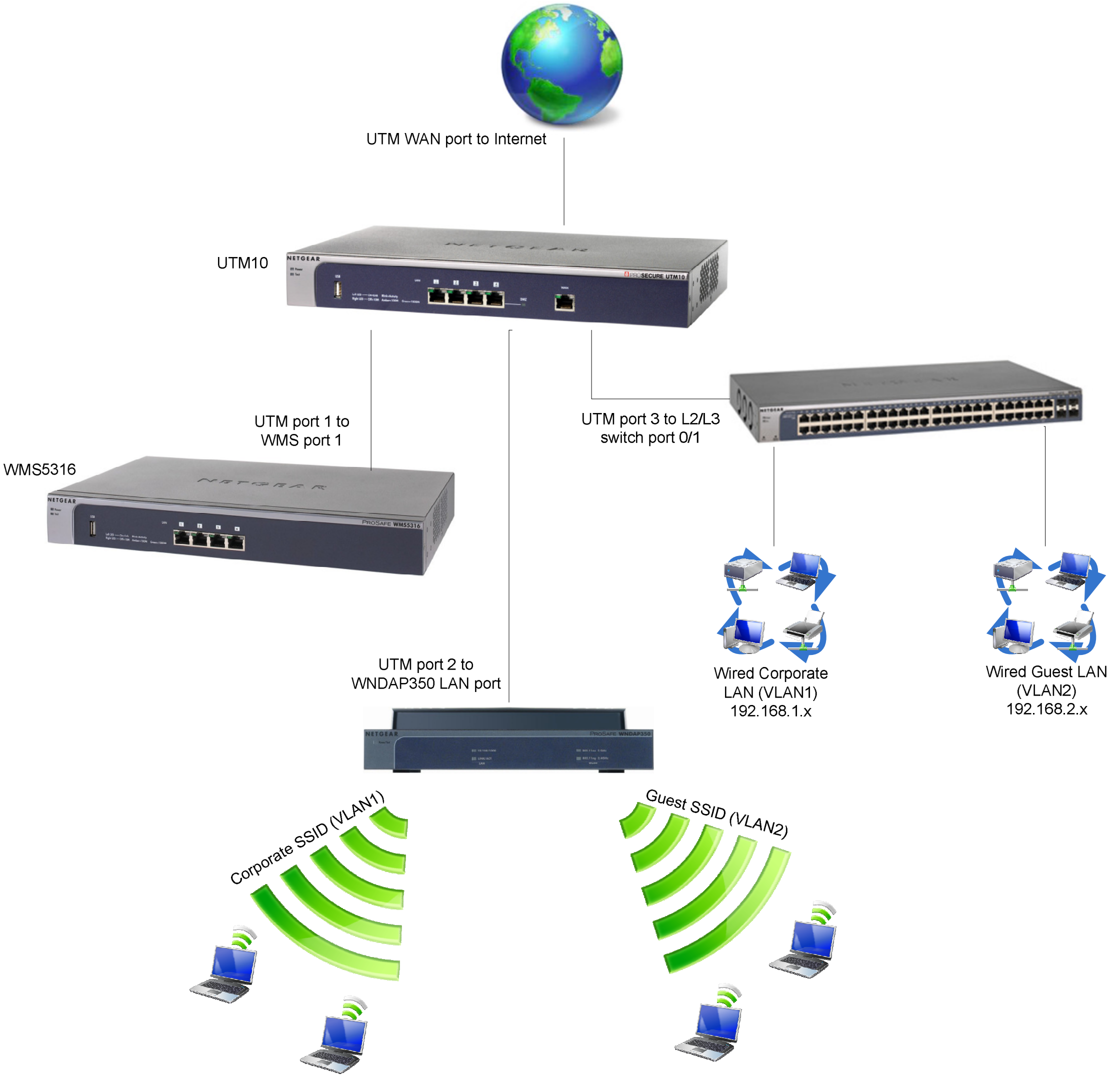
NETGEAR®
Connect with Innovation™

UTM10 in multi-SSID, multi-VLAN network with WMS5316

This document describes how to use the UTM10 (unified threat management system) and WMS5316 (wireless management system) to create a multi-VLAN, multi-SSID network in conjunction with a layer 2 or layer 3 switch. Each wired network will have a corresponding wireless network. Wired clients will be able to communicate with wireless clients on the same VLAN. Clients (wired or wireless) will not be able to communicate with clients on other VLANs.

For simplicity this example will only use one wireless access point (WNDAP350). Further access points can be added following the configuration laid out here. Also, if a L3 switch is used, this example assumes routing between VLANs is not set up on the switch.

Network diagram


UTM WAN port to Internet
UTM10
UTM port 1 to WMS port 1
WMS5316
UTM port 3 to L2/L3 switch port 0/1
Wired Corporate LAN (VLAN1) 192.168.1.x
Wired Guest LAN (VLAN2) 192.168.2.x
UTM port 2 to WNDAP350 LAN port
Corporate SSID (VLAN1)
Guest SSID (VLAN2)

Network setup

UTM10 WAN port connected to internet
UTM10 port 1 connected to WMS5316 port 1
UTM10 port 2 connected to WNDAP350 LAN port
UTM10 port 3 connected to L2/L3 switch port 0/1

UTM10 configuration:

LAN IP
192.168.1.1

VLAN1 (default)
Corporate network
192.168.1.1
Membership: Ports 1, 2, 3, 4
DHCP enabled 192.168.1.0 /24

VLAN2
Guest network
192.168.20.1
Membership: Ports 2, 3
DHCP enabled 192.168.2.0 /24

WMS5316 configuration:

LAN IP
192.168.1.250
Untagged VLAN: 1 / Management VLAN: 1

Access Point (WNDAP350) configuration:

LAN IP
192.168.1.235
Corporate SSID – VLAN 1
Guest SSID – VLAN 2
Note: WNDAP350 is not configured directly. It is configured from the WMS5316.

Layer 2 / Layer 3 switch configuration:

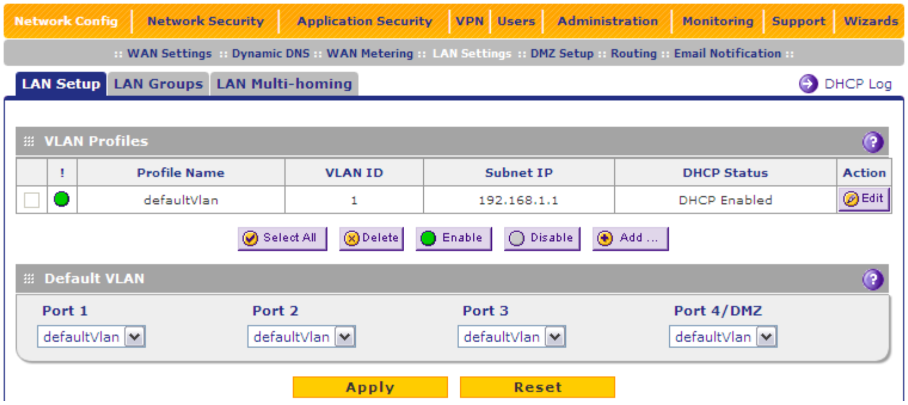
Management IP
192.168.1.239
Management VLAN = VLAN1

Port configuration:
(Untagged = U; Tagged = T)

	VLAN1	VLAN2
0/1	T	T
0/2	U	
0/3		U

PVID settings: 0/1 = 1; 0/2 = 1; 0/3 = 2

UTM10 Configuration


Network Config | Network Security | Application Security | VPN | Users | Administration | Monitoring | Support | Wizards
:: WAN Settings :: Dynamic DNS :: WAN Metering :: LAN Settings :: DMZ Setup :: Routing :: Email Notification ::
LAN Setup
LAN Groups
LAN Multi-homing
DHCP Log
Select All
Delete
Enable
Disable
Add ...
Apply
Reset

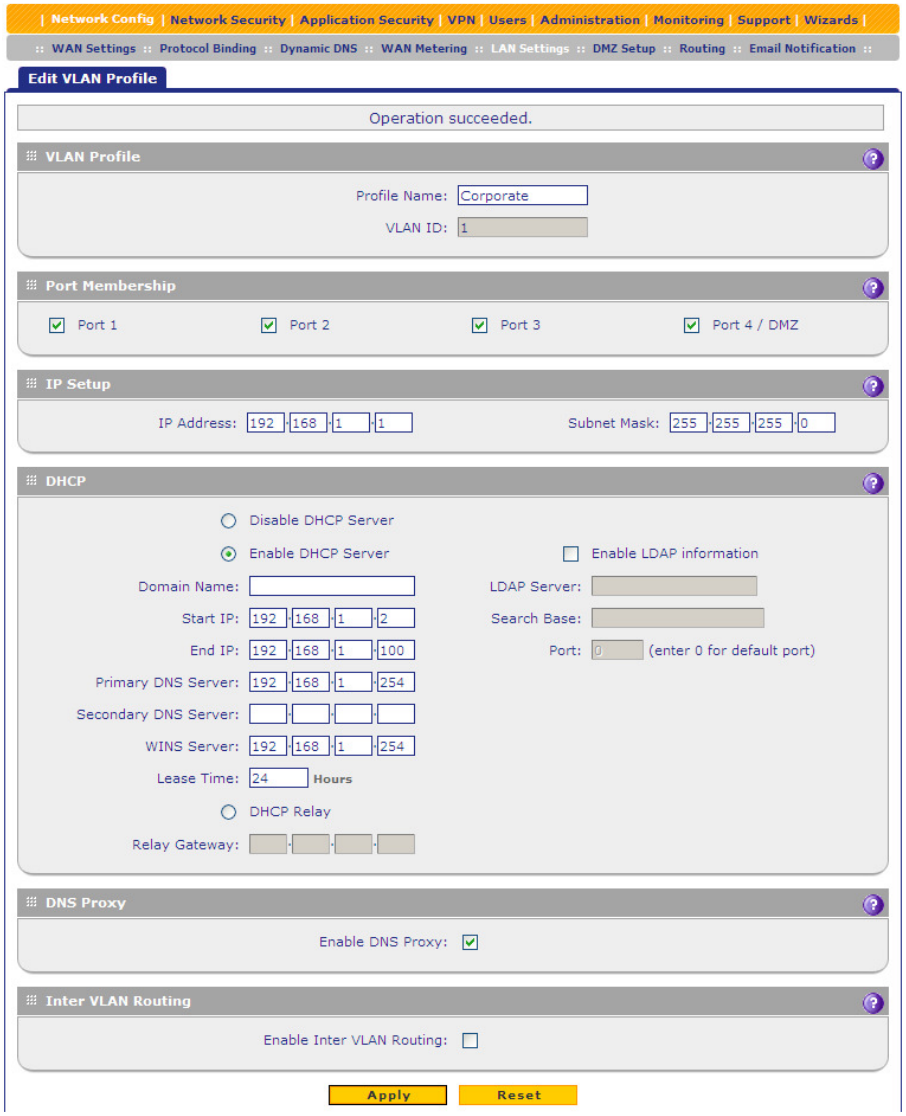
VLAN Profiles

	!	Profile Name	VLAN ID	Subnet IP	DHCP Status	Action
□	●	defaultVlan	1	192.168.1.1	DHCP Enabled	Edit

Default VLAN

Port 1	Port 2	Port 3	Port 4/DMZ
defaultVlan	defaultVlan	defaultVlan	defaultVlan

- Go to Network Config – LAN Settings
- Click on Edit for VLAN1


| Network Config | Network Security | Application Security | VPN | Users | Administration | Monitoring | Support | Wizards |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: WAN Metering :: LAN Settings :: DMZ Setup :: Routing :: Email Notification ::
Edit VLAN Profile
Apply
Reset

Operation succeeded.

VLAN Profile

Profile Name: Corporate

VLAN ID: 1

Port Membership

☑ Port 1 ☑ Port 2 ☑ Port 3 ☑ Port 4 / DMZ

IP Setup

IP Address: 192 . 168 . 1 . 1 Subnet Mask: 255 . 255 . 255 . 0

DHCP

○ Disable DHCP Server

● Enable DHCP Server □ Enable LDAP information

Domain Name: LDAP Server:

Start IP: 192 . 168 . 1 . 2 Search Base:

End IP: 192 . 168 . 1 . 100 Port: 0 (enter 0 for default port)

Primary DNS Server: 192 . 168 . 1 . 254

Secondary DNS Server:

WINS Server: 192 . 168 . 1 . 254

Lease Time: 24 Hours

○ DHCP Relay

Relay Gateway:

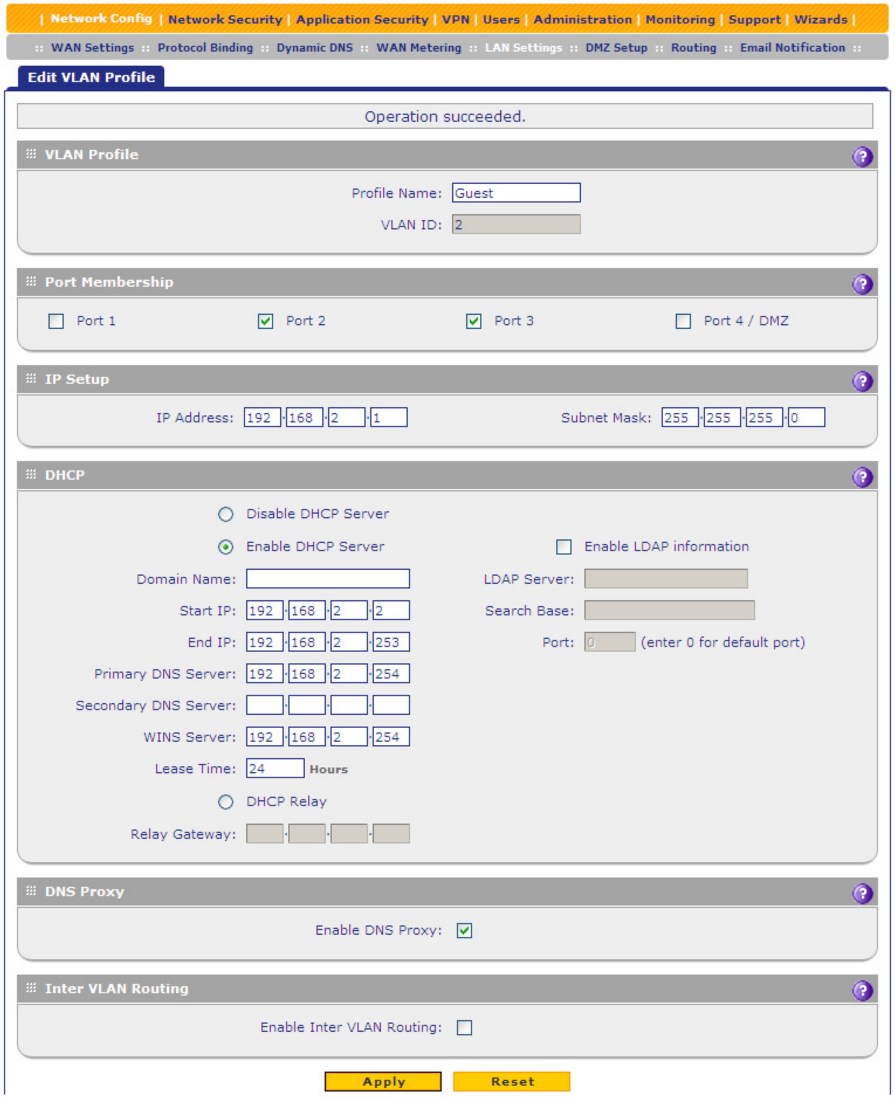
DNS Proxy

Enable DNS Proxy: ☑

Inter VLAN Routing

Enable Inter VLAN Routing: □

- Change the name of VLAN1 to Corporate and ensure that all ports are a member of it
- Press Apply


| Network Config | Network Security | Application Security | VPN | Users | Administration | Monitoring | Support | Wizards |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: WAN Metering :: LAN Settings :: DMZ Setup :: Routing :: Email Notification ::

Edit VLAN Profile

Operation succeeded.

VLAN Profile

Profile Name: Guest

VLAN ID: 2

Port Membership

☐ Port 1 ☑ Port 2 ☑ Port 3 ☐ Port 4 / DMZ

IP Setup

IP Address: 192 . 168 . 2 . 1 Subnet Mask: 255 . 255 . 255 . 0

DHCP

○ Disable DHCP Server

● Enable DHCP Server ☐ Enable LDAP information

Domain Name: LDAP Server:

Start IP: 192 . 168 . 2 . 2 Search Base:

End IP: 192 . 168 . 2 . 253 Port: 0 (enter 0 for default port)

Primary DNS Server: 192 . 168 . 2 . 254

Secondary DNS Server:

WINS Server: 192 . 168 . 2 . 254

Lease Time: 24 Hours

○ DHCP Relay

Relay Gateway:

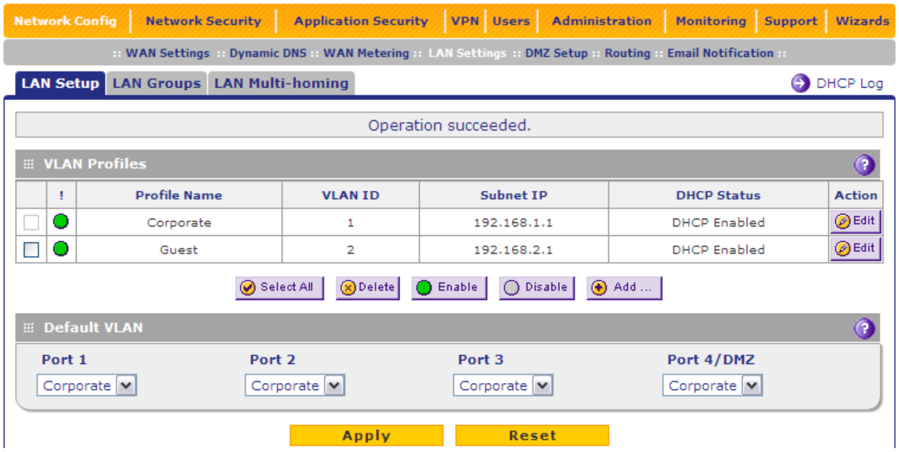
DNS Proxy

Enable DNS Proxy: ☑

Inter VLAN Routing

Enable Inter VLAN Routing: ☐

- Once back at the LAN Setup screen, press Add under VLAN Profiles
- The Add VLAN Profile screen will display (shown on the left)
- Create VLAN2 as shown, making ports 2 and 3 a member of it
- Configure IP address as 192.168.2.1 and enable DHCP Server as shown
- Press Apply


Network Config | Network Security | Application Security | VPN | Users | Administration | Monitoring | Support | Wizards
:: WAN Settings :: Dynamic DNS :: WAN Metering :: LAN Settings :: DMZ Setup :: Routing :: Email Notification ::
LAN Setup
LAN Groups
LAN Multi-homing
DHCP Log

Operation succeeded.

VLAN Profiles

	!	Profile Name	VLAN ID	Subnet IP	DHCP Status	Action
☐	●	Corporate	1	192.168.1.1	DHCP Enabled	Edit
☐	●	Guest	2	192.168.2.1	DHCP Enabled	Edit

Select All
Delete
Enable
Disable
Add ...

Default VLAN

Port 1	Port 2	Port 3	Port 4/DMZ
Corporate	Corporate	Corporate	Corporate

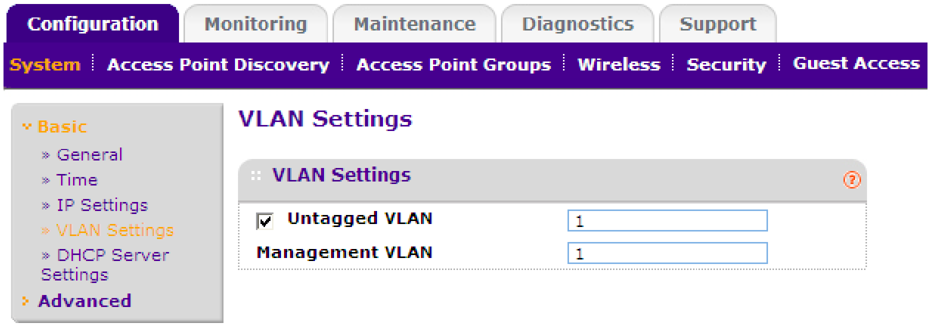
- You will be returned to the LAN Setup screen which will display a summary of the VLANs as shown

WMS5316 Configuration

Note:

1: This document will assume that you have already synchronized one or more access points with the WMS5316. If you are unfamiliar with how to do this, please see chapter 2 of the manual at http://kb.netgear.com/app/answers/detail/a_id/13374

2: We will use Basic Security Profiles which will mean that the SSIDs configured in these profiles will be assigned to all APs. Should you wish to have certain SSIDs assigned to certain APs only, you should use Access Point Groups.



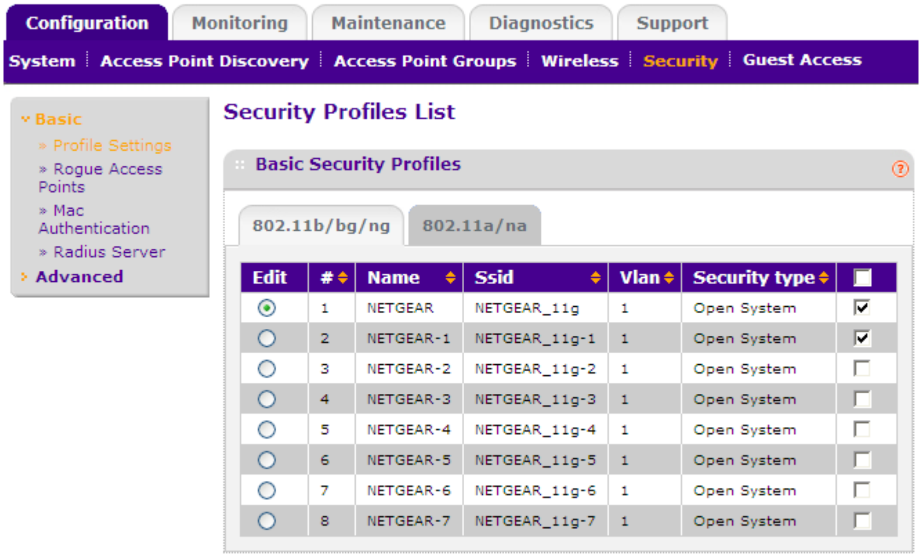
VLAN Settings

VLAN Settings

☑ Untagged VLAN 1

Management VLAN 1

- Under Configuration – System – Basic – VLAN Settings, ensure the settings are as shown



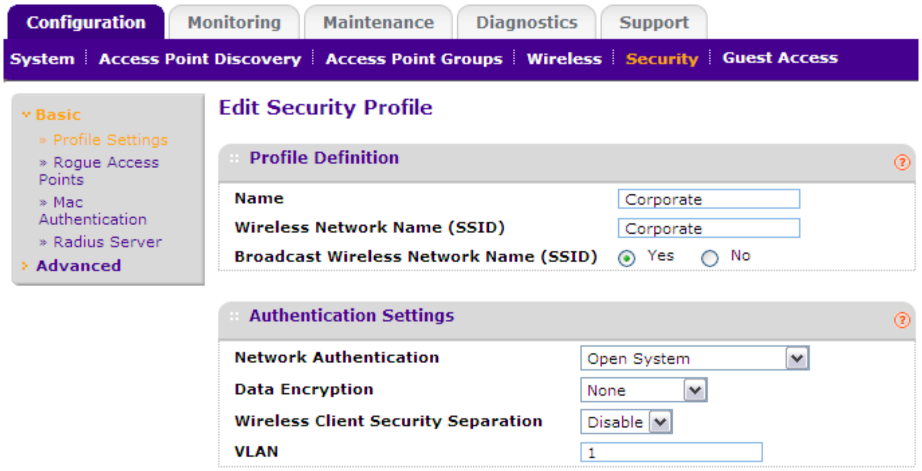
Security Profiles List

Basic Security Profiles

802.11b/bg/ng | 802.11a/na

Edit	#	Name	Ssid	Vlan	Security type	□
●	1	NETGEAR	NETGEAR_11g	1	Open System	☑
○	2	NETGEAR-1	NETGEAR_11g-1	1	Open System	☑
○	3	NETGEAR-2	NETGEAR_11g-2	1	Open System	□
○	4	NETGEAR-3	NETGEAR_11g-3	1	Open System	□
○	5	NETGEAR-4	NETGEAR_11g-4	1	Open System	□
○	6	NETGEAR-5	NETGEAR_11g-5	1	Open System	□
○	7	NETGEAR-6	NETGEAR_11g-6	1	Open System	□
○	8	NETGEAR-7	NETGEAR_11g-7	1	Open System	□

- Go to Configuration – Security – Basic – Profile Settings
- Ensure that both profile 1 and 2 are enabled (enable the tick-box at the far right for each profile)
- Press Apply
- Choose the first profile and press Edit



Edit Security Profile

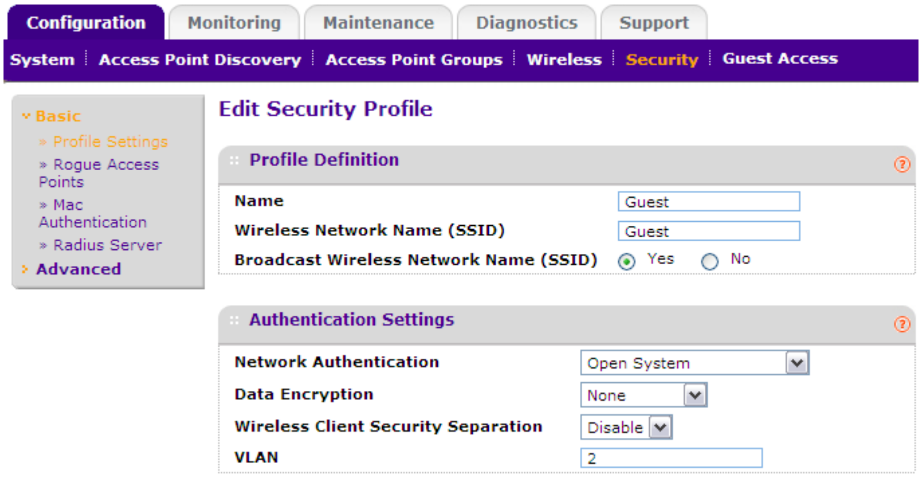
Profile Definition

Name	Corporate
Wireless Network Name (SSID)	Corporate
Broadcast Wireless Network Name (SSID)	● Yes ○ No

Authentication Settings

Network Authentication	Open System
Data Encryption	None
Wireless Client Security Separation	Disable
VLAN	1

- Configure the profile as shown
- Configure encryption as required also
- Press Apply
- Press Back to return to the Security Profiles List
- Choose the second profile and press Edit



Edit Security Profile

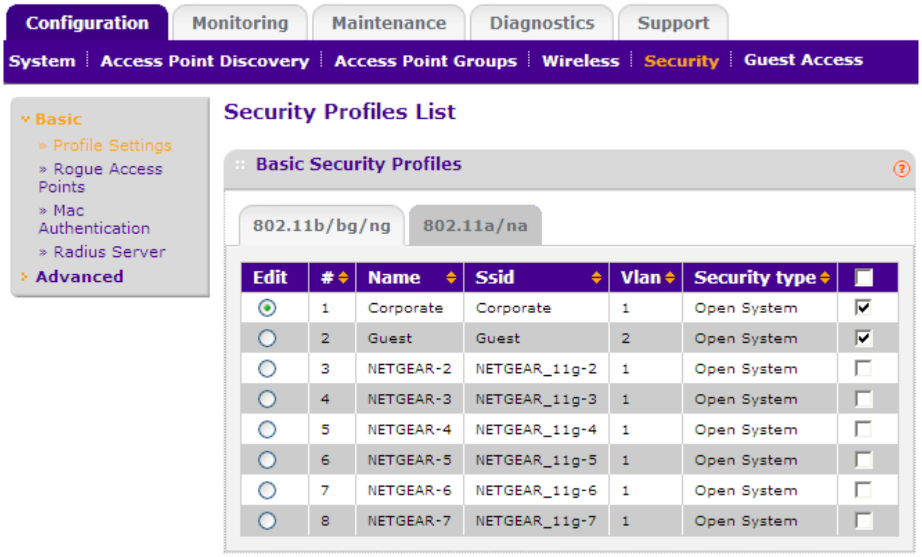
Profile Definition

Name	Guest
Wireless Network Name (SSID)	Guest
Broadcast Wireless Network Name (SSID)	● Yes ○ No

Authentication Settings

Network Authentication	Open System
Data Encryption	None
Wireless Client Security Separation	Disable
VLAN	2

- Again, configure the profile as shown
- Configure encryption as required
- Press Back to return to the Security Profiles List



Security Profiles List

Basic Security Profiles

Edit	#	Name	Ssid	Vlan	Security type	□
●	1	Corporate	Corporate	1	Open System	☑
○	2	Guest	Guest	2	Open System	☑
○	3	NETGEAR-2	NETGEAR_11g-2	1	Open System	□
○	4	NETGEAR-3	NETGEAR_11g-3	1	Open System	□
○	5	NETGEAR-4	NETGEAR_11g-4	1	Open System	□
○	6	NETGEAR-5	NETGEAR_11g-5	1	Open System	□
○	7	NETGEAR-6	NETGEAR_11g-6	1	Open System	□
○	8	NETGEAR-7	NETGEAR_11g-7	1	Open System	□

- The Security Profiles List should now look as shown

Testing

1: Connect to the Corporate SSID (VLAN1) and verify the following:

- Client obtains an IP in the range 192.168.1.x
- Client *can* communicate with devices on the wired corporate LAN (VLAN1)
- Client *cannot* communicate with devices on the wired guest LAN (VLAN2)
- Client can access the internet

2: Connect to the Guest SSID (VLAN2) and verify the following:

- Client obtains an IP in the range 192.168.2.x
- Client *can* communicate with devices on the wired guest LAN (VLAN2)
- Client *cannot* communicate with devices on the wired corporate LAN (VLAN1)
- Client can access the internet

Should you require clients on VLAN1 to be able to communicate with clients on VLAN2, then you can enable Inter-VLAN Routing on both VLANs on the UTM10.