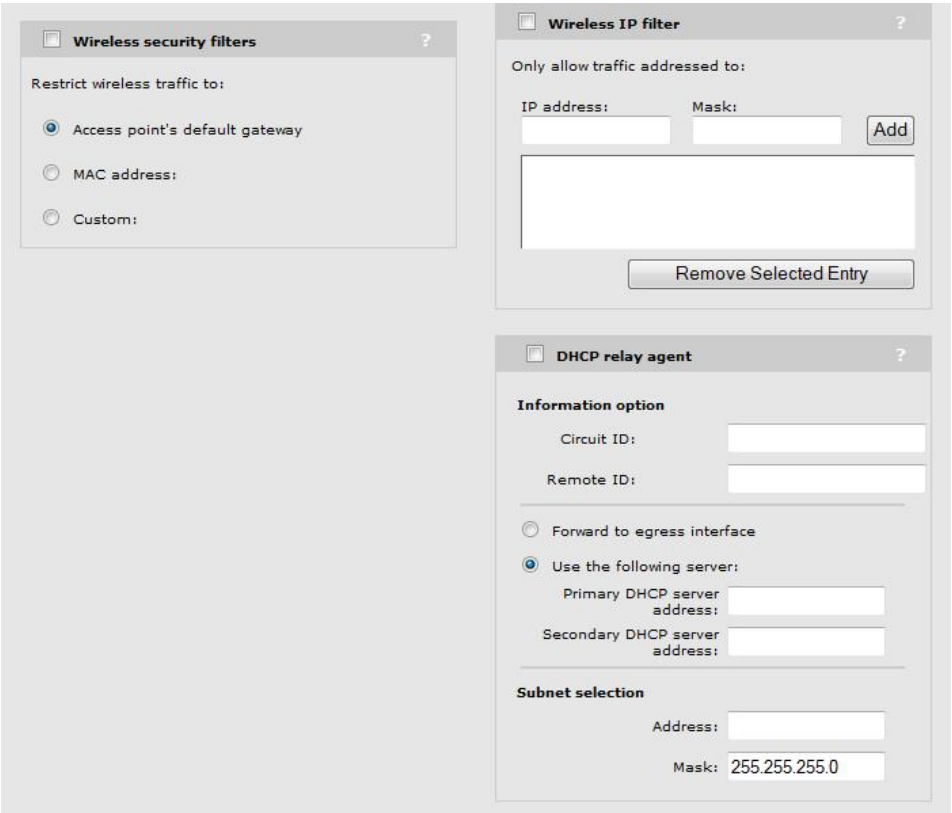
11.2 VoWLAN VSC Configuration

In the example VoWLAN VSC configured below the "Wireless Protection" area has been highlighted, this needs to be configured to meet the security requirements that all WiFi phones connecting to the network will support. Other key points to note:

1. Allow traffic between devices is checked.
2. QoS has been set to "VSC Based Very High" this ensures any traffic destined for an assoicate4d wireless client belonging to this VSC will have priority over traffic associated with other VSCs residing on the same radio. It is recommended only 1 "VSC Based Very-High be configured per radio.
3. When 802.1x/WPA2 is selected as the "Wireless Protection" WPA2 key caching should be selected to allow the WiFi phones to bypass a full 802.1x authentication when roaming between APs.

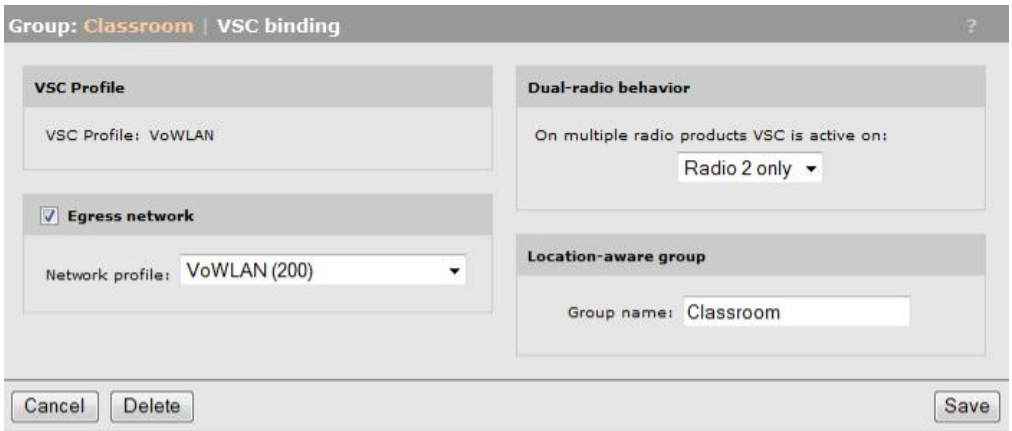
VSC | Add New VSC Profile





11.3 VSC Binding

In this example to cater for b/g capable WiFi phone the VoWLAN VSC has been bound to radio 2. If the fleet of WiFi phones are N capable the VSC should be bound to an “N” capable radio



12 Appendix D: Access Control

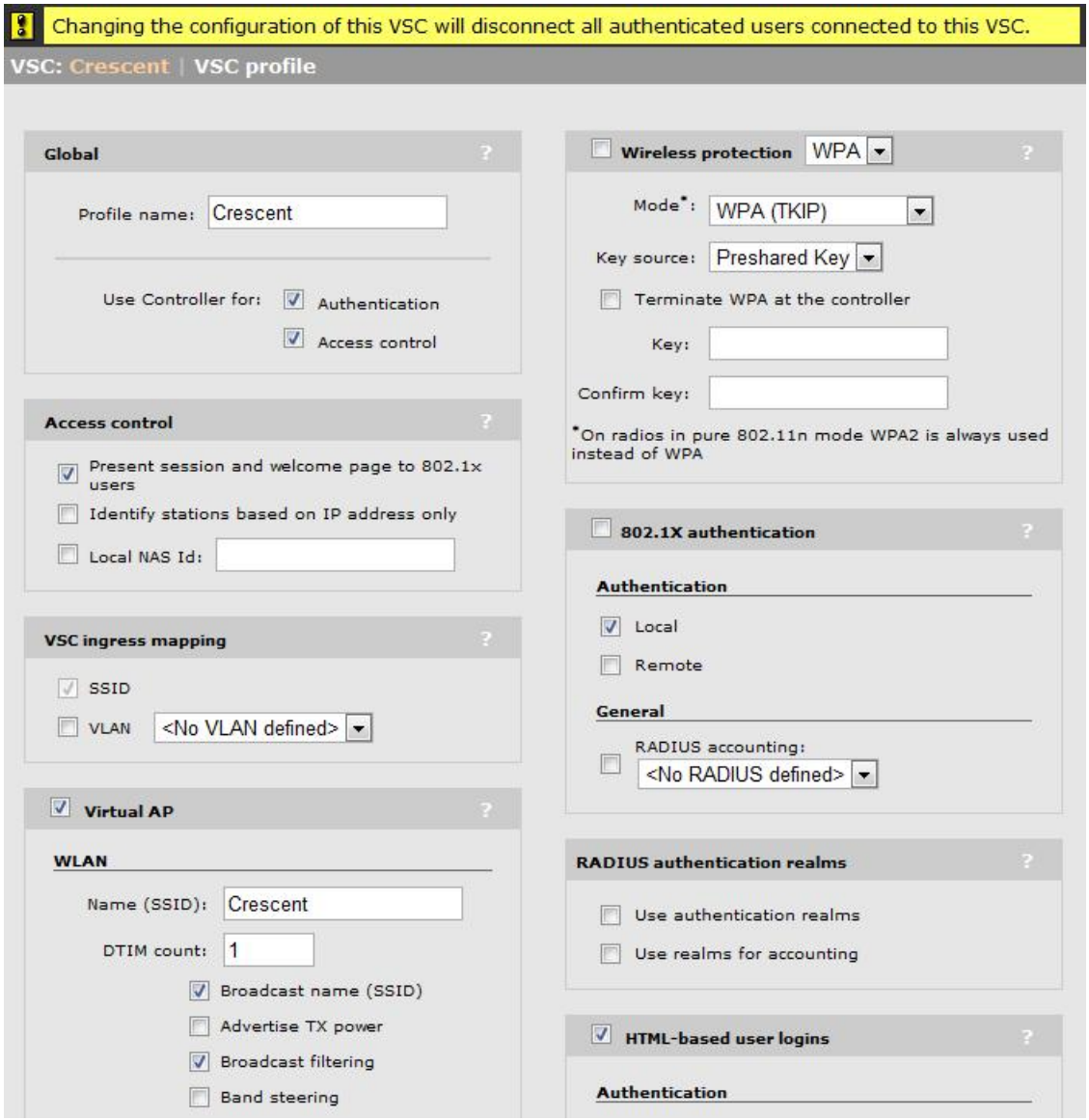
This Section explores the attribute (ACL) function within Access Control. The examples used in this Section came from a slightly different environment to that used in the rest of the document, so some of the addressing and conventions may differ slightly.

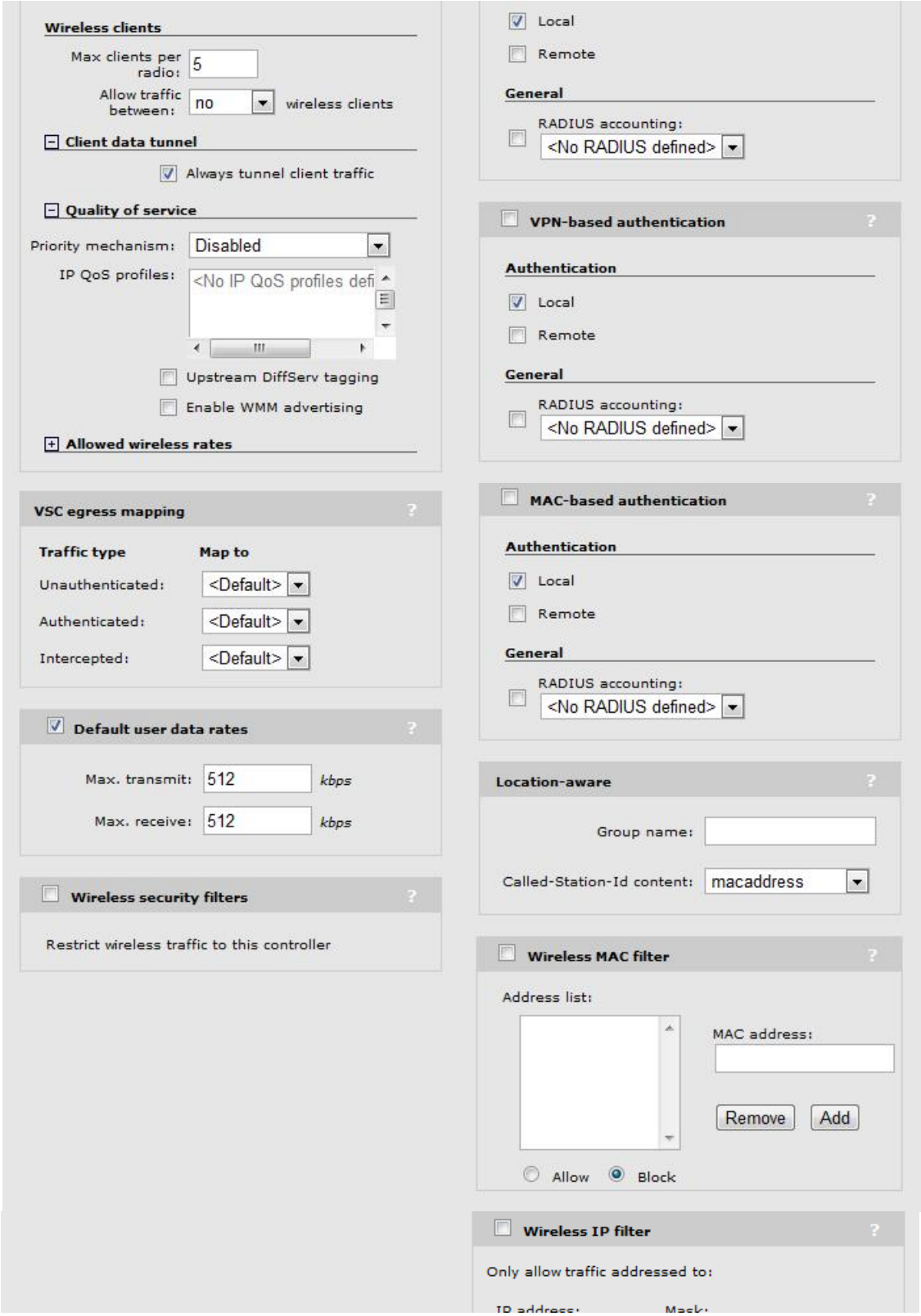
12.1 VSC Preparation

12.1.1 Create VSC

Controller | VSCs | Crescent

This is an access-controlled VSC – all traffic is processed by the controller, along with authentication.

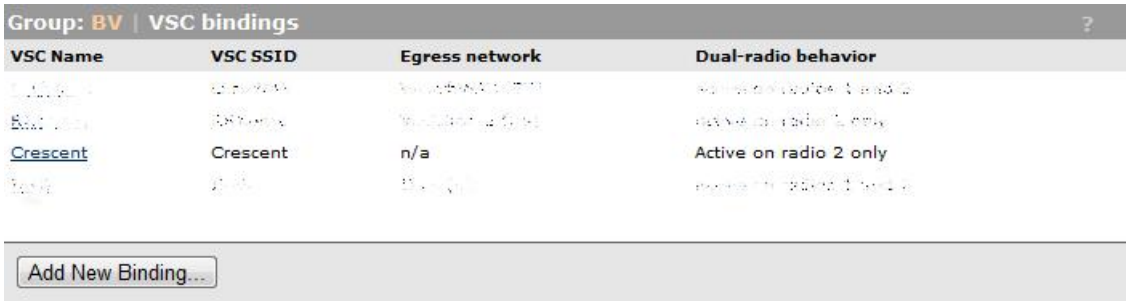




12.1.2 Binding

Bind the VSC to the relevant group(s). In this case, the Crescent VSC is bound to the BV group with no egress VLAN defined (all traffic goes via the tunnel to the controller).

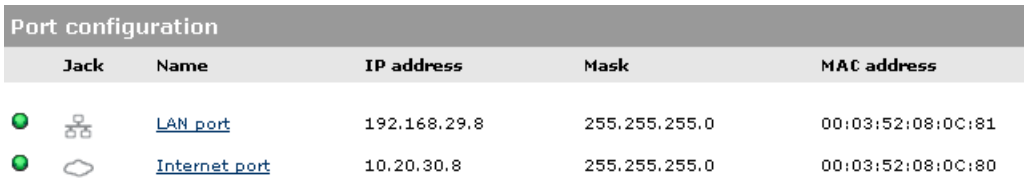
Controlled APs, VSC Bindings



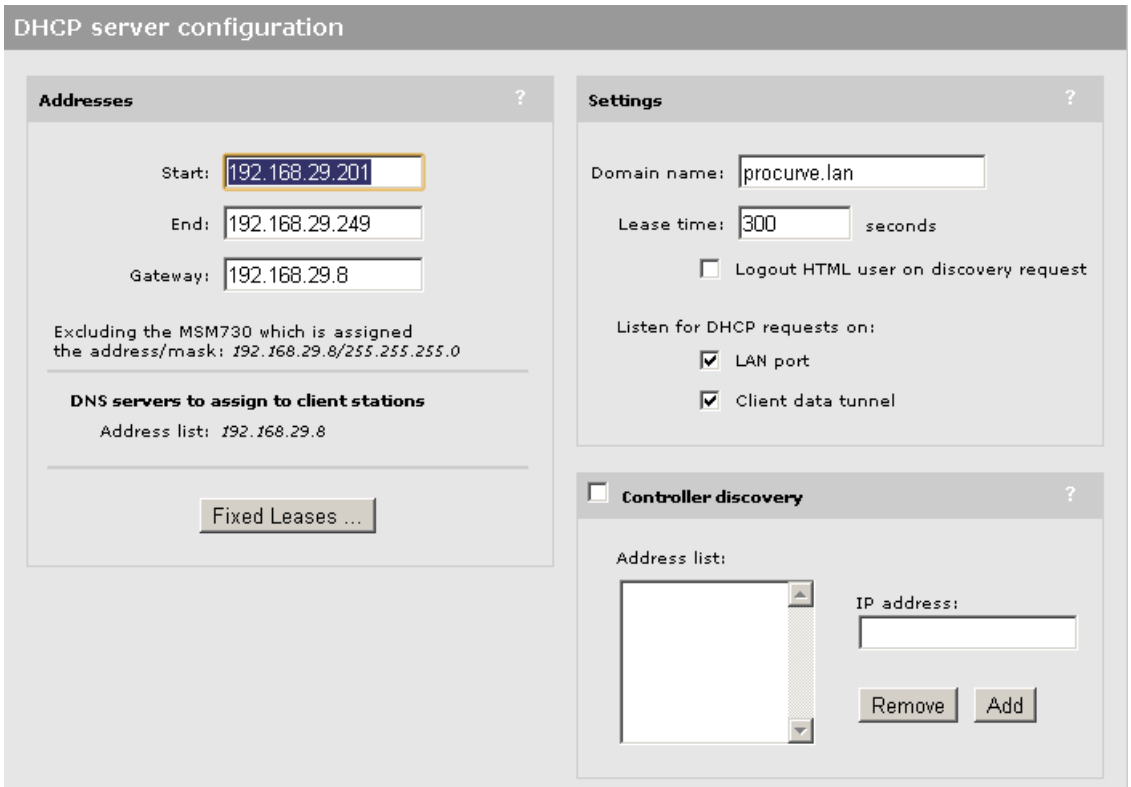
12.1.3 Network and DHCP

The network configuration is shown because it relates to the DHCP configuration. Note the LAN port IP address of 192.168.29.8/24. This is gateway address used in the following DHCP configuration.

Network | Ports



Network | Address Allocation

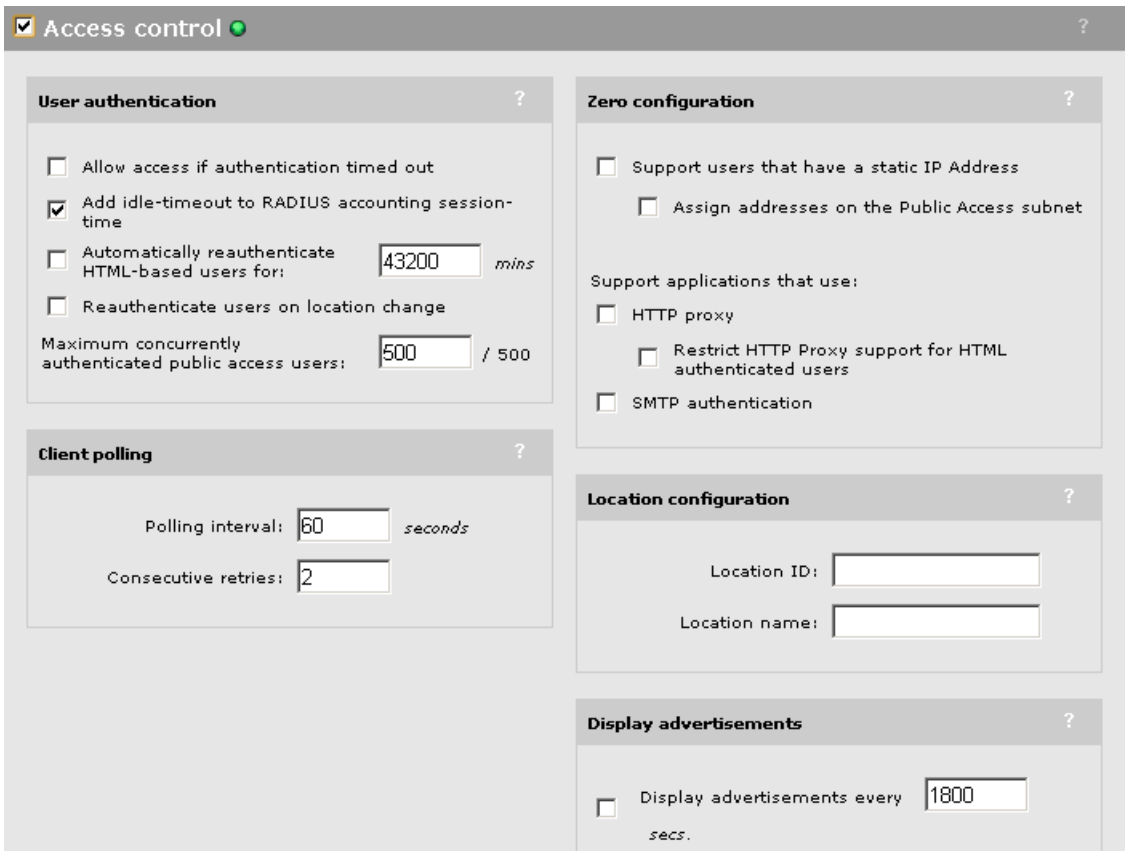


12.2 Access Preparation

12.2.1 Access Control

Public Access | Access Control

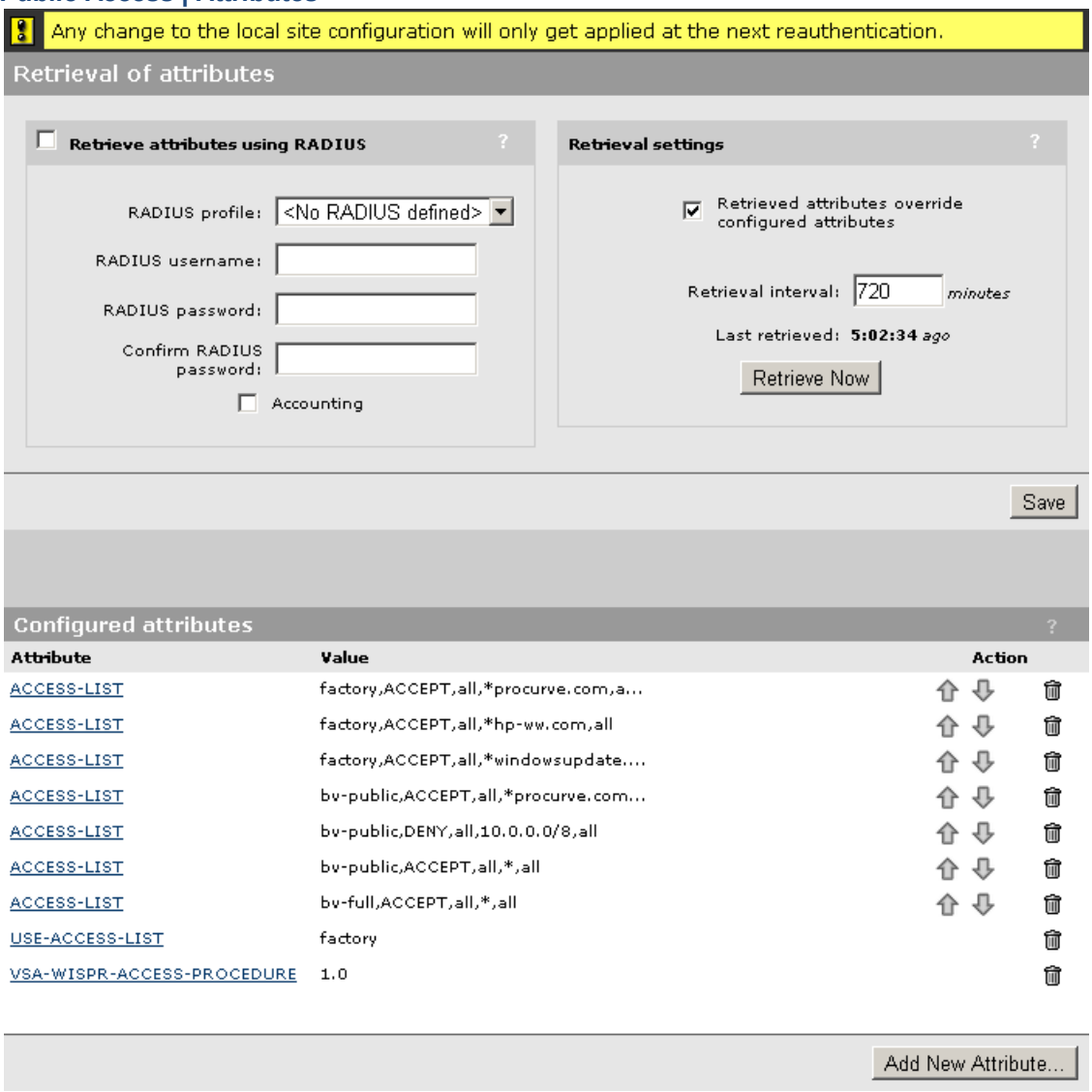
Tick the Access control check-box.



12.2.2 Attributes

Add additional attributes (in this example “bv-public” and bv-full”) are added. This is where the ACL components are configured.

Public Access | Attributes



Precedence is important, so the lines

- `bv-public,DENY,all,10.0.0.0/8,all` blocks access to the entire 10 network, followed by
- `bv-public,ACCEPT,all,*,all` which allows access to remaining networks.

13 Appendix E: Teaming

13.1 Overview

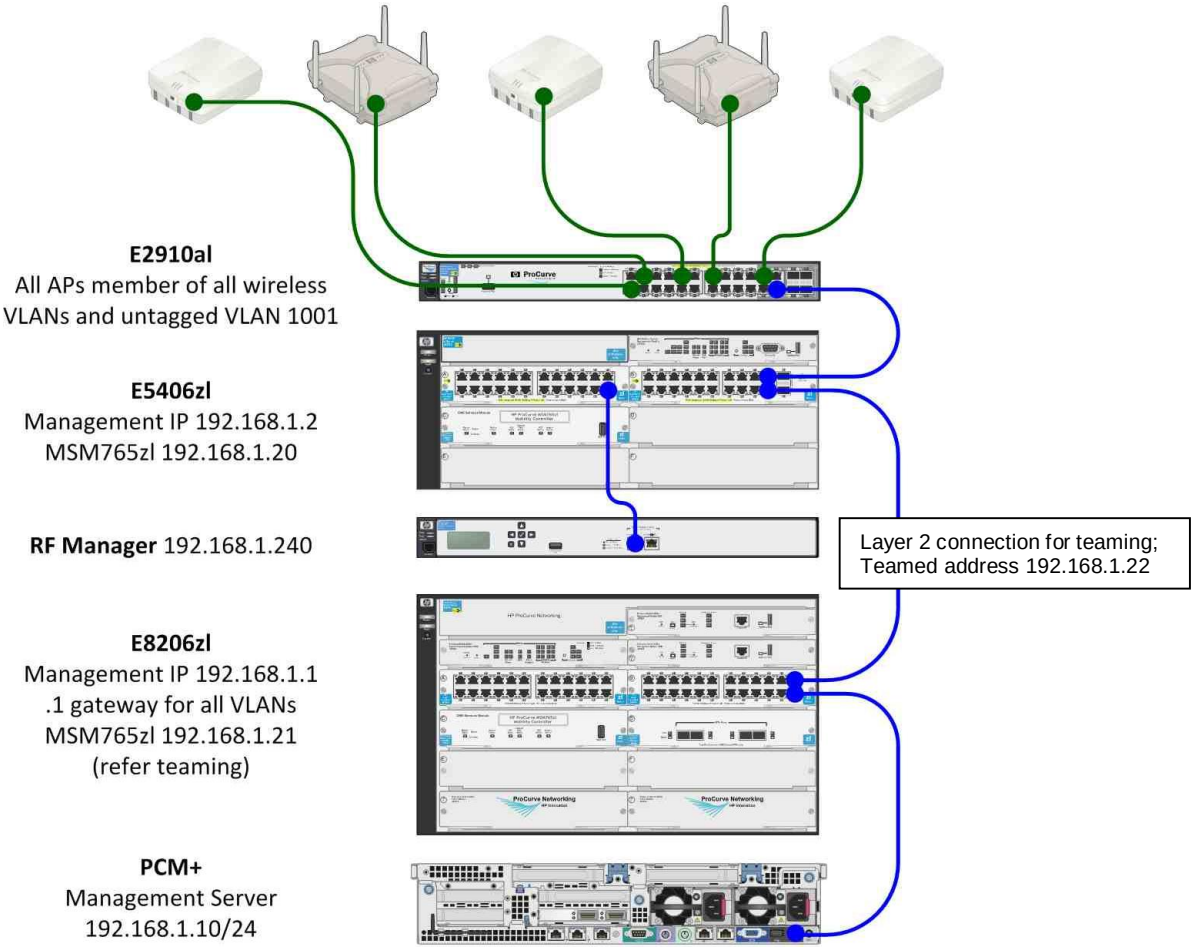
Controller teaming simplifies the configuration and monitoring of multiple controllers and their access points, providing the following key benefits: centralized management and monitoring, service scalability and redundancy in case of controller failure.

Up to five controllers can be combined into a team enabling support for up to 800 APs (four controllers x 200 APs per controller plus one additional controller for backup/redundancy).

13.1.1 Equipment Details

Controller/AP	MAC Address/IP Address	Firmware Details
765zl Controller	Internet Port IP:192.168.1.20 LAN port	5.5.0.0
765zl Controller	Internet Port IP:192.168.1.21 LAN Port	5.5.0.0
MSM422 Radio	Radio 1:00-03-52-b3-dd-70 Radio 2: 00-03-52-b3-dd-70 IP:10.20.30.105	As the APs were configured for controlled mode they received their firmware from the controller, hence the firmware revision was the same as the controller.
MSM410 Radio	IP: 10.20.30.101	As the APs were configured for controlled mode they received their firmware from the controller, hence the firmware revision was the same as the controller.

13.1.2 Teamed Controller Network Diagram



VLANs:
50 Contractors – 10.20.50.x
110 wired Guest – 10.20.110.x
111 Wireless Guests – 10.20.111.x
120 Wired Students – 10.20.120.x
121 Wireless Students - 10.20.121.x
130 Wired Teachers – 10.20.130.x
131 Wireless Teachers 10.20.131.x
1001 Infrastructure/management 192.168.1.x
1100 Guest Roaming –192.168.20.x

13.2 Configuring the Team

13.2.1– Resetting the Member controllers

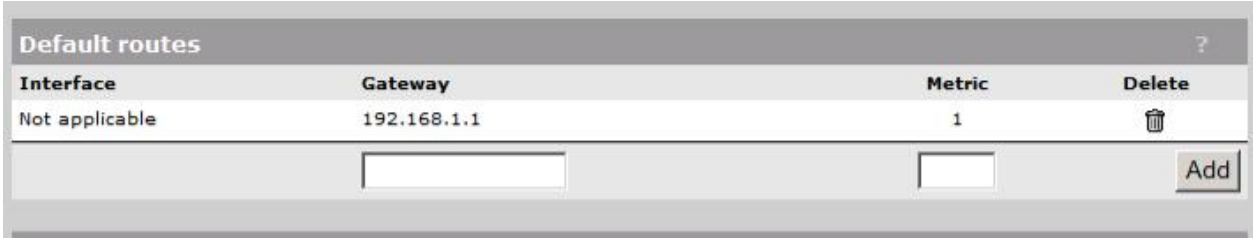
1. Backup the configuration from **ALL** controller **Maintenance | Configuration** , select “Backup and Save
2. Factory reset the **MEMBER** Controllers only. To reset the member controller go to **Maintenance | Configuration** and click Reset. This will cause the controller to default to factory settings

13.2.2– Team Manager IP Address Assignment

Ensure the Internet port and LAN port reside in separate networks, in our example we have assigned the 192.168.1.x address to the Internet port and 192.168.20.x to the LAN Port. Ensure the Internet Port is an untagged member of the management/infrastructure VLAN, in our example we are using VLAN 1001. The LAN port can either be disabled or place into a NULL Vlan (it will be configured later).

Configure the default gateway for the Internet Port, in this example we are using 192.168.1.1, the IP address assigned to VLAN 1001

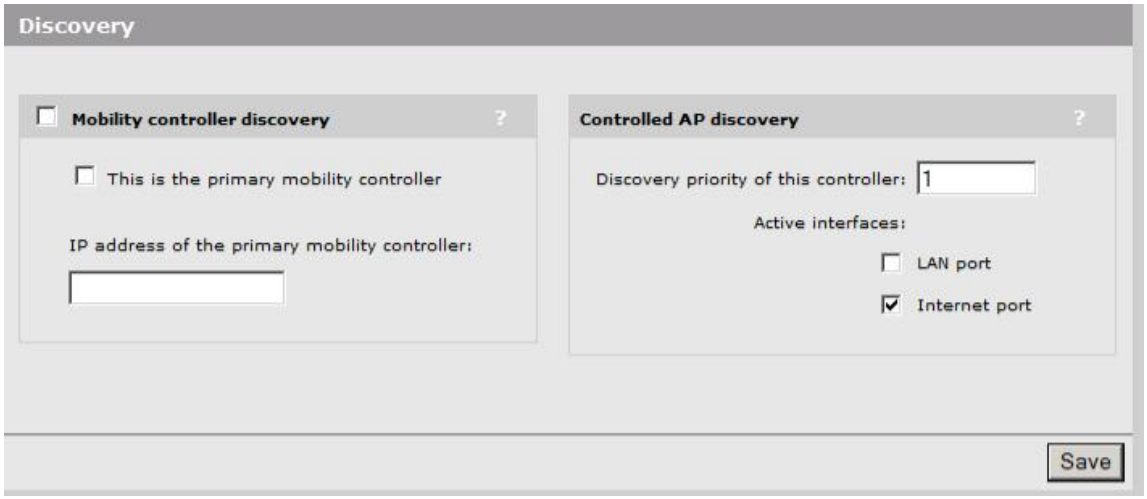
Network | IP Route



13.2.3 – Device Discovery

Management | Device Discovery

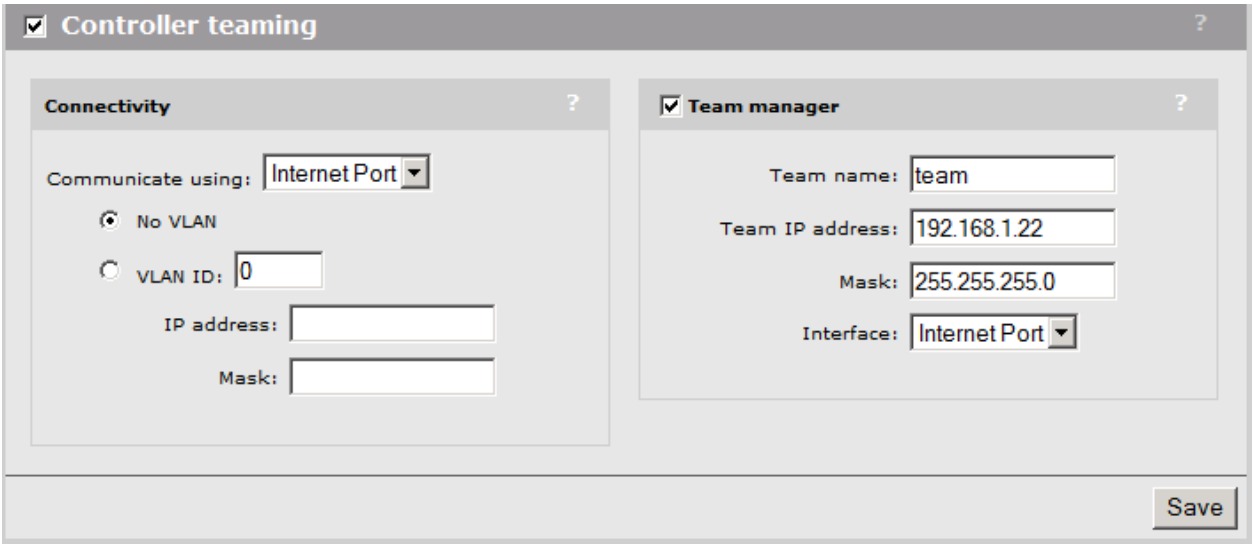
Ensure Device discover of the APs is enabled on the Internet port.



13.2.4 – Enable Teaming

Management | Teaming

From the Team Manager assign a virtual IP address to the Team. Ensure this IP address is within the same subnet as the Internet port. Configure the Team Manager to listen for teaming requests using the Internet port.

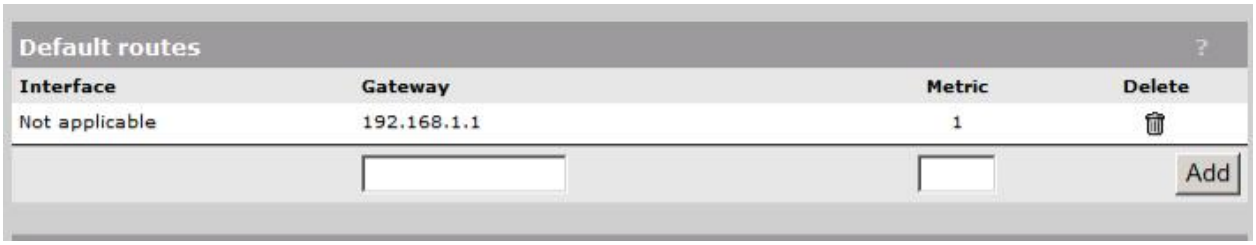


13.2.5 – Configure Team Members

Login or console into the Team Members and reconfigure the basis IP settings for the LAN and Internet ports by assigning the Internet port and IP address within the same range as the Team Manager and ensuring it is an untagged member of the same VLAN as the Team Manager. In the example we have assigned 192.168.1.21 to the Team Member's Internet port.

Network | IP Route

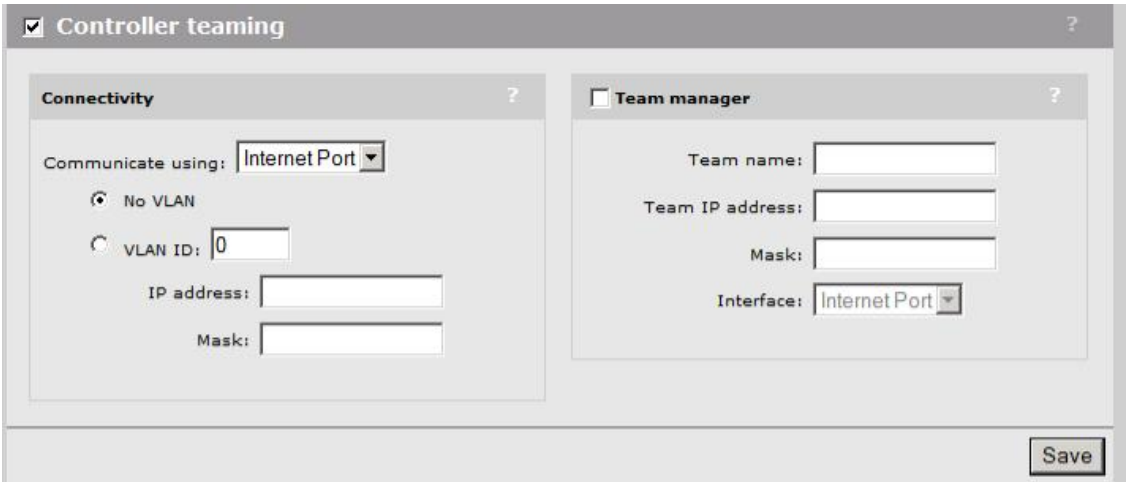
Set the default gateway of all the Team Members to use the same interface as the Team Manager. In the example we are using a gateway of 192.168.1.1



13.2.6 – Enable Teaming

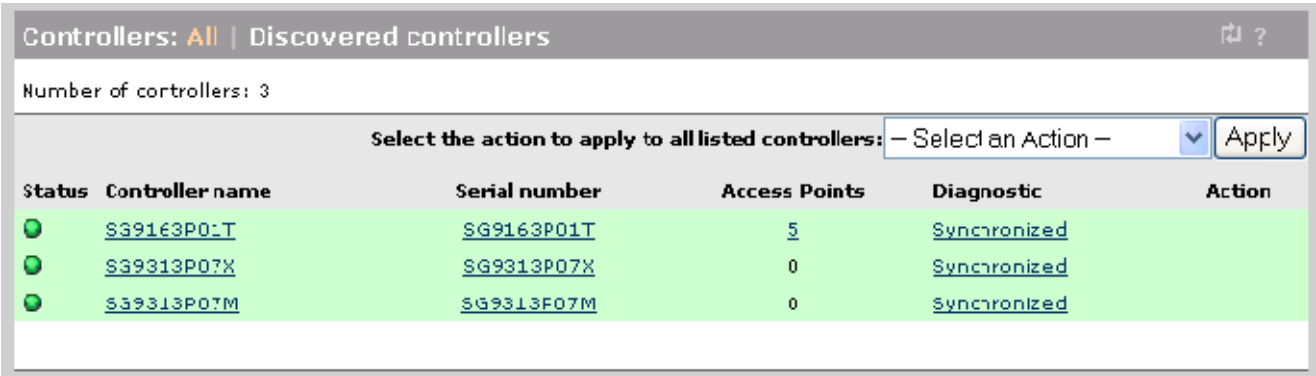
Enable Teaming on each member switch and ensure communication is via the Internet port

Management | Teaming



At this stage the member controller(s) should become joined and synced into the Team. To verify this check the status of discovered controllers

Controllers | Overview | Discovered Controllers



Below is a description of the status lights

Green: The controller has joined the team and its configuration is synchronized with the settings defined on the team manager. It is fully operational.
Red: The controller is not functioning normally. Select **Overview | Discovered controllers** and refer to the **Diagnostic** column for details.
Grey flashing: An action is pending. Select **Overview | Discovered controllers** and refer to the **Action** column for details.
Grey solid: The controller is configured as a member of the team, but is currently not active.

The APs should now begin re-syncing on all controllers.

Ensure ALL controllers and APs have been discovered and synchronised with the Team prior to making any further changes.

14 Appendix F: Guest Access in a Teamed Environment

When the controllers are in a teamed configuration the existing enterprise DHCP[1] and NAT[2] platforms are leveraged to provide these services for guest access.

The controller will act as a relay agent forwarding requests received from the wireless clients via the secure tunnel to a defined egress VLAN.

14.1 – Creating DHCP Scopes

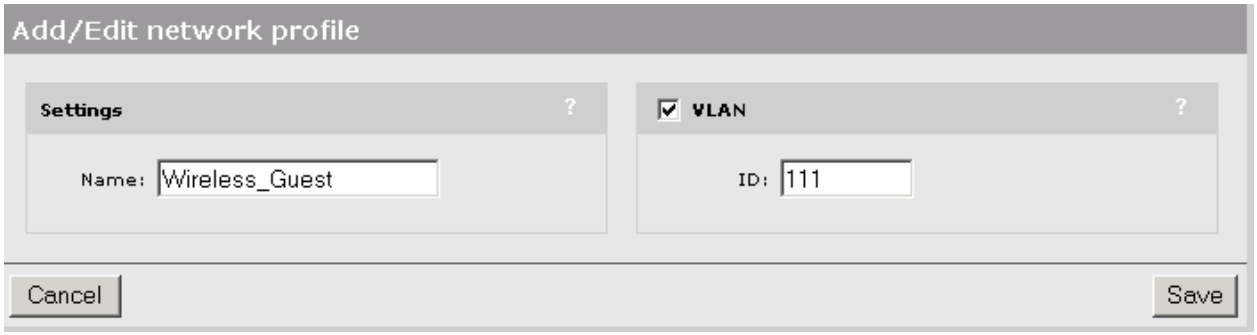
Create a scope on your DHCP server for Guest Access. Be sure to reserve/exclude some of the addresses controllers' the LAN ports. The MSM controllers use the LAN port as the DHCP relay interface.

13.2 – Creating Egress VLAN For Guests

Either re-use the existing Guest Network profile or if one does not exist on the Team create a new one

At the TEAM level create a network profile for the Guest VLAN.

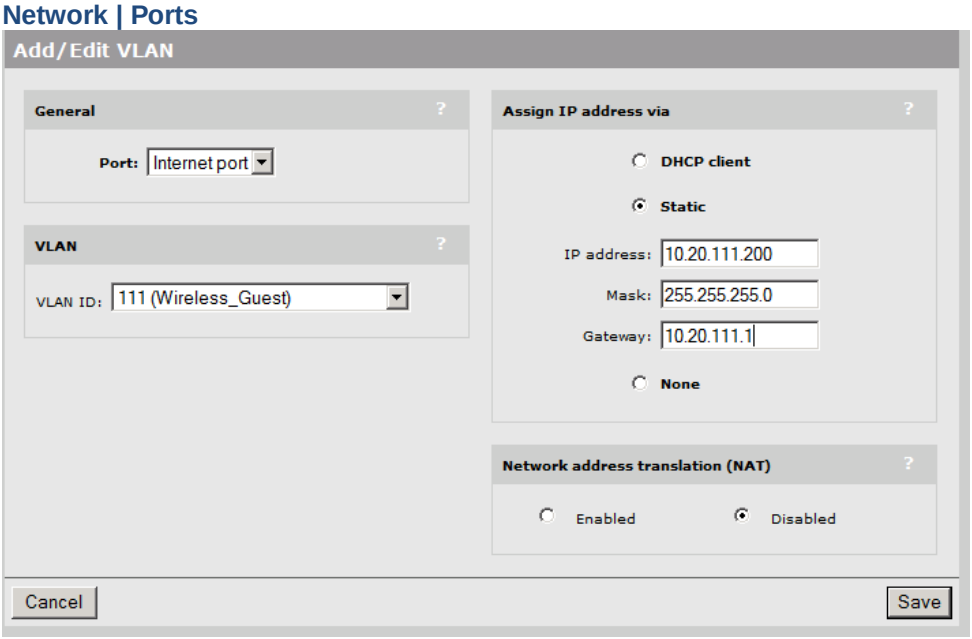
Team | Network | Network Profiles



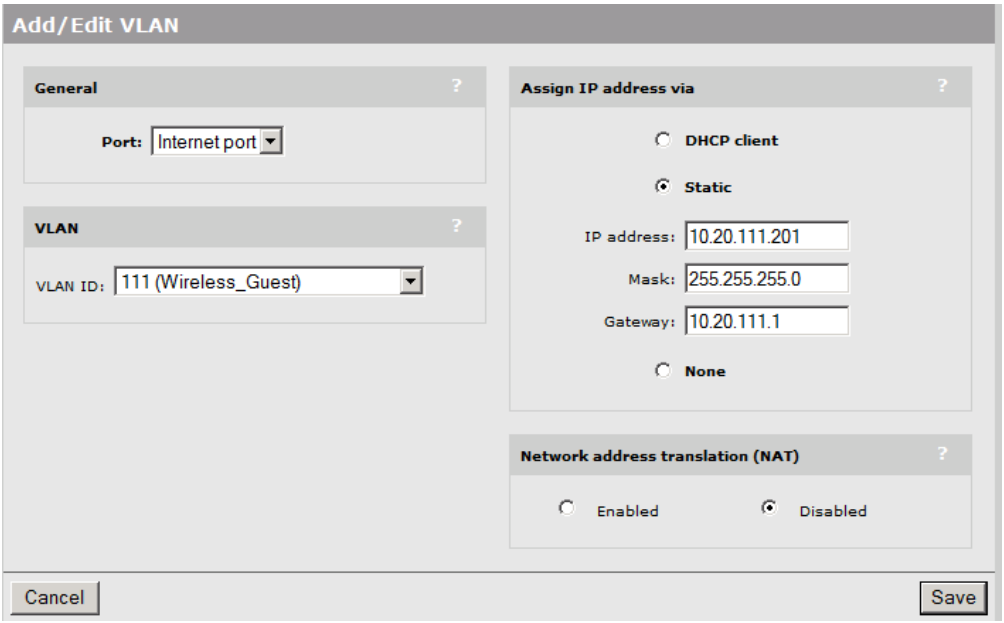
[1] Ensure DCHP scope for Guests is defined and activated
[2] The configuration of enterprise NAT services is outside the scope of this document

The next step is to assign the Wireless_Guest Network Profile to and Egress VLAN.

Network | Ports



The IP addressing configuration will need to be completed on **EACH** controller. For example the image above depicts the Team Manager configuration and image below depicts the Team Member configuration.



Key points to Note:

- The Controllers share the same subnet mask and gateway configuration
- NAT is disabled
- Ensure the Internet Port is configured as a Tagged member of VLAN 111

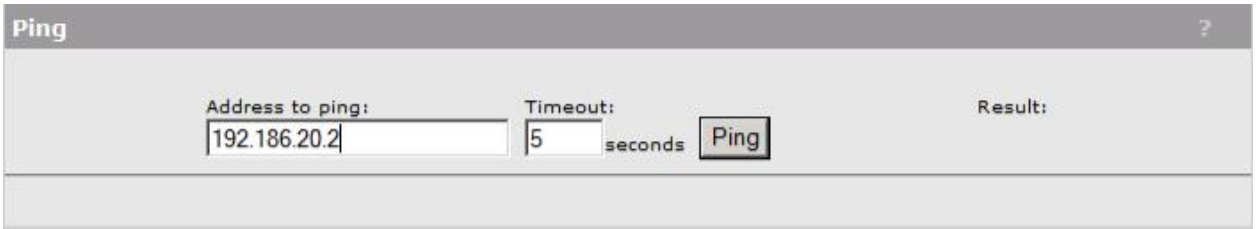
The controllers must be rebooted for the Egress VLAN assignment to take effect.

13.3 – Guest Roaming

To facilitate Guest Roaming between the controllers the LAN ports must be inter-connected on their own isolated network. Enable the LAN ports (if disconnected) and assign them the IP addresses previously reserved/excluded from the Guest DHCP scope configured in Step 1. The LAN ports must be configured with unique IP addresses within the same subnet.

Create a "Guest Roaming" VLAN, on your routing switch assign it the Gateway address and move the LAN ports into this VLAN as untagged members. Verify connectivity by pinging the LAN interface

Team | Tools | Ping



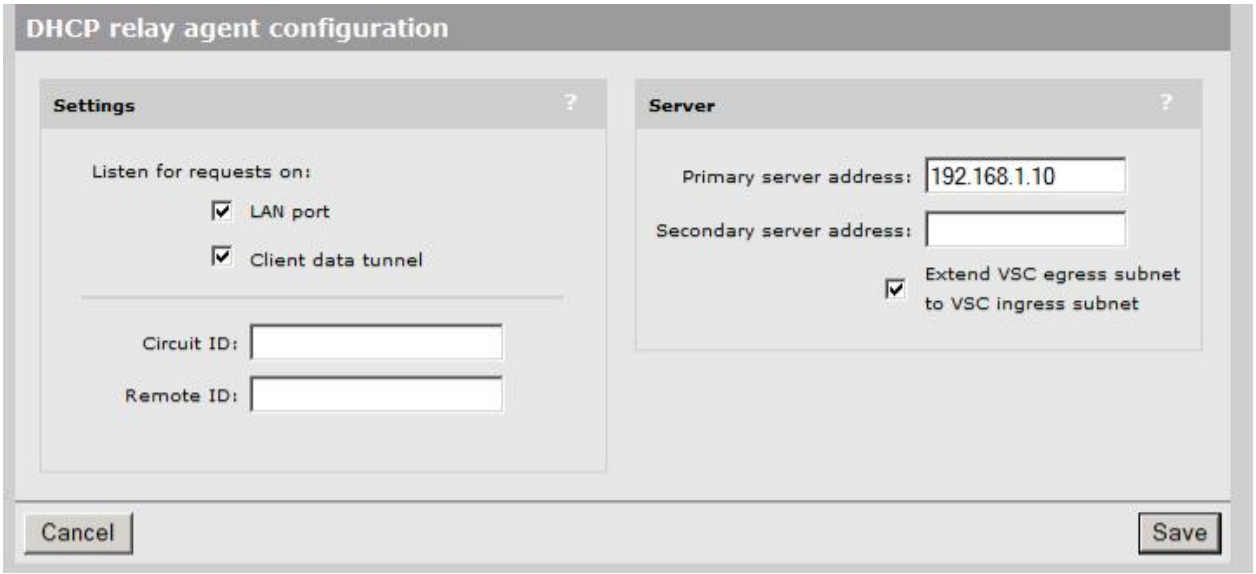
13.4 – Routing configuration

The DHCP Relay agent must be configured for the Team. If the DHCP servers are 1 hop or more away from the controller's subnet then static routes will need to be added to either the DHCP server, the router in the middle or both. For example if the DCHP relay request address is 192.168.20.1, then the DHCP server will reply with a destination address of 192.168.20.1 and will not find a route back to the correct controller. The DHCP server needs a gateway address or static route pointing to the router connected to the controllers. The router will have to have ***static host routes,*** one for each controller. For example

Host=192.168.20.21 mask=255.255.255.255 gateway=192.168.1.21
Host= 192168.20.22 mask= 255.255.255.255 gateway=192.168.1.22

Team | Network | Address Allocation

Enable the DHCP relay agent for the Team and specify the Primary and secondary DHCP servers

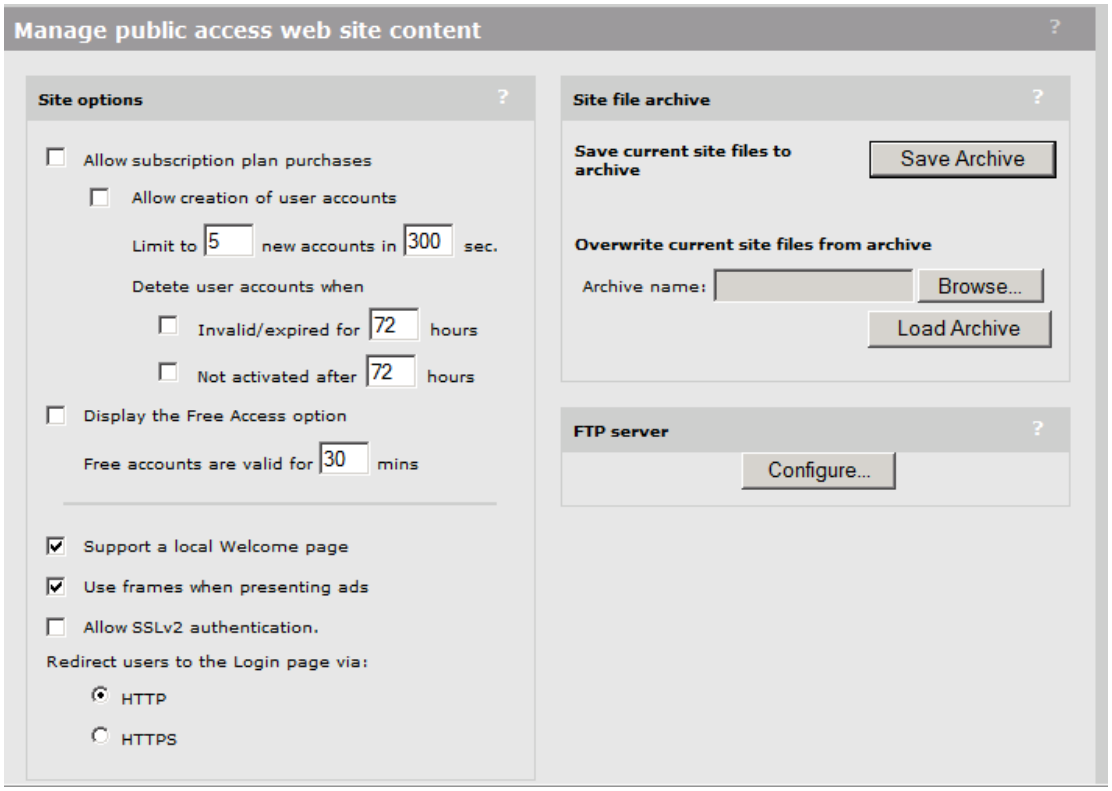


13.5 – Web Pages

If you have customised the Login Page, these files will need to be copied from the Team Manager to all controllers within the Team. Skip this step if you are using default setting for Login Page

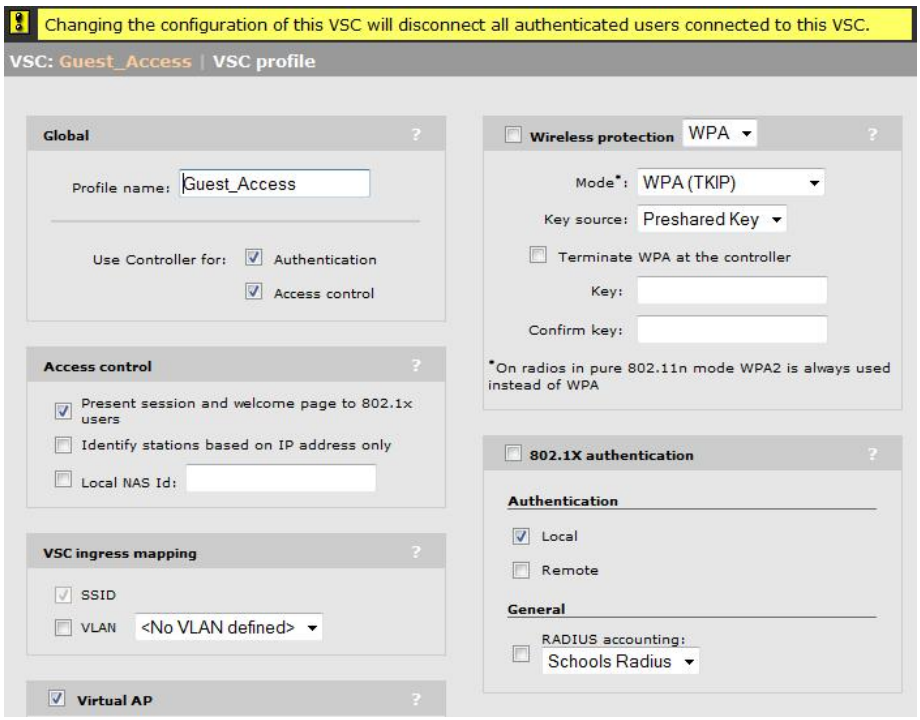
Team Controller | Public Access | Web Content

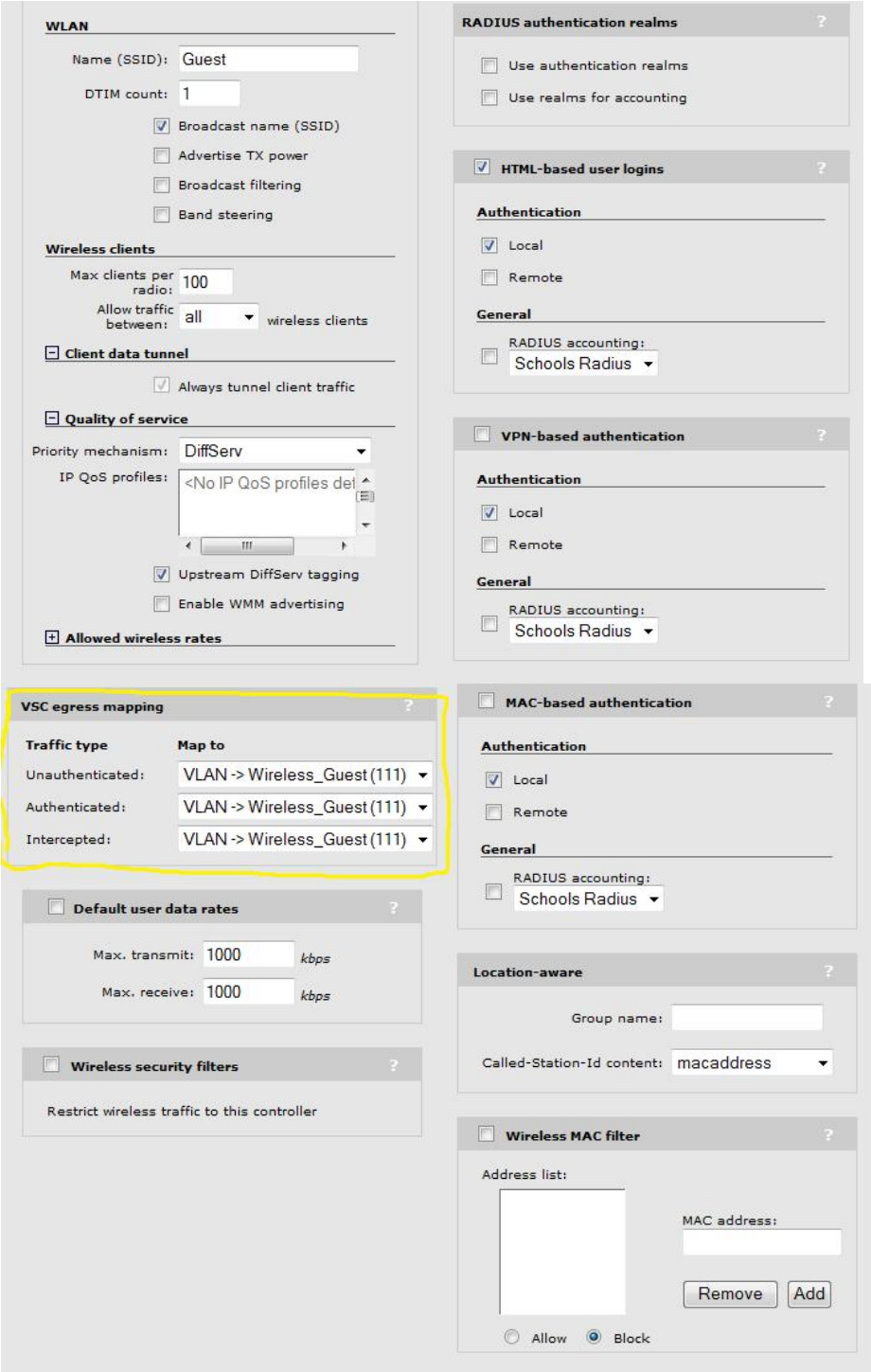
Select “Save Archive”

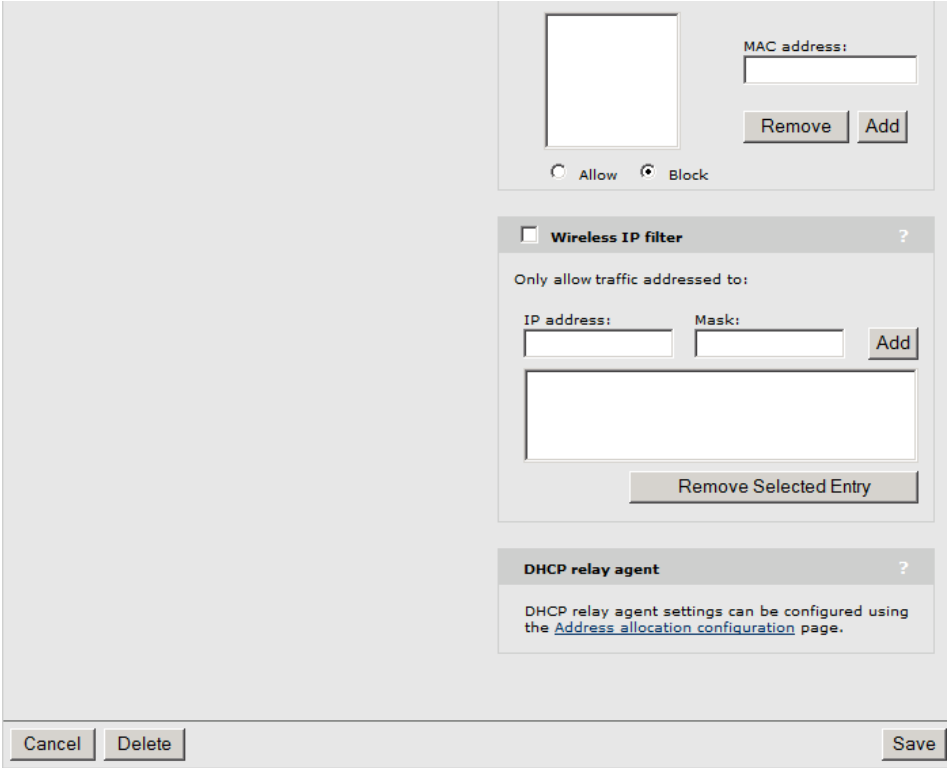


Login to each controller using via its Internet Port IP address; go to the above screen and select “Load Archive” to restore the web content. This must be completed on each controller within the Team.

Because this is an access controlled VSC all traffic will be traversing the controller, therefore in this example we are defining the egress VLAN on the VSC. Similar to the single controller Guest Access example HTML login will be used.





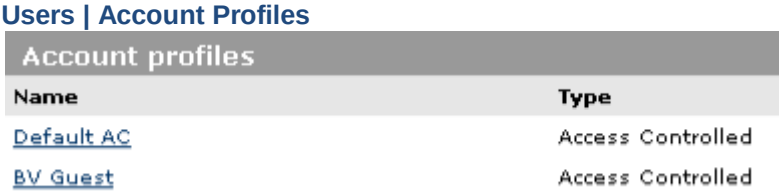


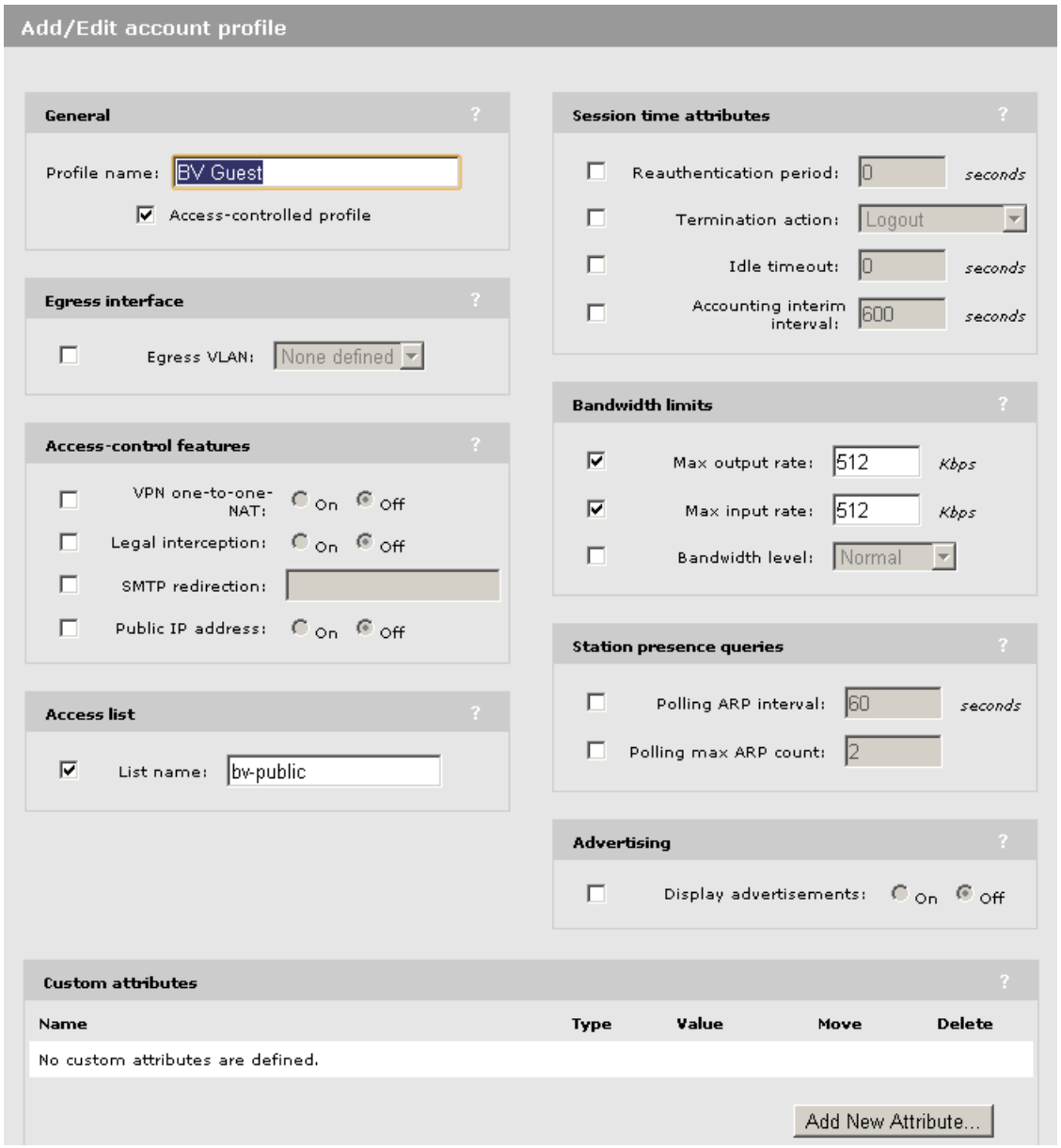
Note: Ensure any “DHCP-Relay Agent per VSC” configuration have been disabled for the Guest VSC as the Guest VSC will use the DHCP-Rely configuration under the Network | Address Allocation | DHCP-Relay.

14.1.1 Account Profiles

Account profiles need to be configured before they can be allocated in the user accounts (Section 14.1.2). In this example, the profile BV Guest is created.

Users | Account Profiles





The key feature is the List name set here to “bv-public”. This is what the attributes in Section 12.2.2 were referencing.

14.1.2 Users

The account “bakers” makes use of the Crescent access-controlled VSC, along with the configured ACLs.

Users | User Accounts