NETGEAR®
Connect with Innovation™

WFS709TP – Case Scenario: Wireless deployment for a Corporate and Public network

This document describes the activities undertaken to deploy a Wireless solution using the Wireless Controller WFS709TP and multiple Lightweight Access Points (WGL102).

The description will encompass how to create an environment with multiple SSIDs, with VLAN separation, VLAN routing and DHCP enabled for each VLAN to serve the Wireless clients with the relevant TCP/IP settings.

NOTE:

To ensure the configuration changes are retained in case of Power cycles please ensure that the configuration is saved at all time using the Save Configuration tab.

Table of Contents

Section 1 – Initial Setup

Physical Setup

VLAN1: Ports 1/0 – 4

Connected to the **Corporate** network via Trunk to a Layer2/Layer3 switch (in the Diagram below a Netgear Layer 2/Layer 3 switch)

VLAN2: Port 1/5

Connected to the **Public** via a Trunk to a Layer 2/Layer 3 switch

VLAN100:

Separate the APs traffic from the rest of the network

Logical setup

APs Wireless Configuration

VLAN1: SSID = Corporate
Authentication WPA-PSK

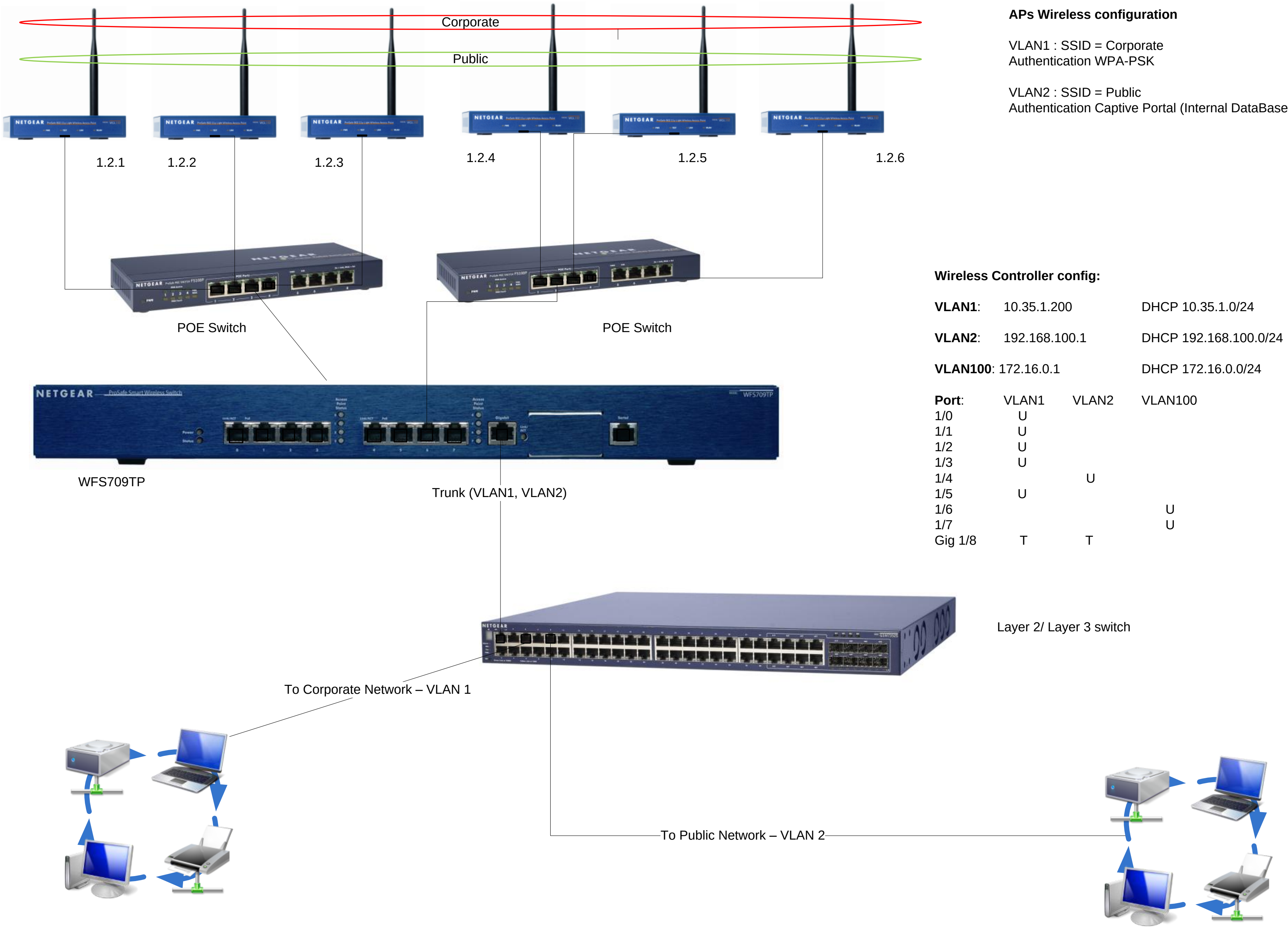
VLAN2: SSID = Public
Authentication Captive Portal (Internal Database)

Wireless Controller Configuration:

VLAN1:	10.35.1.200	DHCP 10.35.1.0/24
VLAN2:	192.168.100.1	DHCP 192.168.100.0/24
VLAN100:	172.16.0.1	DHCP 172.16.0.0/24

U = Untagged T= Tagged

Port:	**VLAN1**	**VLAN2**	**VLAN100**
1/0	U		
1/1	U		
1/2	U		
1/3	U		
1/4	U		
1/5		U	
1/6			U
1/7			U
Gig 1/8	T	T	



APs Wireless configuration

VLAN1 : SSID = Corporate
Authentication WPA-PSK

VLAN2 : SSID = Public
Authentication Captive Portal (Internal DataBase)

Wireless Controller config:

VLAN1: 10.35.1.200 DHCP 10.35.1.0/24

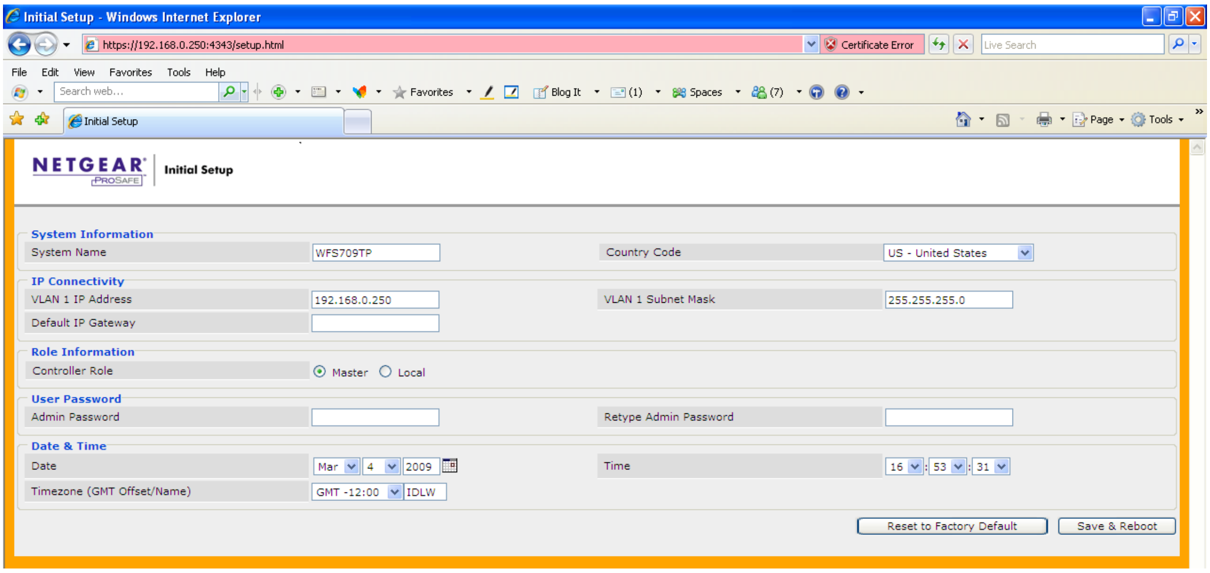
VLAN2: 192.168.100.1 DHCP 192.168.100.0/24

VLAN100: 172.16.0.1 DHCP 172.16.0.0/24

Port:	VLAN1	VLAN2	VLAN100
1/0	U		
1/1	U		
1/2	U		
1/3	U		
1/4		U	
1/5	U		
1/6			U
1/7			U
Gig 1/8	T	T	

Initial configuration

When connecting the first time to the unit via the Web Interface (default IP address 192.168.0.250) the User is presented with the following page:


Initial Setup - Windows Internet Explorer
https://192.168.0.250:4343/setup.html
Certificate Error
Live Search
File Edit View Favorites Tools Help
Initial Setup
NETGEAR PROSAFE

Initial Setup

System Information

System Name	WFS709TP	Country Code	US - United States

IP Connectivity

VLAN 1 IP Address	192.168.0.250	VLAN 1 Subnet Mask	255.255.255.0
Default IP Gateway			

Role Information

Controller Role	● Master ○ Local

User Password

Admin Password		Retype Admin Password	

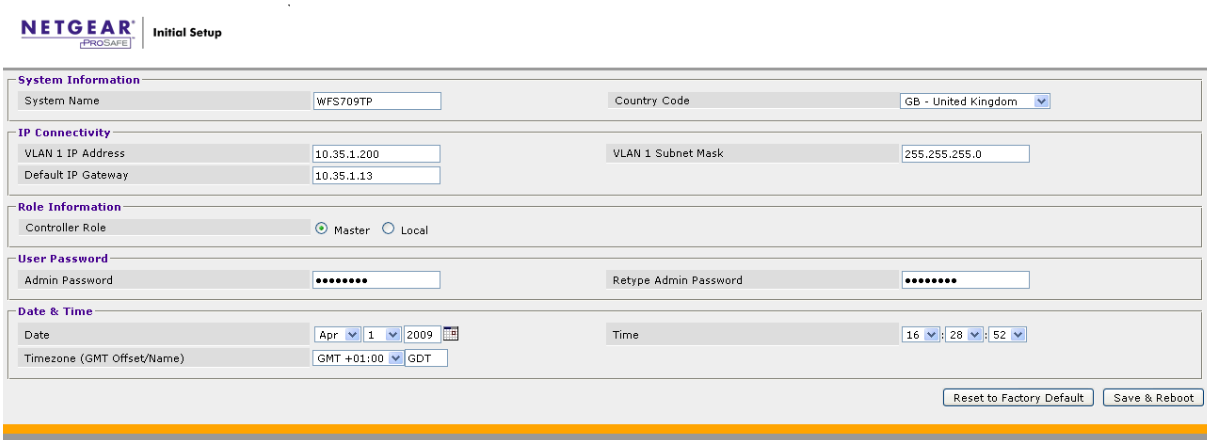
Date & Time

Date	Mar 4 2009	Time	16 : 53 : 31
Timezone (GMT Offset/Name)	GMT -12:00 IDLW		

Reset to Factory Default | Save & Reboot

The default configuration can be kept or changes can be made to suit the local LAN setup.

In this scenario the unit will be connected to a Corporate network via VLAN1 which is also retained as the management VLAN.



Initial Setup

System Information

System Name	WFS709TP	Country Code	GB - United Kingdom

IP Connectivity

VLAN 1 IP Address	10.35.1.200	VLAN 1 Subnet Mask	255.255.255.0
Default IP Gateway	10.35.1.13		

Role Information

Controller Role	● Master ○ Local

User Password

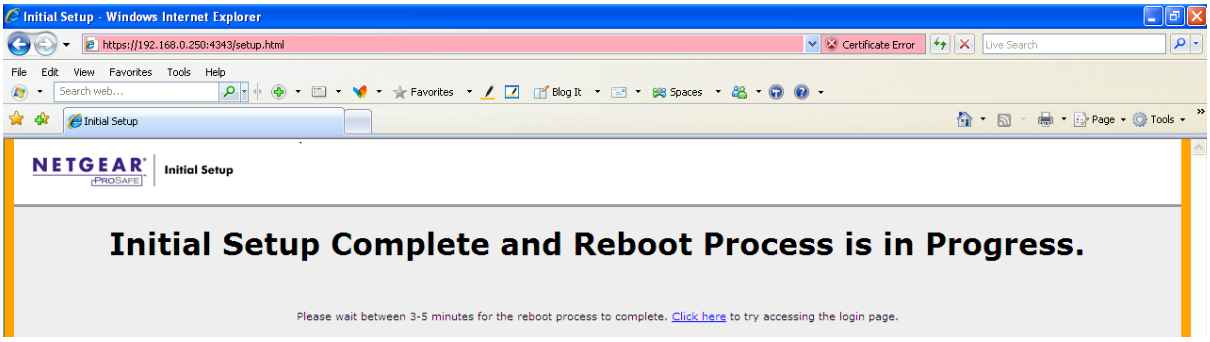
Admin Password	••••••••	Retype Admin Password	••••••••

Date & Time

Date	Apr 1 2009	Time	16 : 28 : 52
Timezone (GMT Offset/Name)	GMT +01:00 GDT		

Reset to Factory Default | Save & Reboot

Hit the **Save & Reboot** button is and the unit will Reboot.



Initial Setup - Windows Internet Explorer

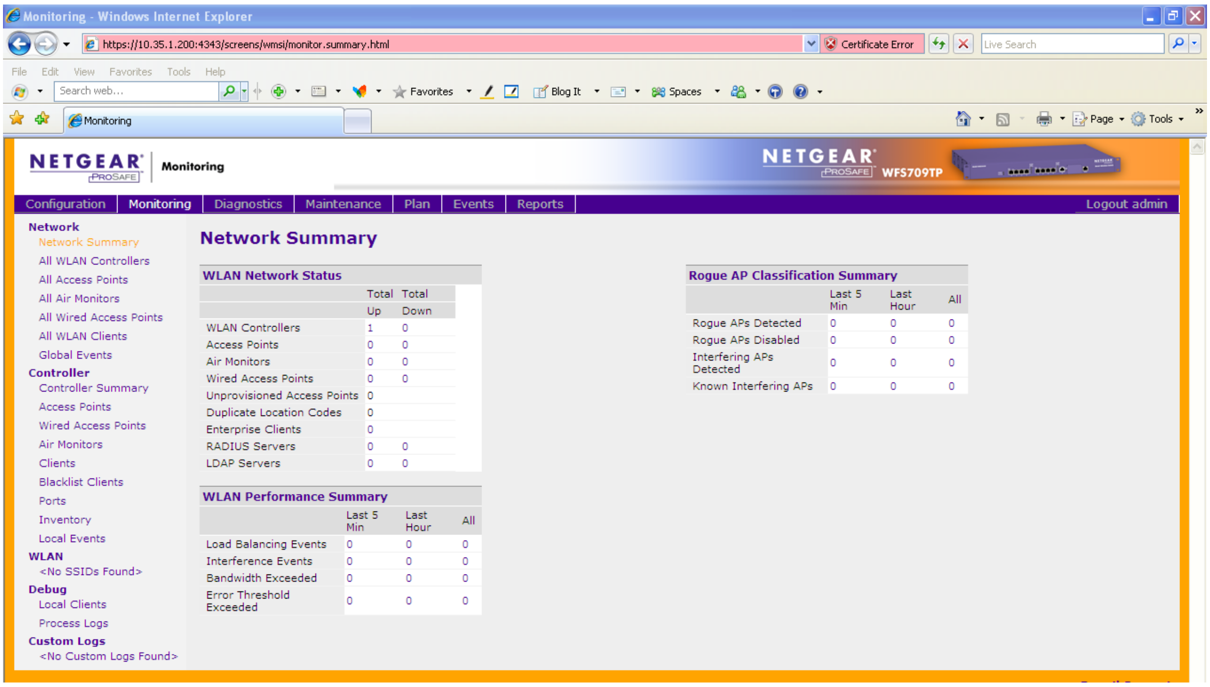
https://192.168.0.250:4343/setup.html

Initial Setup

Initial Setup Complete and Reboot Process is in Progress.

Please wait between 3-5 minutes for the reboot process to complete. Click here to try accessing the login page.

The next picture shows the Network summary, after reconnecting to the unit Web Interface upon its reboot.



Monitoring - Windows Internet Explorer

https://10.35.1.200:4343/screens/wmsi/monitor.summary.html

Monitoring

NETGEAR PROSAFE WFS709TP

Configuration | Monitoring | Diagnostics | Maintenance | Plan | Events | Reports | Logout admin

Network
- Network Summary
- All WLAN Controllers
- All Access Points
- All Air Monitors
- All Wired Access Points
- All WLAN Clients
- Global Events

Controller
- Controller Summary
- Access Points
- Wired Access Points
- Air Monitors
- Clients
- Blacklist Clients
- Ports
- Inventory
- Local Events

WLAN
- <No SSIDs Found>

Debug
- Local Clients
- Process Logs

Custom Logs
- <No Custom Logs Found>

Network Summary

WLAN Network Status

	Total	Total
	Up	Down
WLAN Controllers	1	0
Access Points	0	0
Air Monitors	0	0
Wired Access Points	0	0
Unprovisioned Access Points	0	
Duplicate Location Codes	0	
Enterprise Clients	0	
RADIUS Servers	0	0
LDAP Servers	0	0

WLAN Performance Summary

	Last 5 Min	Last Hour	All
Load Balancing Events	0	0	0
Interference Events	0	0	0
Bandwidth Exceeded	0	0	0
Error Threshold Exceeded	0	0	0

Rogue AP Classification Summary

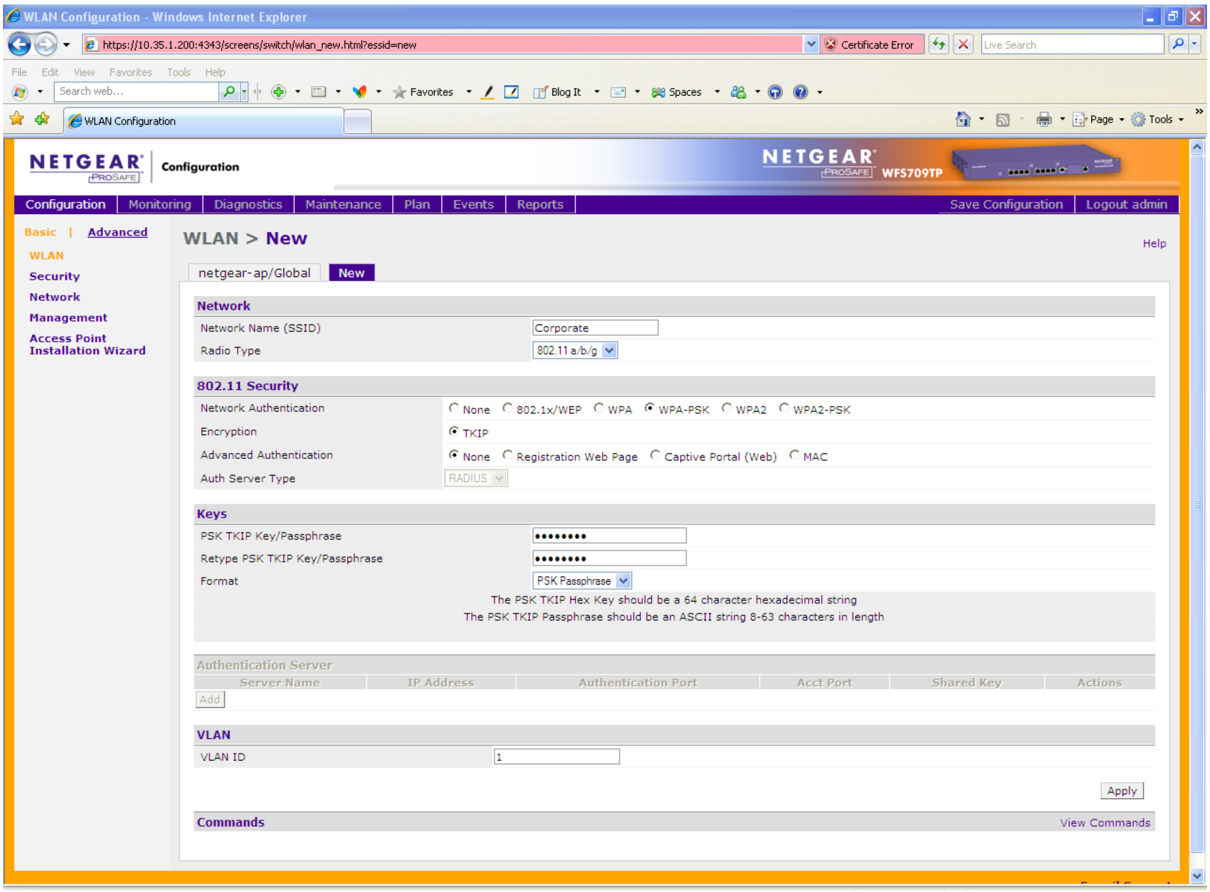
	Last 5 Min	Last Hour	All
Rogue APs Detected	0	0	0
Rogue APs Disabled	0	0	0
Interfering APs Detected	0	0	0
Known Interfering APs	0	0	0

Creating a new SSID

To create a new SSID access Configuration - Basic - WLAN.

In the two pictures below and as described in the **Physical setup** section, two SSIDs will be created:

- **Corporate**, with WPA-PSK authentication (Password = **12345678**)


WLAN Configuration - Windows Internet Explorer
https://10.35.1.200:4343/screens/switch/wlan_new.html?essid=new
Certificate Error
NETGEAR PROSAFE Configuration
NETGEAR PROSAFE WFS709TP
Configuration | Monitoring | Diagnostics | Maintenance | Plan | Events | Reports | Save Configuration | Logout admin
Basic | Advanced
WLAN
Security
Network
Management
Access Point Installation Wizard
Help
netgear-ap/Global
New
Apply
View Commands

WLAN > New

Network

Network Name (SSID)	Corporate
Radio Type	802.11 a/b/g

802.11 Security

Network Authentication	○ None ○ 802.1x/WEP ○ WPA ● WPA-PSK ○ WPA2 ○ WPA2-PSK
Encryption	● TKIP
Advanced Authentication	● None ○ Registration Web Page ○ Captive Portal (Web) ○ MAC
Auth Server Type	RADIUS

Keys

PSK TKIP Key/Passphrase	••••••••
Retype PSK TKIP Key/Passphrase	••••••••
Format	PSK Passphrase

The PSK TKIP Hex Key should be a 64 character hexadecimal string
The PSK TKIP Passphrase should be an ASCII string 8-63 characters in length

Authentication Server

Server Name	IP Address	Authentication Port	Acct Port	Shared Key	Actions

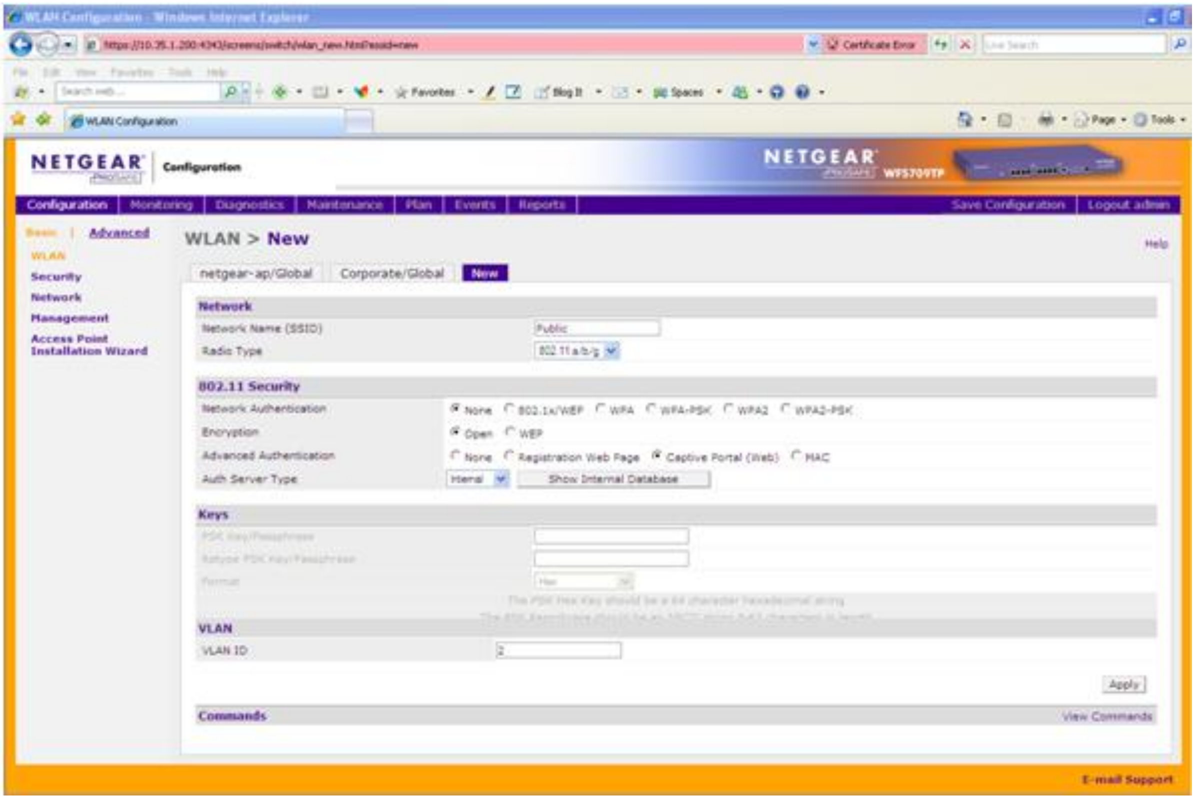
Add

VLAN

VLAN ID	1

Commands

- **Public ,** with Captive Portal (Web) authentication against the WFS709TP internal database


WLAN Configuration - Windows Internet Explorer
https://10.35.1.200:4343/screens/switch/wlan_new.html?essid=new
Certificate Error
NETGEAR PROSAFE Configuration
NETGEAR PROSAFE WFS709TP
Configuration | Monitoring | Diagnostics | Maintenance | Plan | Events | Reports | Save Configuration | Logout admin
Basic | Advanced
WLAN
Security
Network
Management
Access Point Installation Wizard
Help
netgear-ap/Global
Corporate/Global
New
Show Internal Database
Apply
View Commands
E-mail Support

WLAN > New

Network

Network Name (SSID)	Public
Radio Type	802.11 a/b/g

802.11 Security

Network Authentication	● None ○ 802.1x/WEP ○ WPA ○ WPA-PSK ○ WPA2 ○ WPA2-PSK
Encryption	● Open ○ WEP
Advanced Authentication	○ None ○ Registration Web Page ● Captive Portal (Web) ○ MAC
Auth Server Type	Internal

Keys

PSK Key/Passphrase	
Retype PSK Key/Passphrase	
Format	Hex

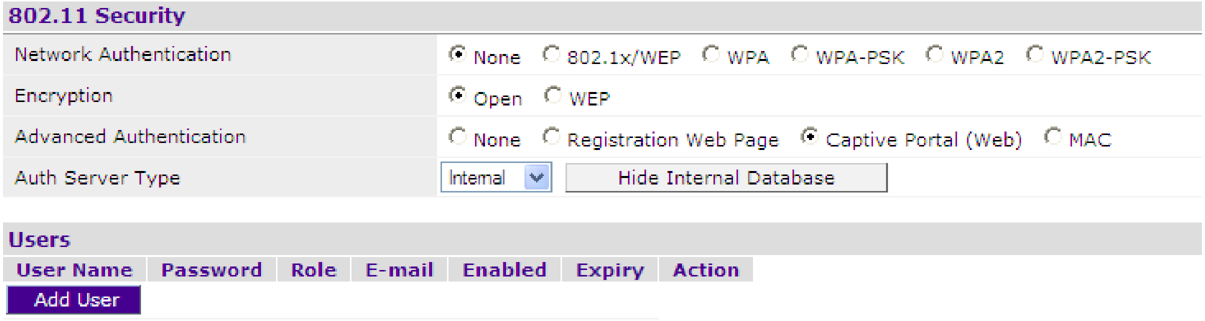
The PSK Hex Key should be a 64 character hexadecimal string
The PSK Passphrase should be an ASCII string 8-63 characters in length

VLAN

VLAN ID	2

Commands

To create Users in the Internal Database, click on Show Internal Database – Add User to add a New user:



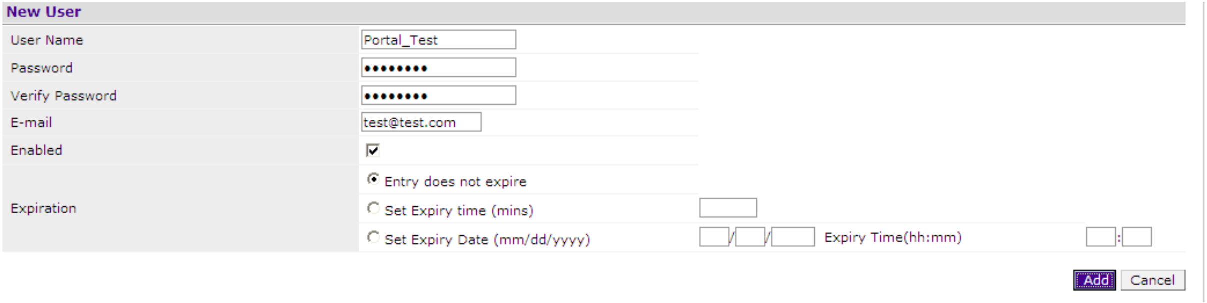
802.11 Security

Network Authentication	● None ○ 802.1x/WEP ○ WPA ○ WPA-PSK ○ WPA2 ○ WPA2-PSK
Encryption	● Open ○ WEP
Advanced Authentication	○ None ○ Registration Web Page ● Captive Portal (Web) ○ MAC
Auth Server Type	Internal ▾ Hide Internal Database

Users

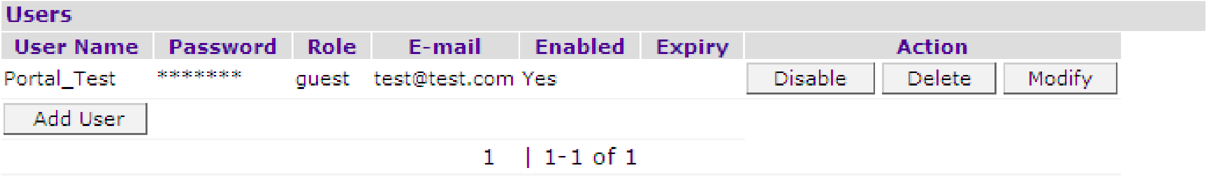
User Name	Password	Role	E-mail	Enabled	Expiry	Action

The example shows the creation of the **Portal_Test** user:



New User

User Name	Portal_Test
Password	••••••••
Verify Password	••••••••
E-mail	test@test.com
Enabled	☑
Expiration	● Entry does not expire ○ Set Expiry time (mins) ○ Set Expiry Date (mm/dd/yyyy) / / Expiry Time(hh:mm) :



Users

User Name	Password	Role	E-mail	Enabled	Expiry	Action
Portal_Test	********	guest	test@test.com	Yes		Disable Delete Modify

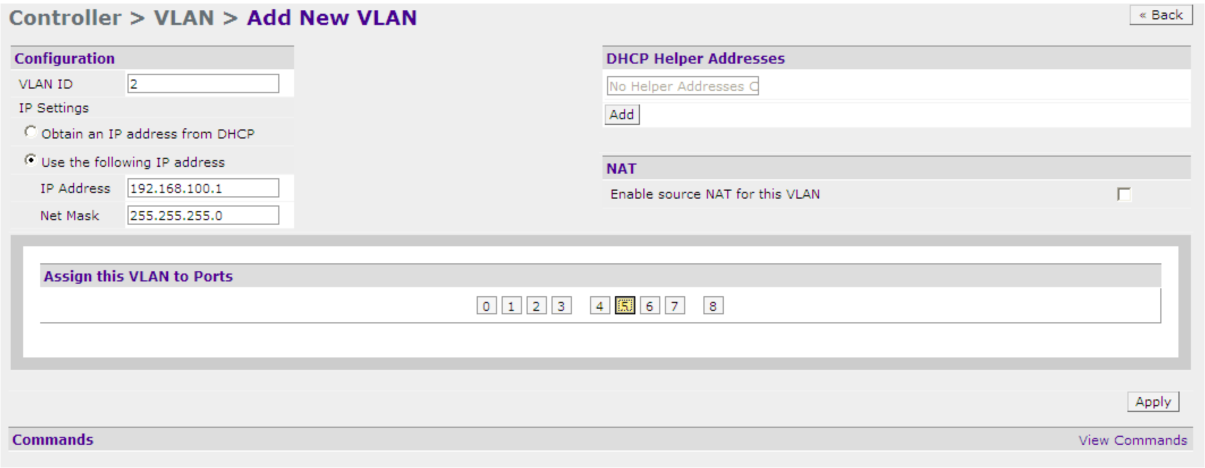
Create a new VLAN

VLAN 1 is the default VLAN for the WFS709TP – by default all the ports (Fa1/0-7, Gig 1/8) are members of VLAN1 – therefore access to the Controller Web Interface can take place connecting to any of the ports.

To create a new VLAN, access the menu via Configuration – Basic - Network – VLAN.

This menu will allow creation of the VLAN, but the IP address assigned to the VLAN and the VLAN Port membership will require to be setup separately.

To combine the setup of all the above settings please use the menu Configuration – Advanced – Controller – VLAN as in the examples below.



Controller > VLAN > Add New VLAN

Configuration

VLAN ID: 2

IP Settings

○ Obtain an IP address from DHCP

● Use the following IP address

IP Address: 192.168.100.1

Net Mask: 255.255.255.0

DHCP Helper Addresses

No Helper Addresses C

NAT

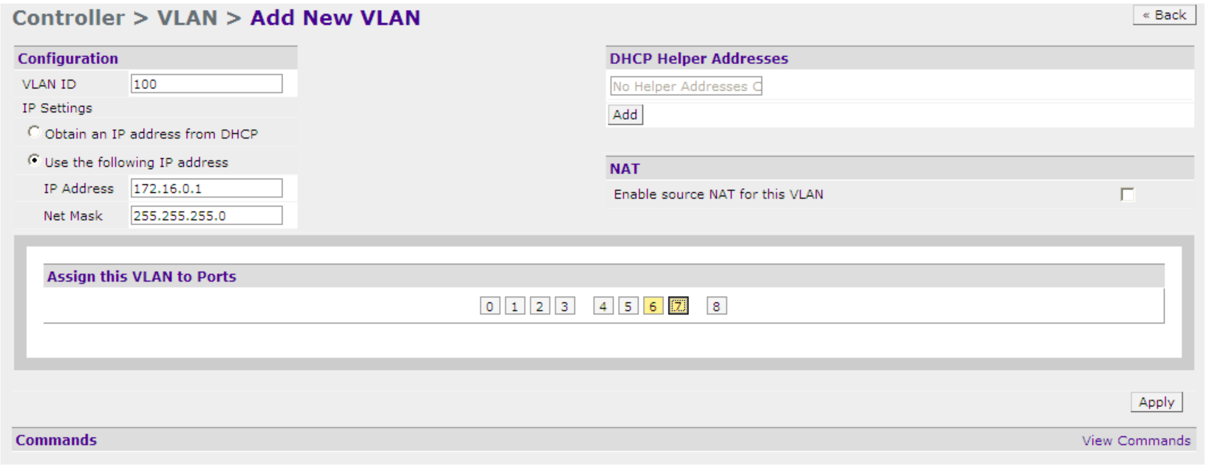
Enable source NAT for this VLAN □

Assign this VLAN to Ports

0 1 2 3 4 [✓ 5] 6 7 8

Commands

The example shows how to create VLAN 100 and configure Port 0/6 and 0/7 to be part of the VLAN.



Controller > VLAN > Add New VLAN

Configuration

VLAN ID: 100

IP Settings

○ Obtain an IP address from DHCP

● Use the following IP address

IP Address: 172.16.0.1

Net Mask: 255.255.255.0

DHCP Helper Addresses

No Helper Addresses C

NAT

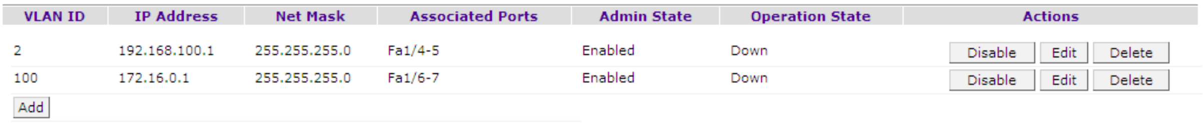
Enable source NAT for this VLAN □

Assign this VLAN to Ports

0 1 2 3 4 5 [✓ 6] [✓ 7] 8

Commands

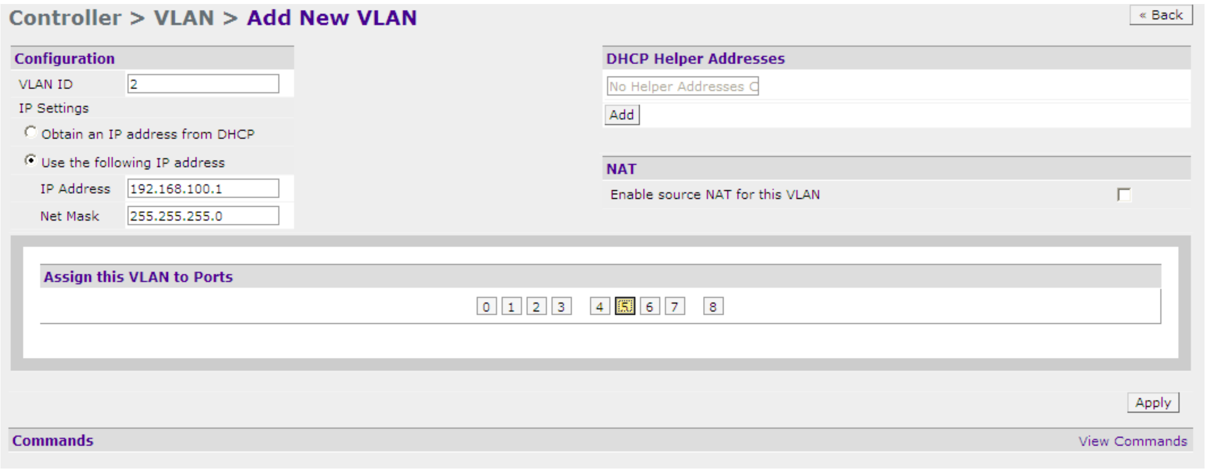
The result after apply the changes to both VLANs will be the following:



VLAN ID	IP Address	Net Mask	Associated Ports	Admin State	Operation State	Actions
2	192.168.100.1	255.255.255.0	Fa1/4-5	Enabled	Down	Disable Edit Delete
100	172.16.0.1	255.255.255.0	Fa1/6-7	Enabled	Down	Disable Edit Delete

This confirms the IP address assigned to the VLAN interface, what ports are members of the VLAN and whether the Admin state is enabled or not.

In our scenario VLAN 2 will be created and port 5 associated to it, and the IP address assigned as 192.168.100.1



Controller > VLAN > Add New VLAN

Configuration

VLAN ID 2

IP Settings

○ Obtain an IP address from DHCP

● Use the following IP address

IP Address 192.168.100.1

Net Mask 255.255.255.0

DHCP Helper Addresses

No Helper Addresses C

NAT

Enable source NAT for this VLAN □

Assign this VLAN to Ports

0 1 2 3 4 [✓ 5] 6 7 8

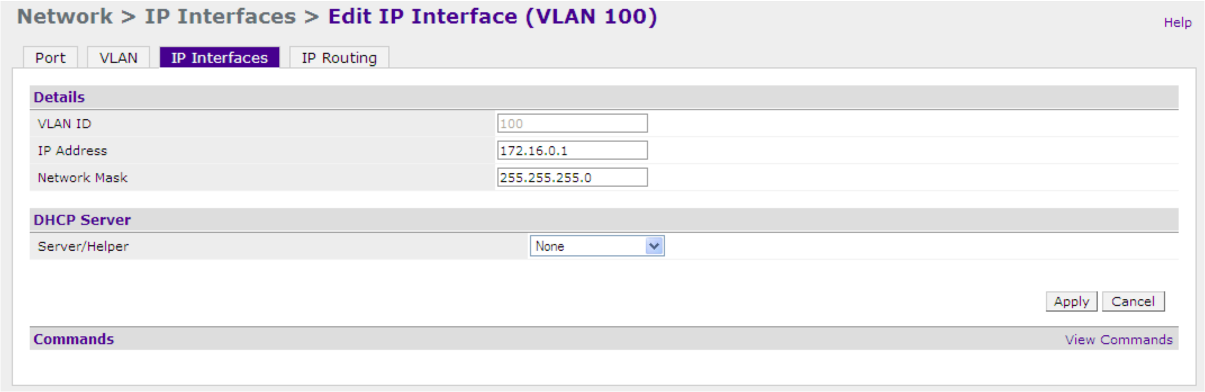
Commands

Configure the IP address (IP Interface of a VLAN) and Enable it

To configure the IP interface of a VLAN – access the menu at Configuration – Basic – Network – IP Interfaces.

Edit the VLAN in question and configure the VLAN IP address and Subnet mask according to the requirements.

This procedure may be used if the IP interface address of the VLAN is not being setup during the VLAN creation.



Network > IP Interfaces > Edit IP Interface (VLAN 100)

Details

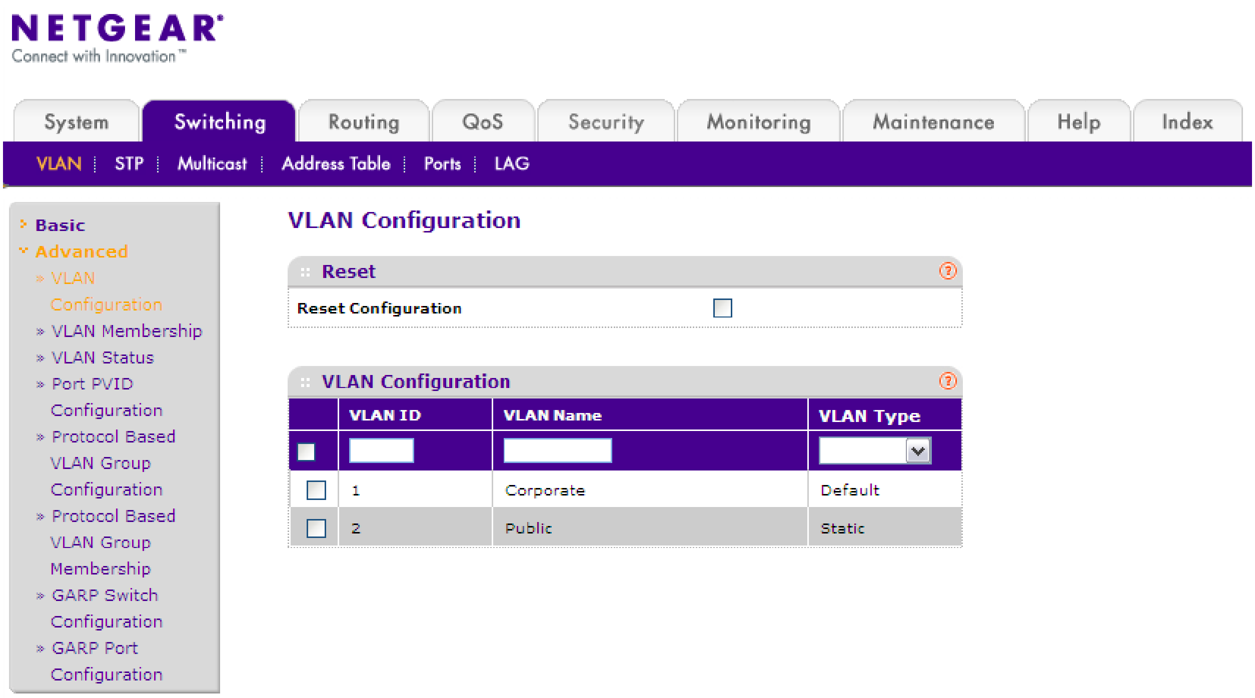
VLAN ID	100
IP Address	172.16.0.1
Network Mask	255.255.255.0

DHCP Server

Server/Helper	None

Configure trunk port on L2/L3 Switch

Rename VLAN1 to Corporate (for reference). Create VLAN2 called Public.



VLAN Configuration

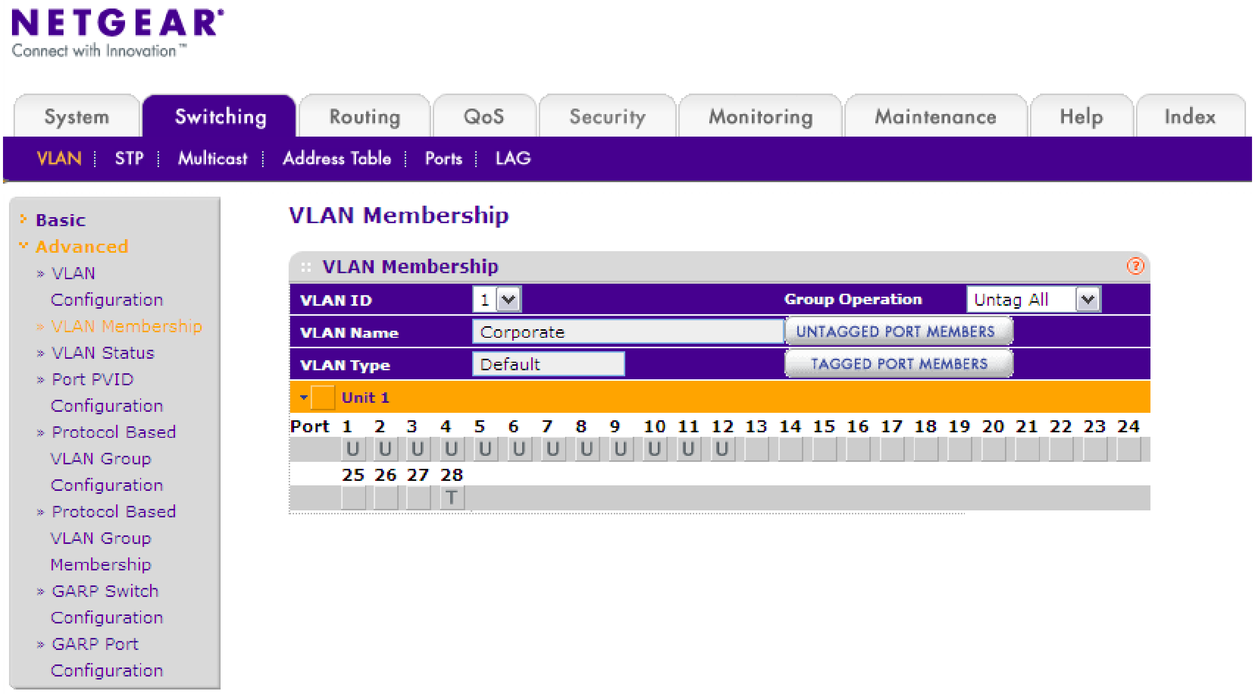
Reset

Reset Configuration □

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type
□			
□	1	Corporate	Default
□	2	Public	Static

Add ports 1 to 12 untagged to VLAN1. Add port 28 tagged to VLAN1.



VLAN Membership

VLAN Membership

VLAN ID 1 Group Operation Untag All

VLAN Name Corporate

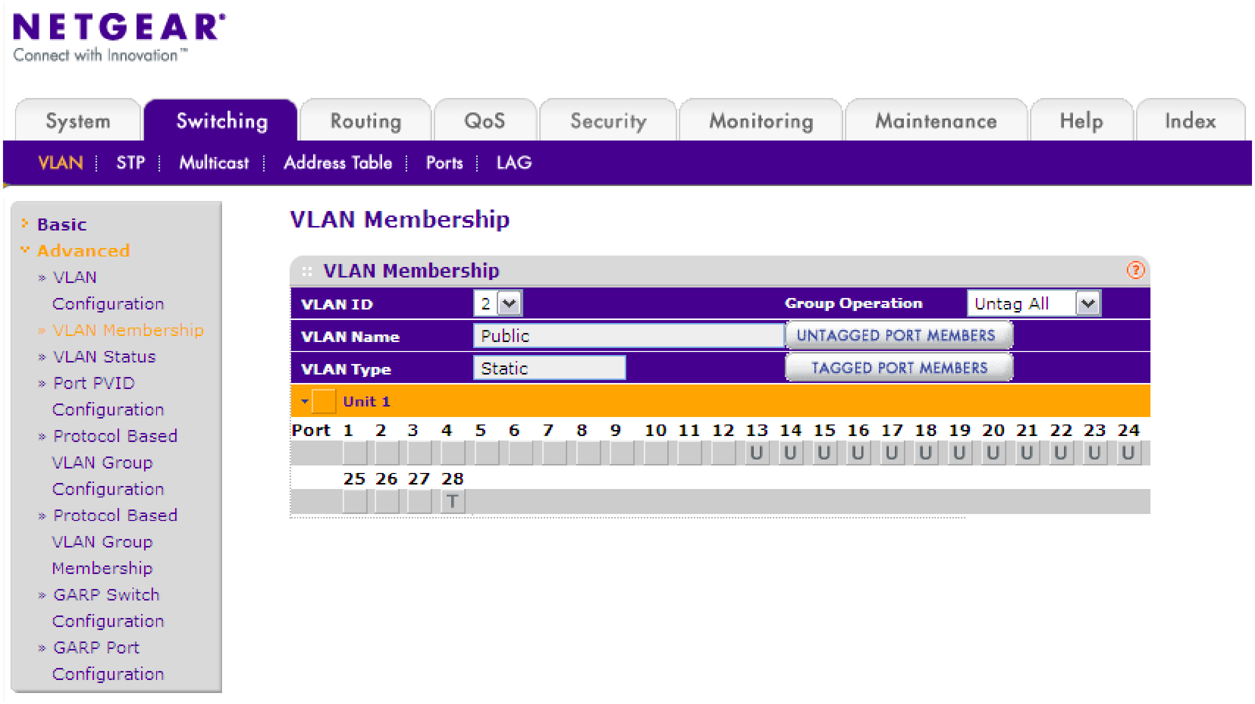
VLAN Type Default

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	U	U	U	U	U	U	U	U	U	U	U	U												

	25	26	27	28
				T

Add ports 13 to 24 untagged to VLAN2. Add port 28 tagged to VLAN2.



VLAN Membership

VLAN Membership

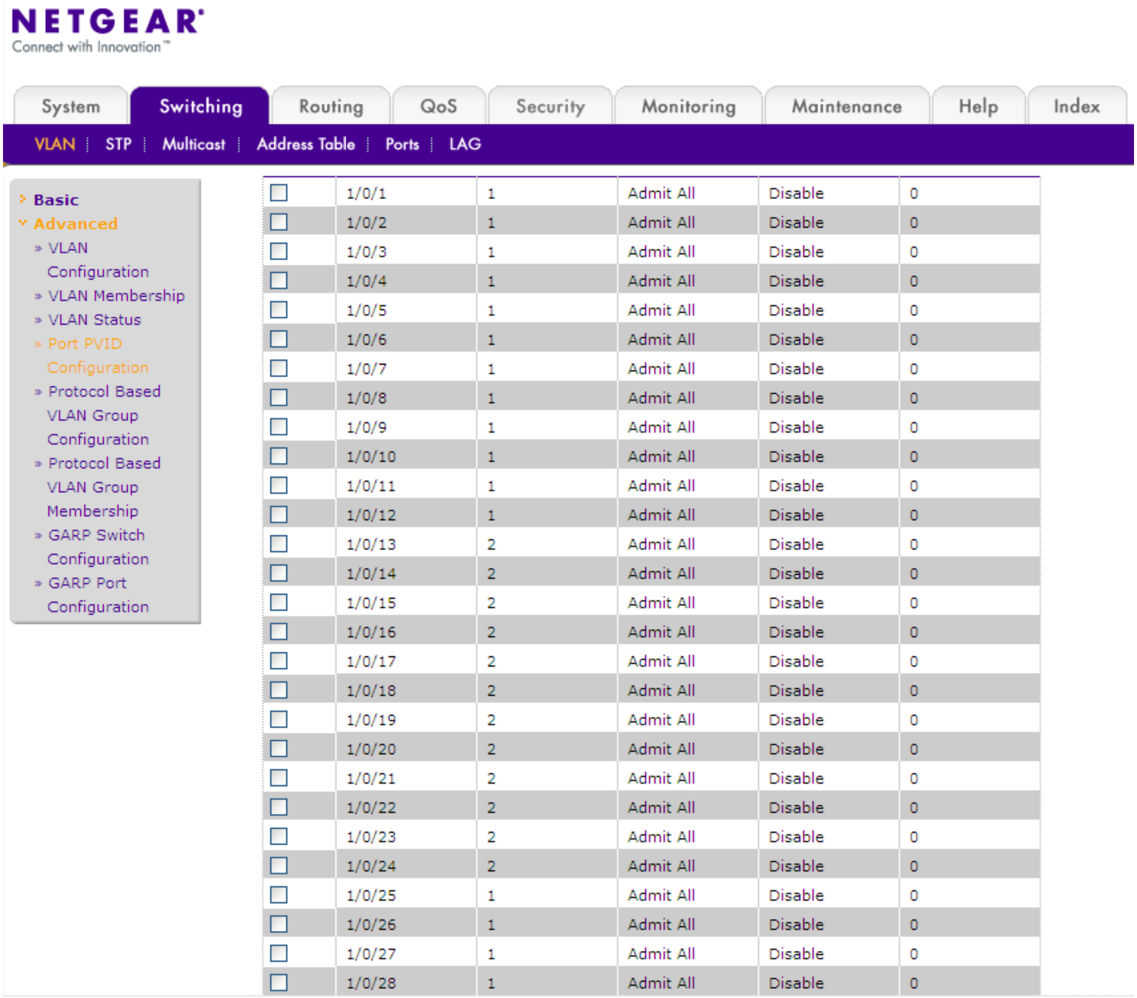
VLAN ID	2	Group Operation	Untag All
VLAN Name	Public	UNTAGGED PORT MEMBERS	
VLAN Type	Static	TAGGED PORT MEMBERS	

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
													U	U	U	U	U	U	U	U	U	U	U	U

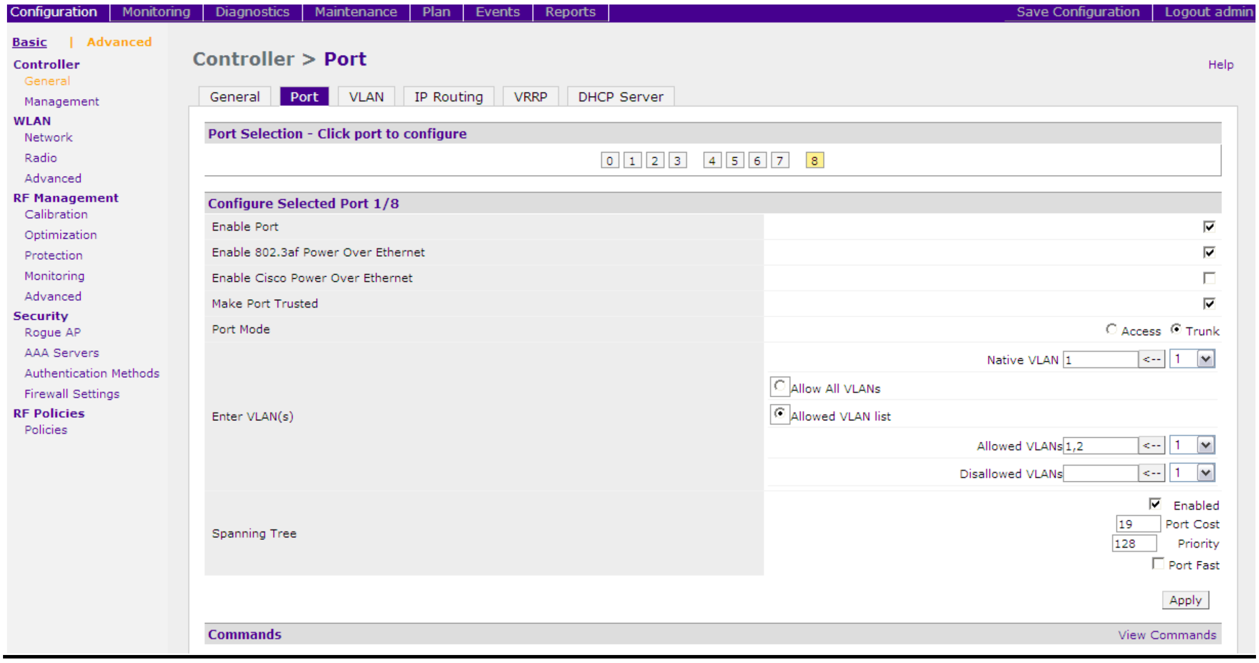
	25	26	27	28
				T

Configure PVID settings – ports 1 to 12 with PVID of 1, ports 13 to 24 with PVID of 2. PVID on trunk port (port 28) is not relevant.



□	1/0/1	1	Admit All	Disable	0
□	1/0/2	1	Admit All	Disable	0
□	1/0/3	1	Admit All	Disable	0
□	1/0/4	1	Admit All	Disable	0
□	1/0/5	1	Admit All	Disable	0
□	1/0/6	1	Admit All	Disable	0
□	1/0/7	1	Admit All	Disable	0
□	1/0/8	1	Admit All	Disable	0
□	1/0/9	1	Admit All	Disable	0
□	1/0/10	1	Admit All	Disable	0
□	1/0/11	1	Admit All	Disable	0
□	1/0/12	1	Admit All	Disable	0
□	1/0/13	2	Admit All	Disable	0
□	1/0/14	2	Admit All	Disable	0
□	1/0/15	2	Admit All	Disable	0
□	1/0/16	2	Admit All	Disable	0
□	1/0/17	2	Admit All	Disable	0
□	1/0/18	2	Admit All	Disable	0
□	1/0/19	2	Admit All	Disable	0
□	1/0/20	2	Admit All	Disable	0
□	1/0/21	2	Admit All	Disable	0
□	1/0/22	2	Admit All	Disable	0
□	1/0/23	2	Admit All	Disable	0
□	1/0/24	2	Admit All	Disable	0
□	1/0/25	1	Admit All	Disable	0
□	1/0/26	1	Admit All	Disable	0
□	1/0/27	1	Admit All	Disable	0
□	1/0/28	1	Admit All	Disable	0

WFS709TP trunk port configuration



Controller > Port

Port Selection - Click port to configure

Configure Selected Port 1/8

Enable Port	☑
Enable 802.3af Power Over Ethernet	☑
Enable Cisco Power Over Ethernet	□
Make Port Trusted	☑
Port Mode	○ Access ● Trunk
Enter VLAN(s)	Native VLAN 1 <-- 1 ○ Allow All VLANs ● Allowed VLAN list Allowed VLANs 1,2 <-- 1 Disallowed VLANs <-- 1
Spanning Tree	☑ Enabled 19 Port Cost 128 Priority □ Port Fast

Commands

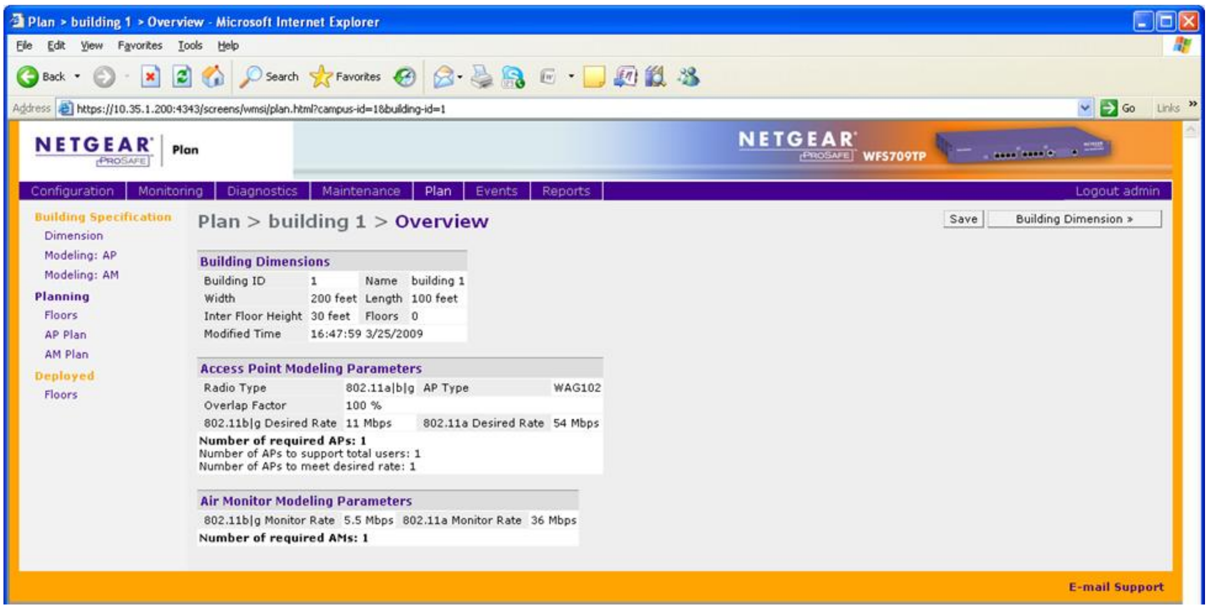
Performed testing

- Connect WFS709TP on gigabit port to FSM7328PS on port 28
- Connect PC to port 1 on FSM7328PS (VLAN1)
- PC obtains IP address from DHCP server on WFS709TP in the range 10.35.1.0/24
- Connect laptop wirelessly to ‘Corporate’ SSID
- Laptop obtains IP address from DHCP server on WFS709TP in the range 10.35.1.0/24
- Verify that PC can ping laptop and vice versa

Section 2 - RF Plan & provisioning Access Points

1. Starting position for this exercise: Any previously provisioned AP's were reset to factory defaults and disconnected from the WFS, any previously existing buildings were deleted, old entries were cleared from WFS database. Configuration was saved and WFS was rebooted.

2. Click on "Plan". The following screen appears, with the default building setup which is to be customised. Click "Building Dimension".


Plan > building 1 > Overview - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.35.1.200:4343/screens/wmsi/plan.html?campus-id=1&building-id=1
Go Links
NETGEAR PROSAFE Plan
NETGEAR PROSAFE WFS709TP
Configuration Monitoring Diagnostics Maintenance Plan Events Reports Logout admin
Building Specification
Dimension
Modeling: AP
Modeling: AM
Planning
Floors
AP Plan
AM Plan
Deployed
Floors
Save
Building Dimension »
E-mail Support

Plan > building 1 > Overview

Building Dimensions

Building ID	1	Name	building 1
Width	200 feet	Length	100 feet
Inter Floor Height	30 feet	Floors	0
Modified Time	16:47:59 3/25/2009		

Access Point Modeling Parameters

Radio Type	802.11a|b|g	AP Type	WAG102
Overlap Factor	100 %		
802.11b|g Desired Rate	11 Mbps	802.11a Desired Rate	54 Mbps

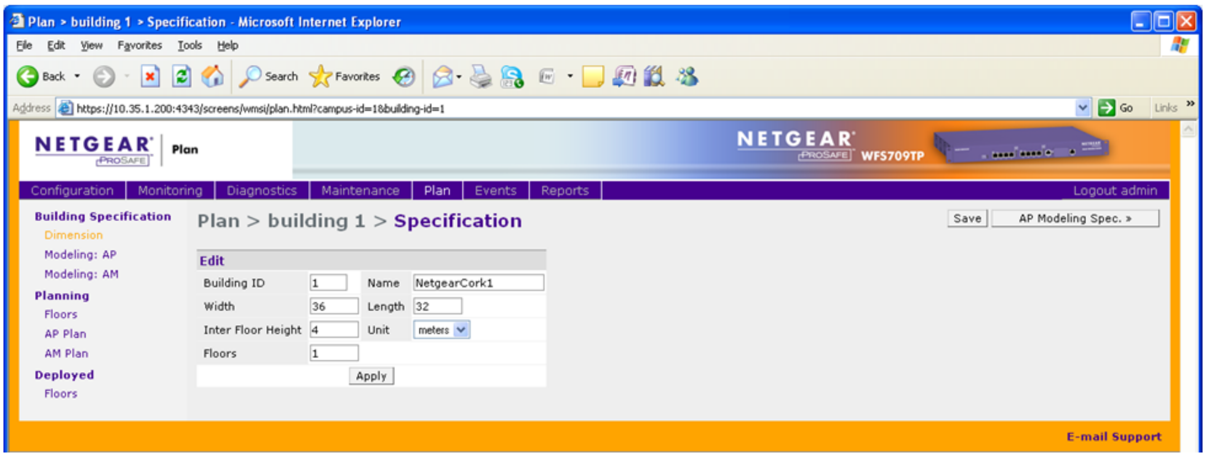
Number of required APs: 1
Number of APs to support total users: 1
Number of APs to meet desired rate: 1

Air Monitor Modeling Parameters

802.11b|g Monitor Rate	5.5 Mbps	802.11a Monitor Rate	36 Mbps

Number of required AMs: 1

3. On this screen, select "Unit" as Feet or Metres, and fill in the rest of the details. In this example, the RF plan is only for the top floor of a 2-floor building, so "Floors" =1. Note that the dimensions are for the full area covered by the floorplan .jpg that will be loaded at a later step, which may be slightly larger than the area covered by the physical building. Click "Apply", then "AP Modelling Spec".

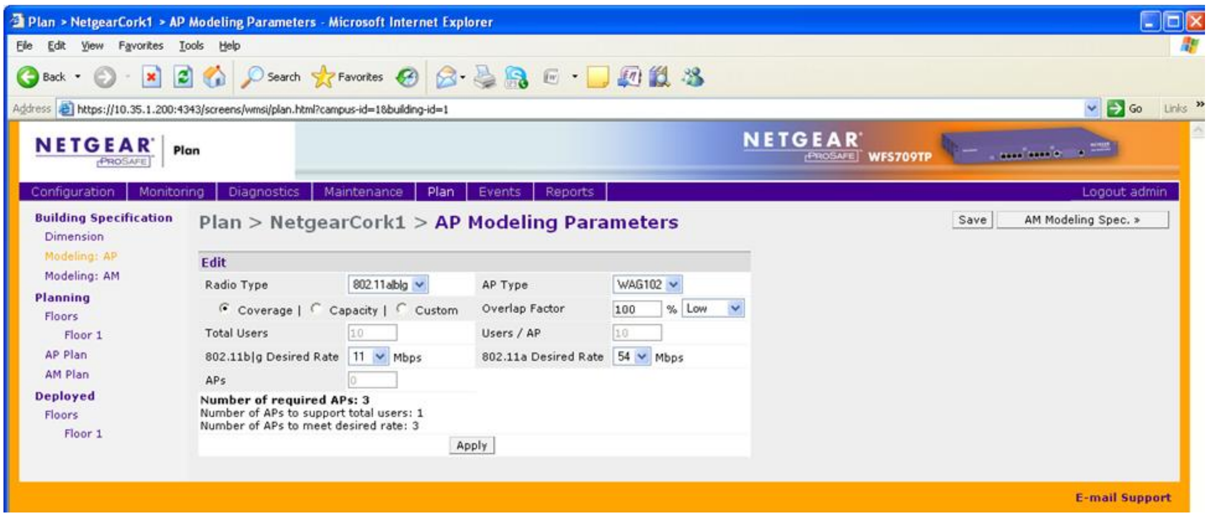

Plan > building 1 > Specification - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.35.1.200:4343/screens/wmsi/plan.html?campus-id=1&building-id=1
Go Links
NETGEAR PROSAFE Plan
NETGEAR PROSAFE WFS709TP
Configuration Monitoring Diagnostics Maintenance Plan Events Reports Logout admin
Building Specification
Dimension
Modeling: AP
Modeling: AM
Planning
Floors
AP Plan
AM Plan
Deployed
Floors
Save
AP Modeling Spec. »
Apply
E-mail Support

Plan > building 1 > Specification

Edit

Building ID	1	Name	NetgearCork1
Width	36	Length	32
Inter Floor Height	4	Unit	meters
Floors	1		

4. This screen shows the default Access Point parameters.



Plan > NetgearCork1 > AP Modeling Parameters - Microsoft Internet Explorer

Address: https://10.35.1.200:4343/screens/wmsi/plan.html?campus-id=1&building-id=1

Plan

Plan > NetgearCork1 > AP Modeling Parameters

Save | AM Modeling Spec. »

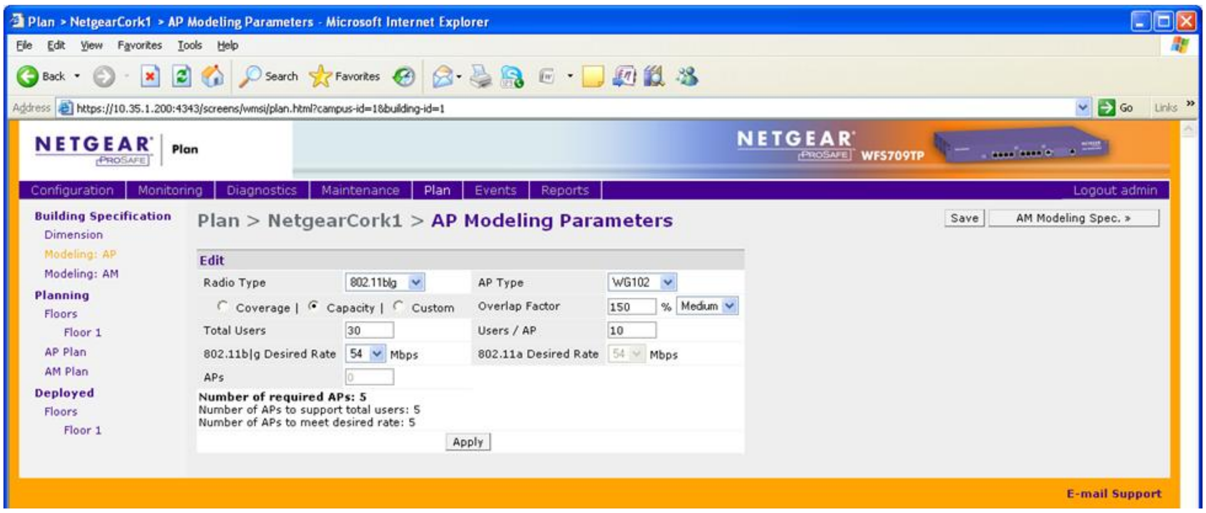
Edit

Radio Type	802.11a|b|g	AP Type	WAG102
● Coverage | ○ Capacity | ○ Custom		Overlap Factor	100 % Low
Total Users	10	Users / AP	10
802.11b|g Desired Rate	11 Mbps	802.11a Desired Rate	54 Mbps
APs	0		

Number of required APs: 3
Number of APs to support total users: 1
Number of APs to meet desired rate: 3

Apply

5. Edit the default AP parameters as required. “Coverage” will calculate required number and location of APs based on the area to be covered, while “Capacity” will calculate this based on number of users to be supported. 100% Overlap Factor indicates that the AP coverage areas should just touch, increasing this parameter will make roaming more reliable. The parameters specified on this screen will determine how many APs are required. Click “Apply”, then “AM Modelling Spec.”.



Plan > NetgearCork1 > AP Modeling Parameters - Microsoft Internet Explorer

Address: https://10.35.1.200:4343/screens/wmsi/plan.html?campus-id=1&building-id=1

Plan

Plan > NetgearCork1 > AP Modeling Parameters

Save | AM Modeling Spec. »

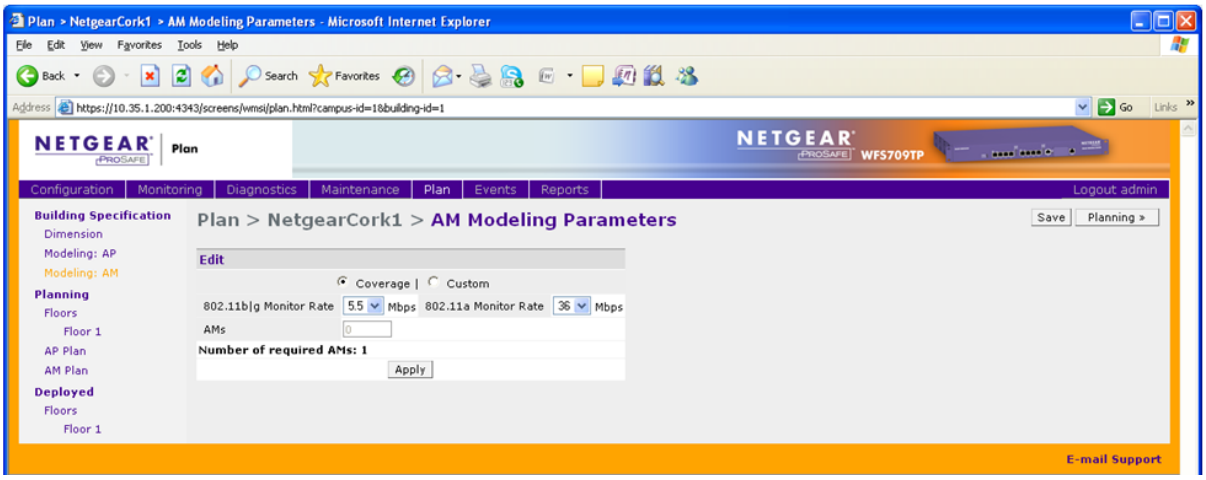
Edit

Radio Type	802.11b|g	AP Type	WG102
○ Coverage | ● Capacity | ○ Custom		Overlap Factor	150 % Medium
Total Users	30	Users / AP	10
802.11b|g Desired Rate	54 Mbps	802.11a Desired Rate	54 Mbps
APs	0		

Number of required APs: 5
Number of APs to support total users: 5
Number of APs to meet desired rate: 5

Apply

6. The Air Monitor Modelling Parameter screen determines how many AMs will be required. In most cases, default settings will be suitable. Click “Apply”, the “Save”, then “Planning”.



Plan > NetgearCork1 > AM Modeling Parameters - Microsoft Internet Explorer

Address: https://10.35.1.200:4343/screens/wmsi/plan.html?campus-id=1&building-id=1

Plan

Plan > NetgearCork1 > AM Modeling Parameters

Save | Planning »

Edit

● Coverage | ○ Custom

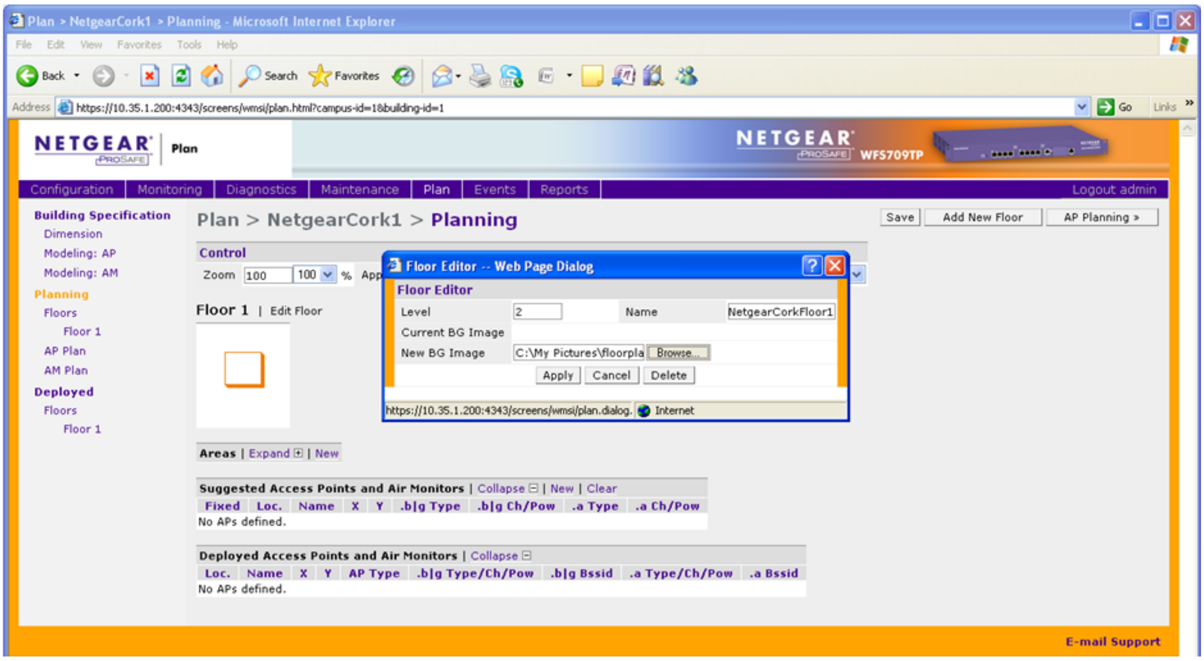
802.11b|g Monitor Rate	5.5 Mbps	802.11a Monitor Rate	36 Mbps
AMs	0		

Number of required AMs: 1

Apply

7. On the Planning screen, click “Add New Floor”.

8. Fill in “Level” and “Name” text boxes, and browse to a .JPG image of the floorplan of the floor to be added. Click “Apply”.



Plan > NetgearCork1 > Planning - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.35.1.200:4343/screens/wmsi/plan.html?campus-id=1&building-id=1
Go Links
NETGEAR ProSafe Plan
NETGEAR ProSafe WFS709TP
Configuration Monitoring Diagnostics Maintenance Plan Events Reports Logout admin
Building Specification
Dimension
Modeling: AP
Modeling: AM
Planning
Floors
Floor 1
AP Plan
AM Plan
Deployed
Floors
Floor 1
Save Add New Floor AP Planning »
Floor Editor -- Web Page Dialog
Browse...
Apply Cancel Delete
https://10.35.1.200:4343/screens/wmsi/plan.dialog. Internet
E-mail Support

Plan > NetgearCork1 > Planning

Control

Zoom 100 100 % App

Floor 1 | Edit Floor

Floor Editor

Level	2	Name	NetgearCorkFloor1
Current BG Image			
New BG Image	C:\My Pictures\floorpla		

Areas | Expand ⊞ | New

Suggested Access Points and Air Monitors | Collapse ⊟ | New | Clear

Fixed	Loc.	Name	X	Y	.b|g Type	.b|g Ch/Pow	.a Type	.a Ch/Pow

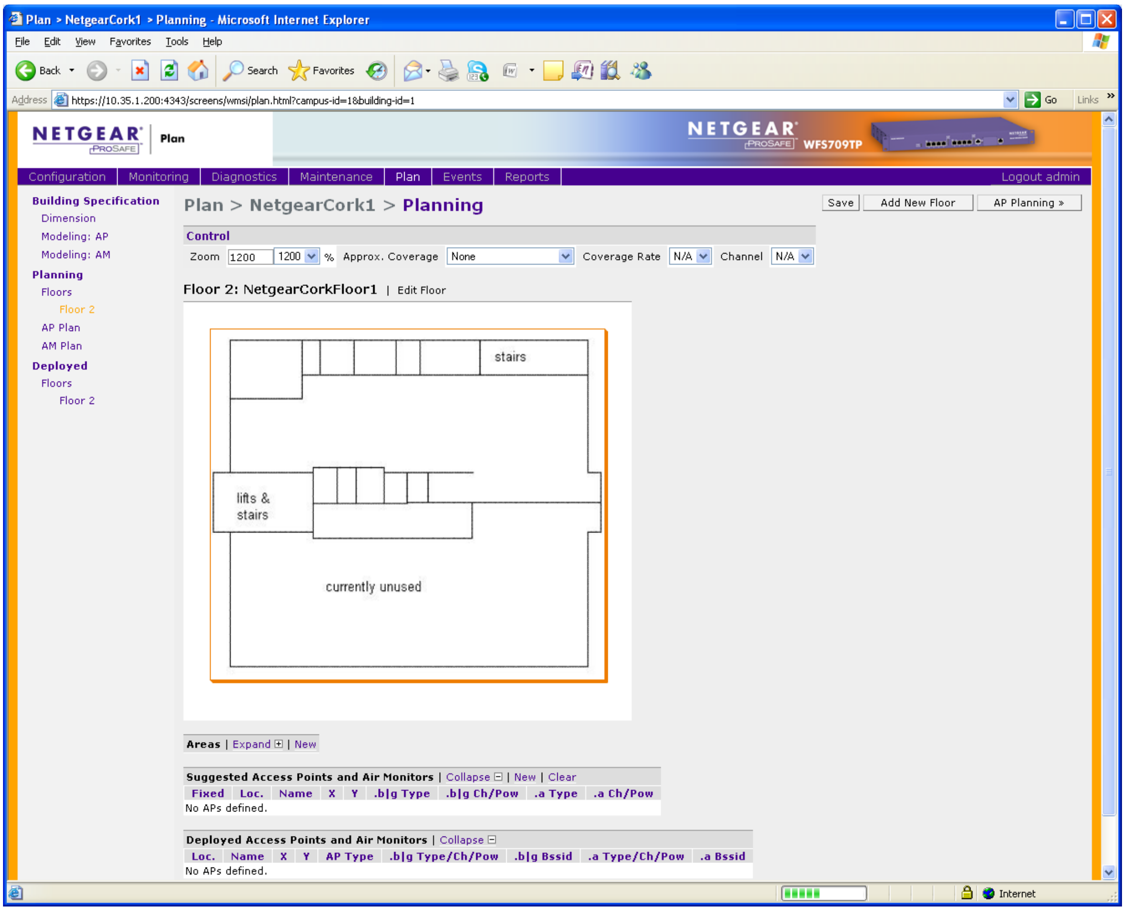
No APs defined.

Deployed Access Points and Air Monitors | Collapse ⊟

Loc.	Name	X	Y	AP Type	.b|g Type/Ch/Pow	.b|g Bssid	.a Type/Ch/Pow	.a Bssid

No APs defined.

9. Adjust “Zoom” value to adjust the size of the image for comfortable viewing.



Plan > NetgearCork1 > Planning - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.35.1.200:4343/screens/wmsi/plan.html?campus-id=1&building-id=1
Go Links
NETGEAR ProSafe Plan
NETGEAR ProSafe WFS709TP
Configuration Monitoring Diagnostics Maintenance Plan Events Reports Logout admin
Building Specification
Dimension
Modeling: AP
Modeling: AM
Planning
Floors
Floor 2
AP Plan
AM Plan
Deployed
Floors
Floor 2
Save Add New Floor AP Planning »
stairs
lifts & stairs
currently unused
Internet

Plan > NetgearCork1 > Planning

Control

Zoom 1200 1200 % Approx. Coverage None Coverage Rate N/A Channel N/A

Floor 2: NetgearCorkFloor1 | Edit Floor

Areas | Expand ⊞ | New

Suggested Access Points and Air Monitors | Collapse ⊟ | New | Clear

Fixed	Loc.	Name	X	Y	.b|g Type	.b|g Ch/Pow	.a Type	.a Ch/Pow

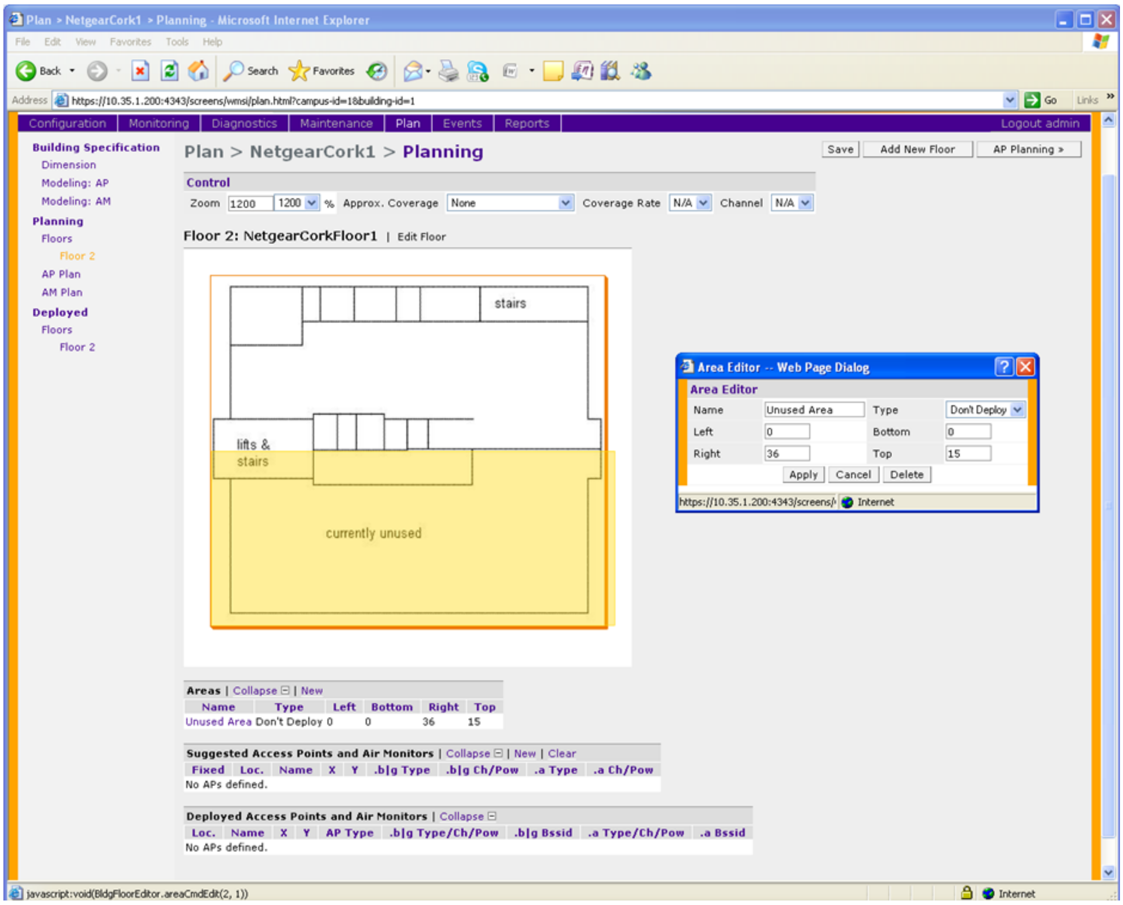
No APs defined.

Deployed Access Points and Air Monitors | Collapse ⊟

Loc.	Name	X	Y	AP Type	.b|g Type/Ch/Pow	.b|g Bssid	.a Type/Ch/Pow	.a Bssid

No APs defined.

10. If there are any areas on the floorplan where coverage is not required or is optional, click "New" in the "Areas" menu. In the Area Editor, specify coordinates to indicate the area where coverage is not required, select "Don't Deploy" or "Don't Care", and click "Apply".


Plan > NetgearCork1 > Planning - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.35.1.200:4343/screens/wmsi/plan.html?campus-id=1&building-id=1
Go Links
Configuration Monitoring Diagnostics Maintenance Plan Events Reports
Logout admin
Building Specification
Dimension
Modeling: AP
Modeling: AM
Planning
Floors
Floor 2
AP Plan
AM Plan
Deployed
Floors
Floor 2
Save
Add New Floor
AP Planning »
stairs
lifts &
stairs
currently unused

Plan > NetgearCork1 > Planning

Control

Zoom 1200 1200 % Approx. Coverage None Coverage Rate N/A Channel N/A

Floor 2: NetgearCorkFloor1 | Edit Floor

Area Editor -- Web Page Dialog

Area Editor

Name	Unused Area	Type	Don't Deploy
Left	0	Bottom	0
Right	36	Top	15

Apply Cancel Delete

https://10.35.1.200:4343/screens/ Internet

Areas | Collapse ⊟ | New

Name	Type	Left	Bottom	Right	Top
Unused Area	Don't Deploy	0	0	36	15

Suggested Access Points and Air Monitors | Collapse ⊟ | New | Clear

Fixed	Loc.	Name	X	Y	.b|g Type	.b|g Ch/Pow	.a Type	.a Ch/Pow

No APs defined.

Deployed Access Points and Air Monitors | Collapse ⊟

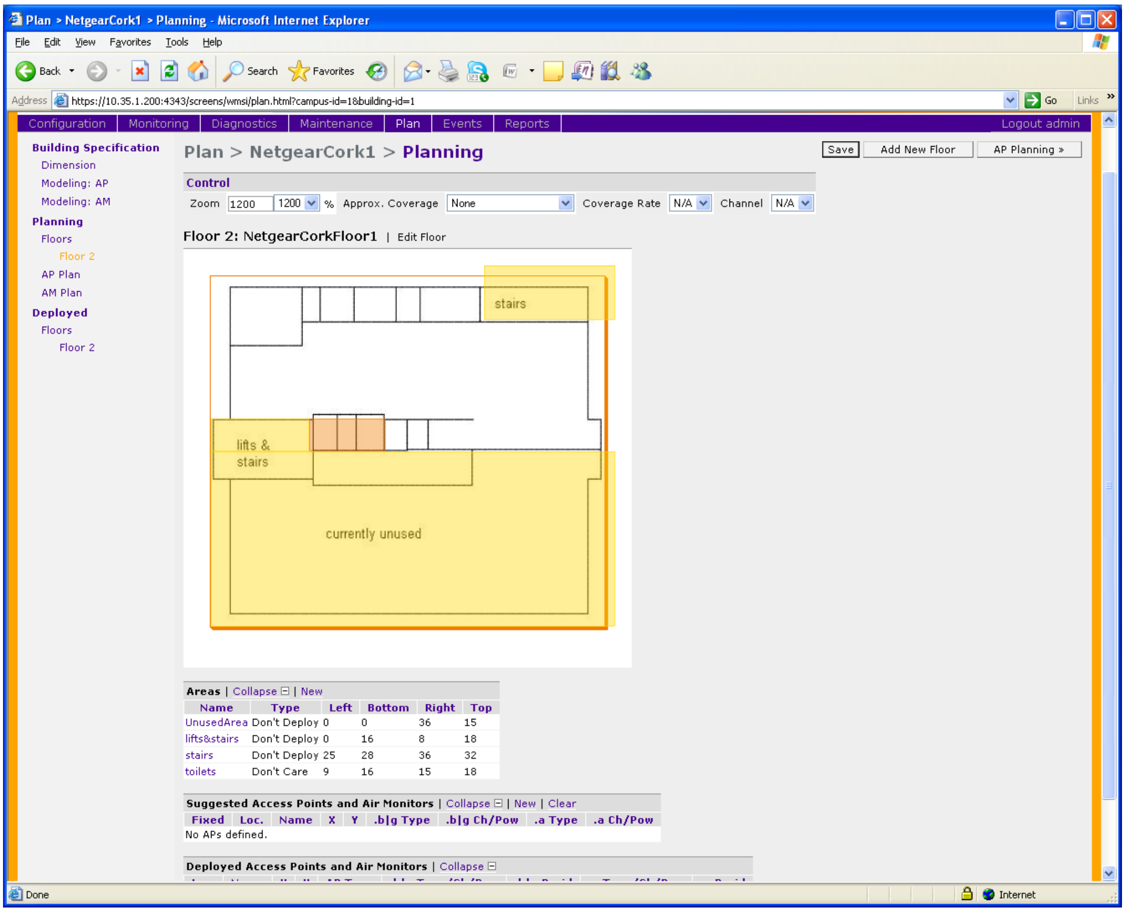
Loc.	Name	X	Y	AP Type	.b|g Type/Ch/Pow	.b|g Bssid	.a Type/Ch/Pow	.a Bssid

No APs defined.

javascript:void(BldgFloorEditor.areaCmdEdit(2, 1))

Internet

11. Repeat for each area on the floorplan where coverage is not required or is optional. Then click "Save", then "AP Planning".


Plan > NetgearCork1 > Planning - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.35.1.200:4343/screens/wmsi/plan.html?campus-id=1&building-id=1
Go Links
Configuration Monitoring Diagnostics Maintenance Plan Events Reports
Logout admin
Building Specification
Dimension
Modeling: AP
Modeling: AM
Planning
Floors
Floor 2
AP Plan
AM Plan
Deployed
Floors
Floor 2
Save
Add New Floor
AP Planning »
stairs
lifts &
stairs
currently unused

Plan > NetgearCork1 > Planning

Control

Zoom 1200 1200 % Approx. Coverage None Coverage Rate N/A Channel N/A

Floor 2: NetgearCorkFloor1 | Edit Floor

Areas | Collapse ⊟ | New

Name	Type	Left	Bottom	Right	Top
UnusedArea	Don't Deploy	0	0	36	15
lifts&stairs	Don't Deploy	0	16	8	18
stairs	Don't Deploy	25	28	36	32
toilets	Don't Care	9	16	15	18

Suggested Access Points and Air Monitors | Collapse ⊟ | New | Clear

Fixed	Loc.	Name	X	Y	.b|g Type	.b|g Ch/Pow	.a Type	.a Ch/Pow

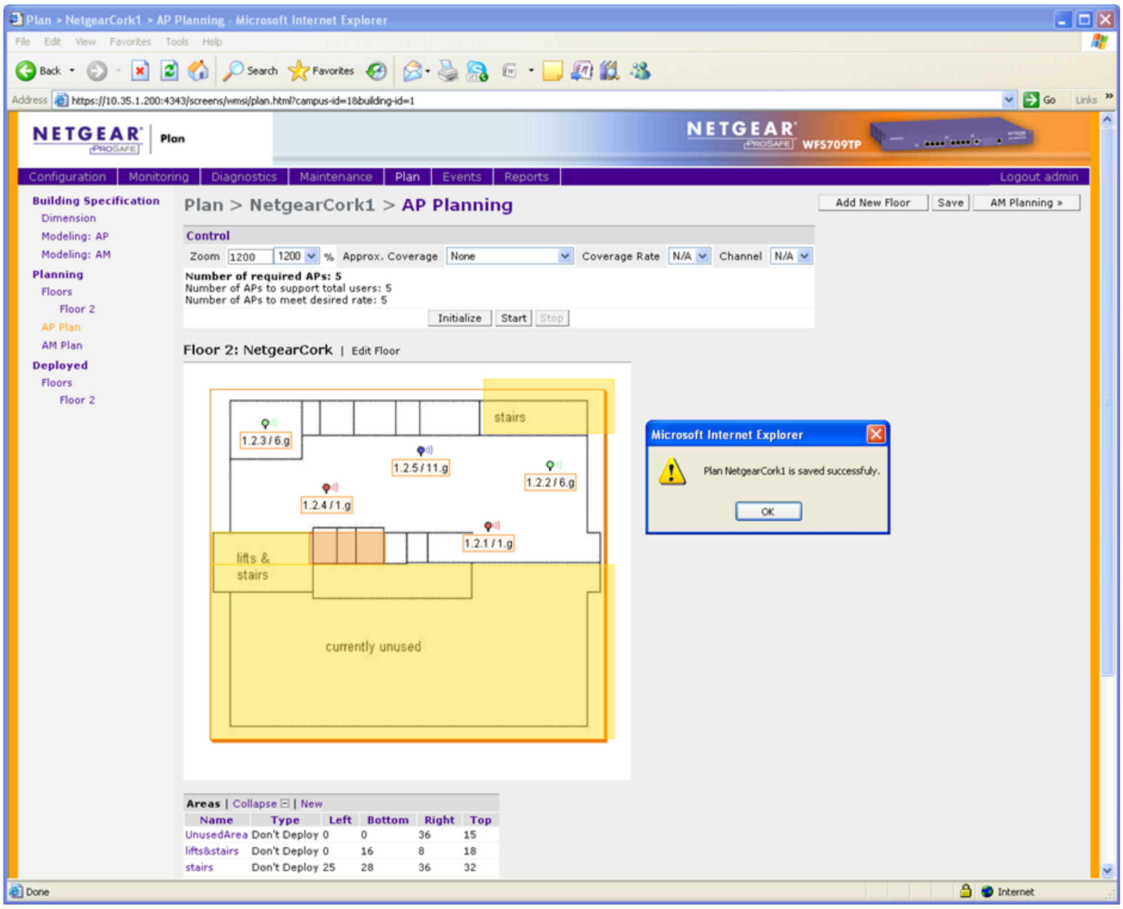
No APs defined.

Deployed Access Points and Air Monitors | Collapse ⊟

Done

Internet

12. Click “Initialize”. Access points will appear on the floorplan. Click “Start”. The software will adjust the position of the AP’s to optimize coverage. When it has finished, you can manually drag AP’s to improve coverage in high-use locations like conference rooms, or to specify the locations where AP’s will really be installed (or already are installed). It is important that this picture gives an accurate representation of where the APs are physically located relative to each other. Click “Save” then “AM Planning”.



Plan > NetgearCork1 > AP Planning

Control

Zoom 1200 1200 % Approx. Coverage None Coverage Rate N/A Channel N/A

Number of required APs: 5
Number of APs to support total users: 5
Number of APs to meet desired rate: 5

Floor 2: NetgearCork | Edit Floor

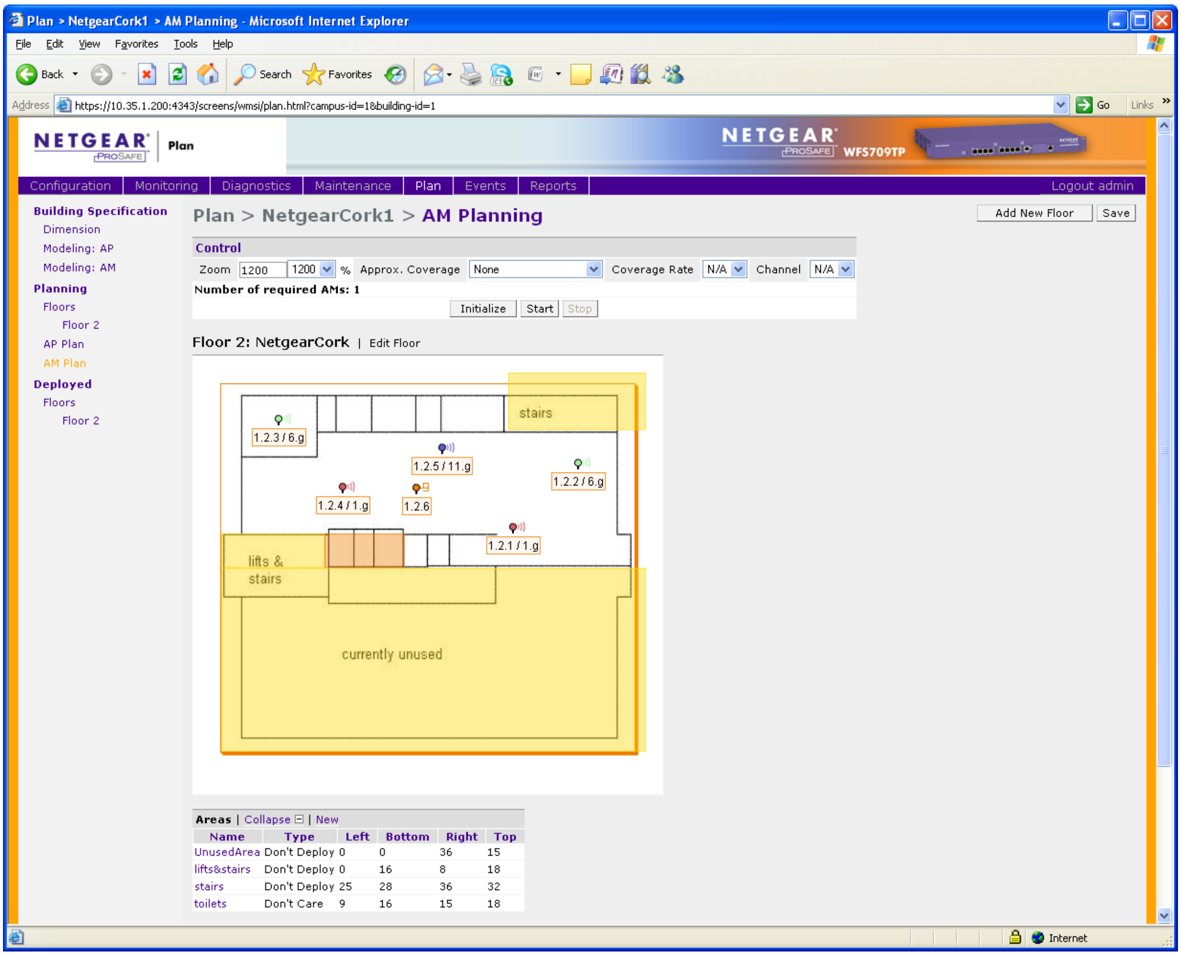
Microsoft Internet Explorer

Plan NetgearCork1 is saved successfuly.

Areas | Collapse | New

Name	Type	Left	Bottom	Right	Top
UnusedArea	Don't Deploy	0	0	36	15
lifts&stairs	Don't Deploy	0	16	8	18
stairs	Don't Deploy	25	28	36	32

13. Click “Initialize”. Air Monitor access point(s) will appear on the floorplan. Click “Start”. The software will adjust the position of the AM’s to optimize effectiveness. When it has finished, you can manually drag AM’s to specify the locations where AM’s will really be installed (or already are installed). It is important that this picture gives an accurate representation of where the AM’s are physically located relative to each other and the AP’s. Click “Save”. The RF plan is now complete. Make a note of the AP/AM location codes that have been generated by the RF Plan (1.2.1 to 1.2.6 in the screenshot).



https://10.35.1.200:4343/screens/wmsi/plan.html?campus-id=1&building-id=1

Plan > NetgearCork1 > AM Planning

Control

Zoom 1200 1200 % Approx. Coverage None Coverage Rate N/A Channel N/A

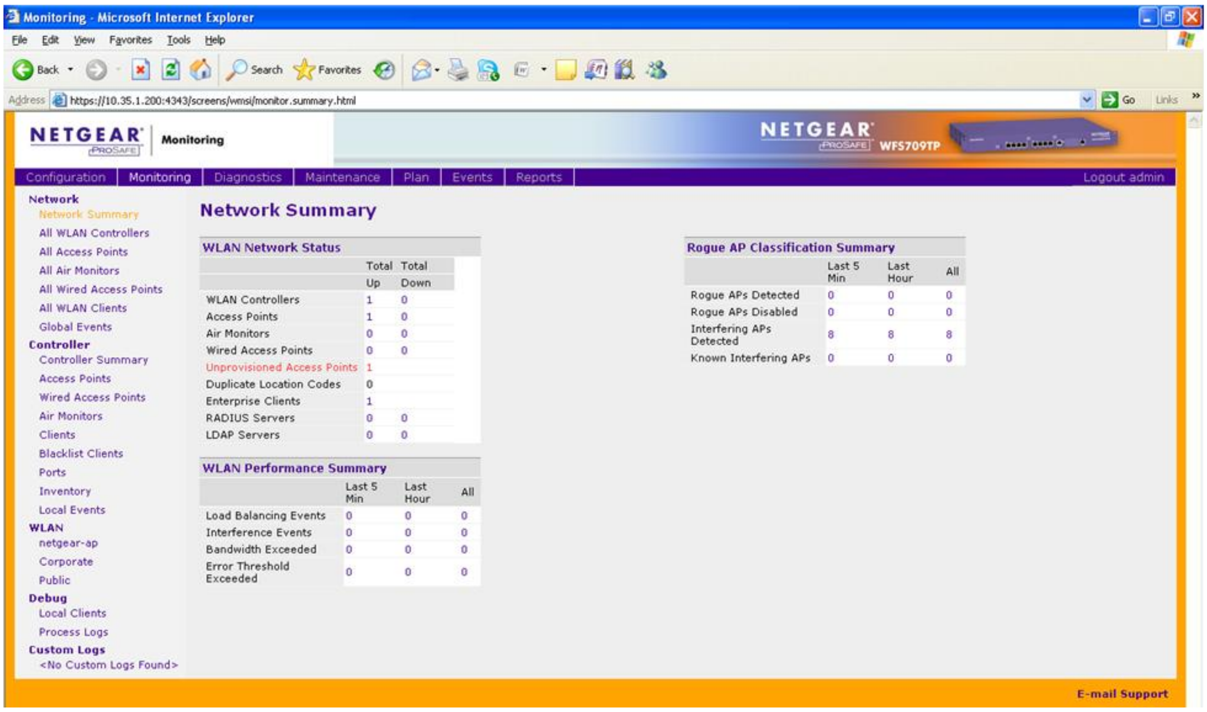
Number of required AMs: 1

Floor 2: NetgearCork | Edit Floor

Areas | Collapse ⊟ | New

Name	Type	Left	Bottom	Right	Top
UnusedArea	Don't Deploy	0	0	36	15
lifts&stairs	Don't Deploy	0	16	8	18
stairs	Don't Deploy	25	28	36	32
toilets	Don't Care	9	16	15	18

14. Connect an access point to the network. Click on “Monitoring” in the main menu, then “Network Summary”. Once the AP has established communication with the WFS, the “Unprovisioned Access Point ” counter will increment and turn red.



Network Summary

WLAN Network Status

	Total Up	Total Down
WLAN Controllers	1	0
Access Points	1	0
Air Monitors	0	0
Wired Access Points	0	0
Unprovisioned Access Points	1	
Duplicate Location Codes	0	
Enterprise Clients	1	
RADIUS Servers	0	0
LDAP Servers	0	0

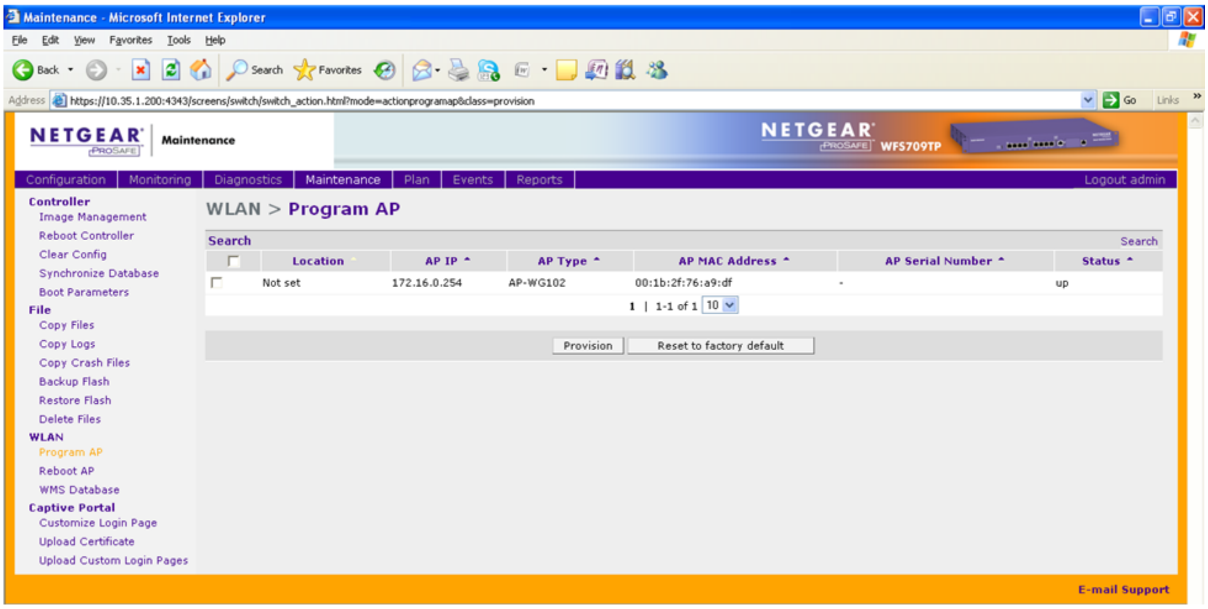
WLAN Performance Summary

	Last 5 Min	Last Hour	All
Load Balancing Events	0	0	0
Interference Events	0	0	0
Bandwidth Exceeded	0	0	0
Error Threshold Exceeded	0	0	0

Rogue AP Classification Summary

	Last 5 Min	Last Hour	All
Rogue APs Detected	0	0	0
Rogue APs Disabled	0	0	0
Interfering APs Detected	8	8	8
Known Interfering APs	0	0	0

15. Click “Maintenance”, then “Program AP”. Select an AP from the list whose Location is Not Set. Click “Provision”.



WLAN > Program AP

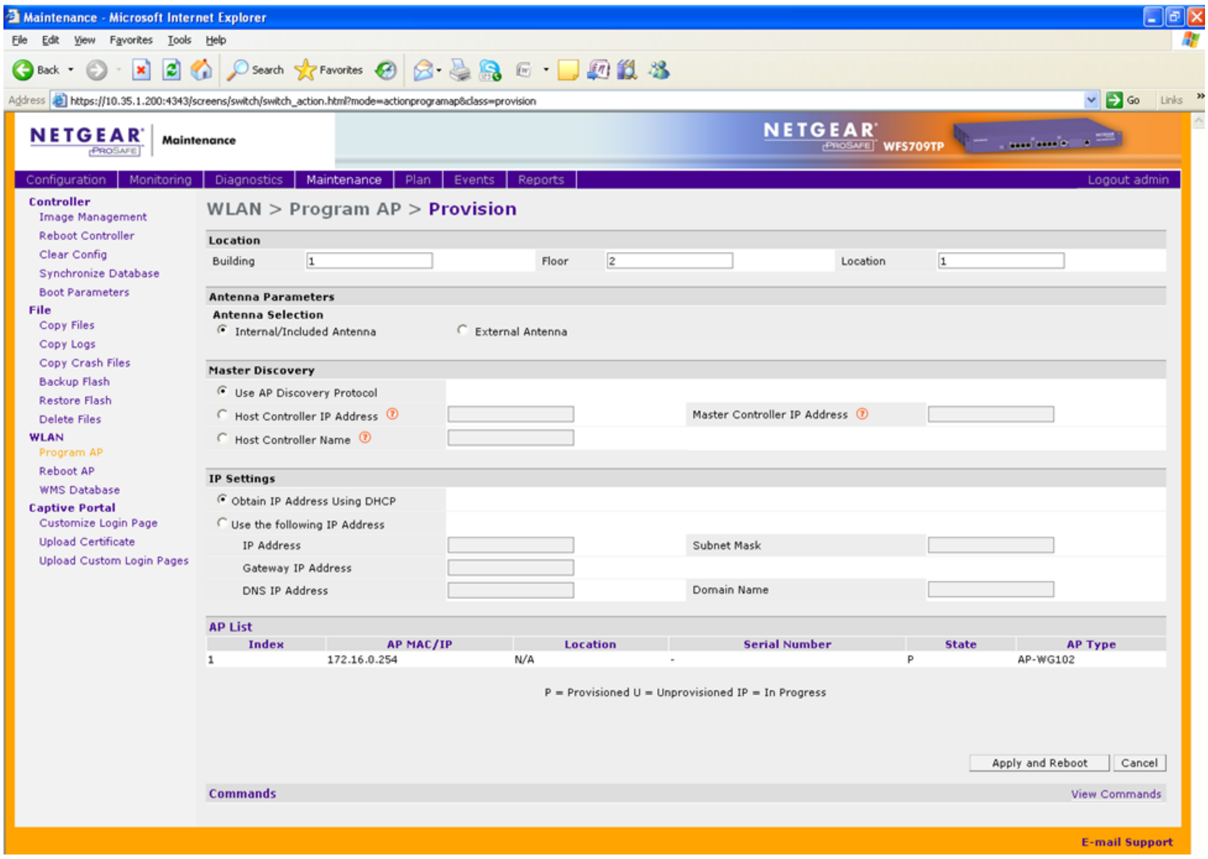
Search | Search

□	Location	AP IP	AP Type	AP MAC Address	AP Serial Number	Status
□	Not set	172.16.0.254	AP-WG102	00:1b:2f:76:a9:df	-	up

1 | 1-1 of 1 10

Provision | Reset to factory default

16. Enter one of the location codes generated in the RF Plan. Click “Apply and Reboot”.



WLAN > Program AP > Provision

Location

Building 1 Floor 2 Location 1

Antenna Parameters

Antenna Selection

● Internal/Included Antenna ○ External Antenna

Master Discovery

● Use AP Discovery Protocol

○ Host Controller IP Address Master Controller IP Address

○ Host Controller Name

IP Settings

● Obtain IP Address Using DHCP

○ Use the following IP Address

IP Address Subnet Mask

Gateway IP Address

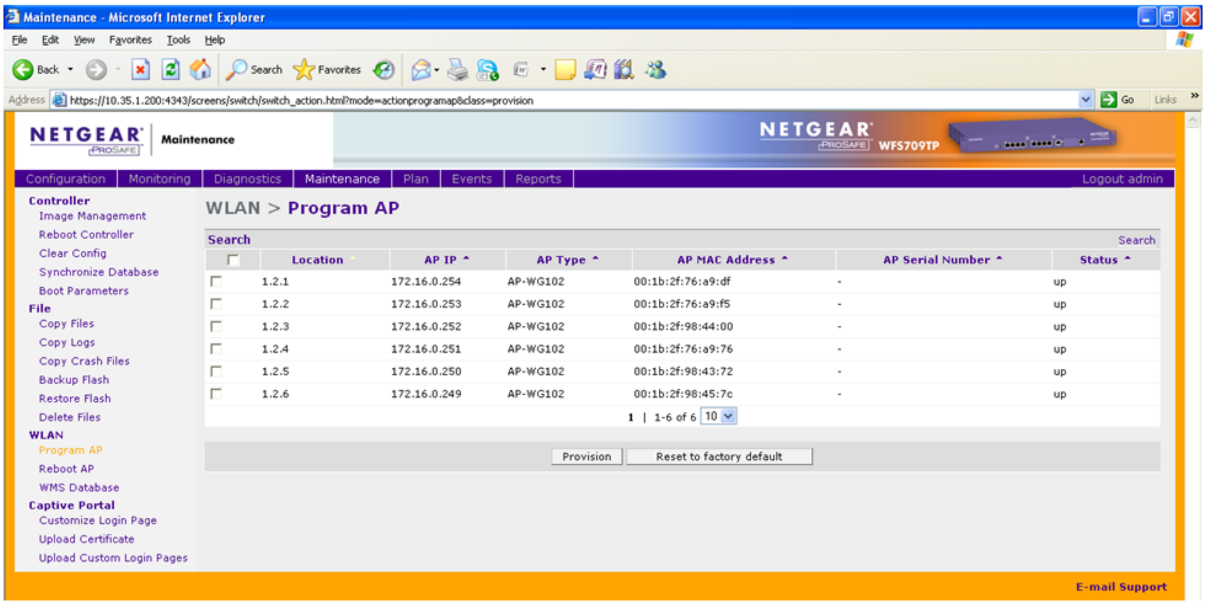
DNS IP Address Domain Name

AP List

Index	AP MAC/IP	Location	Serial Number	State	AP Type
1	172.16.0.254	N/A	-	P	AP-WG102

P = Provisioned U = Unprovisioned IP = In Progress

17. Connect the rest of the AP’s to the network, and provision them one at a time.



WLAN > Program AP

□	Location	AP IP	AP Type	AP MAC Address	AP Serial Number	Status
□	1.2.1	172.16.0.254	AP-WG102	00:1b:2f:76:a9:df	-	up
□	1.2.2	172.16.0.253	AP-WG102	00:1b:2f:76:a9:f5	-	up
□	1.2.3	172.16.0.252	AP-WG102	00:1b:2f:98:44:00	-	up
□	1.2.4	172.16.0.251	AP-WG102	00:1b:2f:76:a9:76	-	up
□	1.2.5	172.16.0.250	AP-WG102	00:1b:2f:98:43:72	-	up
□	1.2.6	172.16.0.249	AP-WG102	00:1b:2f:98:45:7c	-	up

1 | 1-6 of 6 10

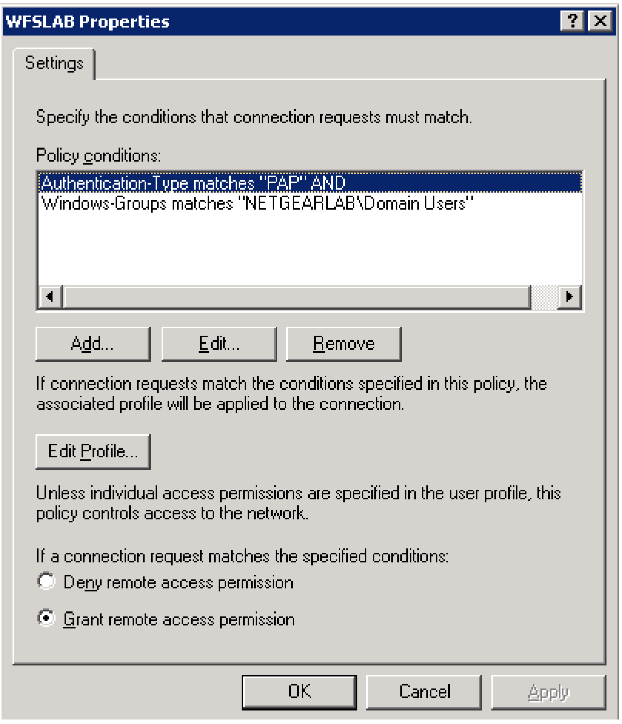
Section 3 – Captive Portal

IAS Server Configuration

First, we will create a Remote Access Policy and RADIUS Client in our IAS Server:

Remote Access policy:

Create a new Remote Access Policy in your IAS server, note that the authentication will be done by simple PAP.



WFSLAB Properties

Settings

Specify the conditions that connection requests must match.

Policy conditions:

Authentication-Type matches "PAP" AND
Windows-Groups matches "NETGEARLAB\Domain Users"

If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.

Unless individual access permissions are specified in the user profile, this policy controls access to the network.

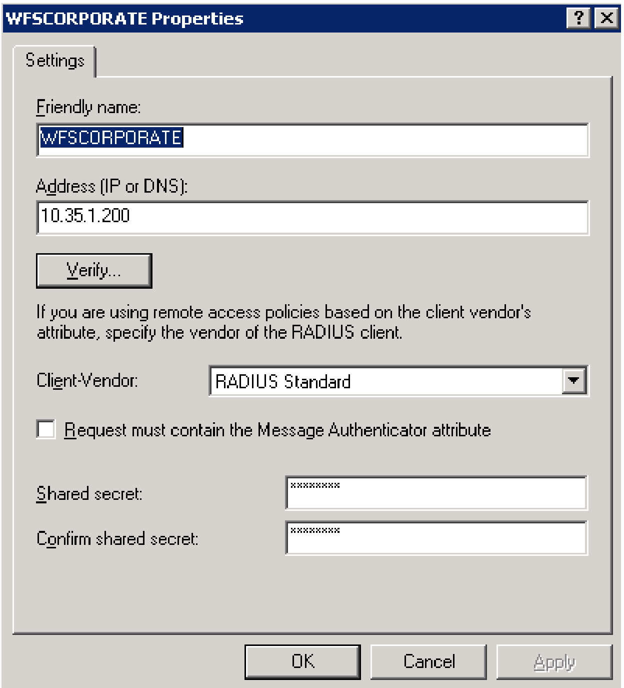
If a connection request matches the specified conditions:

○ Deny remote access permission

● Grant remote access permission

RADIUS Client:

Create a RADIUS Client to match your Controller’s IP and Shared key.



WFSCORPORATE Properties

Settings

Friendly name: WFSCORPORATE

Address (IP or DNS): 10.35.1.200

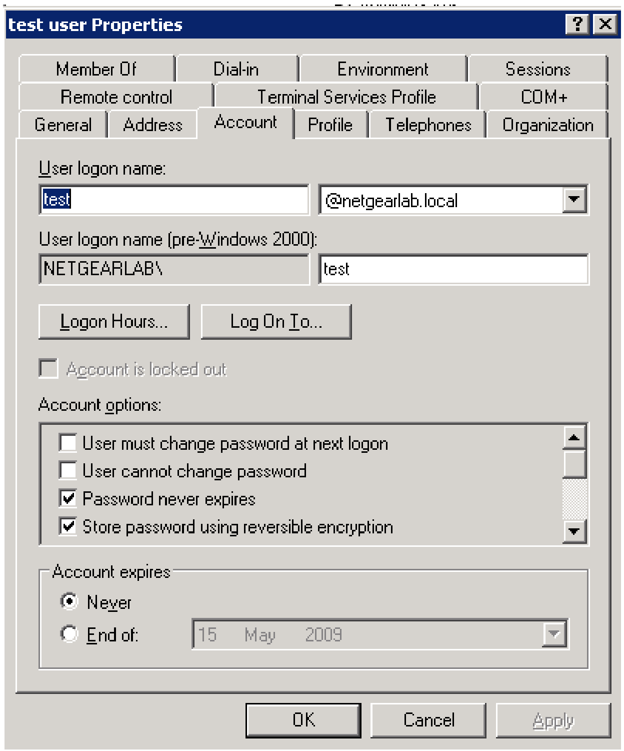
If you are using remote access policies based on the client vendor's attribute, specify the vendor of the RADIUS client.

Client-Vendor: RADIUS Standard

□ Request must contain the Message Authenticator attribute

Shared secret: ********

Confirm shared secret: ********



test user Properties

User logon name: test @netgearlab.local

User logon name (pre-Windows 2000): NETGEARLAB\ test

☐ Account is locked out

Account options:

☐ User must change password at next logon
☐ User cannot change password
☑ Password never expires
☑ Store password using reversible encryption

Account expires

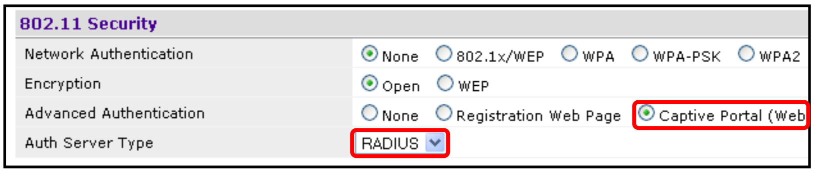
● Never
○ End of: 15 May 2009

NOTE:

When you create users that are meant to connect via Captive Portal, be sure that your user has the option to “Store password using reversible encryption” is ticked on. Otherwise it will fail to authenticate.

WFS709TP Configuration

To enable Captive Portal as the security method for the Public VLAN, go to **Configuration** > **Basic** and **WLAN**:

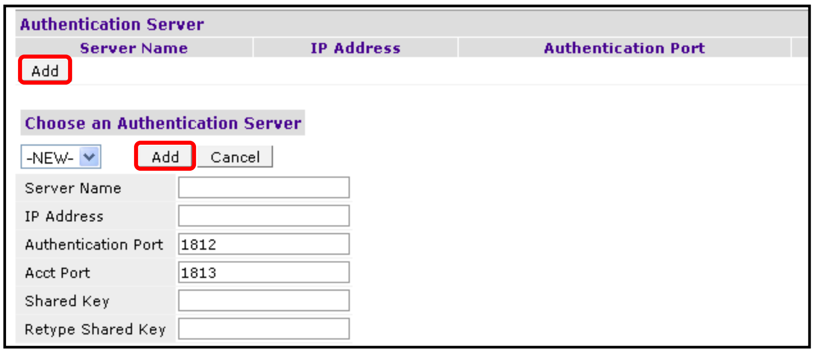


802.11 Security

Network Authentication	● None ○ 802.1x/WEP ○ WPA ○ WPA-PSK ○ WPA2
Encryption	● Open ○ WEP
Advanced Authentication	○ None ○ Registration Web Page ● Captive Portal (Web
Auth Server Type	RADIUS

In there, we will select the SSID that we wish to have under Captive Portal security (Public, in our case) and select the option of **Captive Portal** under advanced Authentication.

For authentication we will use **RADIUS**.



Authentication Server

Server Name	IP Address	Authentication Port

Choose an Authentication Server

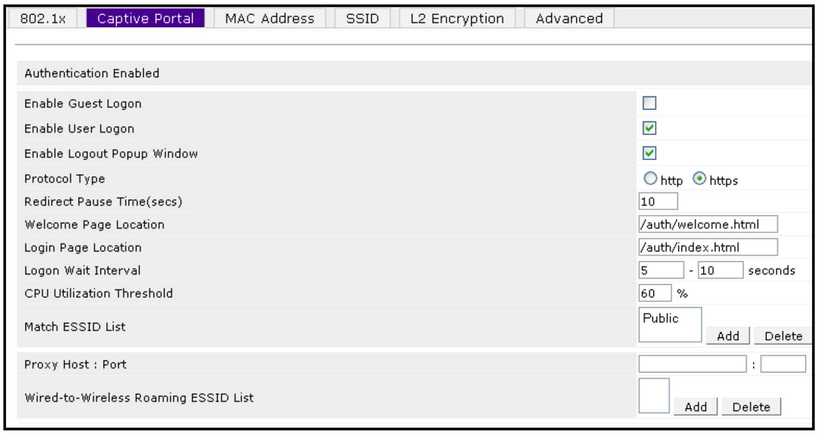
-NEW-

Server Name	
IP Address	
Authentication Port	1812
Acct Port	1813
Shared Key	
Retype Shared Key	

Click on **Add** under “Authentication Server”, and **Add** again under “Choose an Authentication Server”

There we will input our RADIUS Server and Client settings.

There are additional settings to configure in the **Configuration > Advanced > Security > Authentication Methods > Captive Portal > Authentication** page:



Authentication Enabled

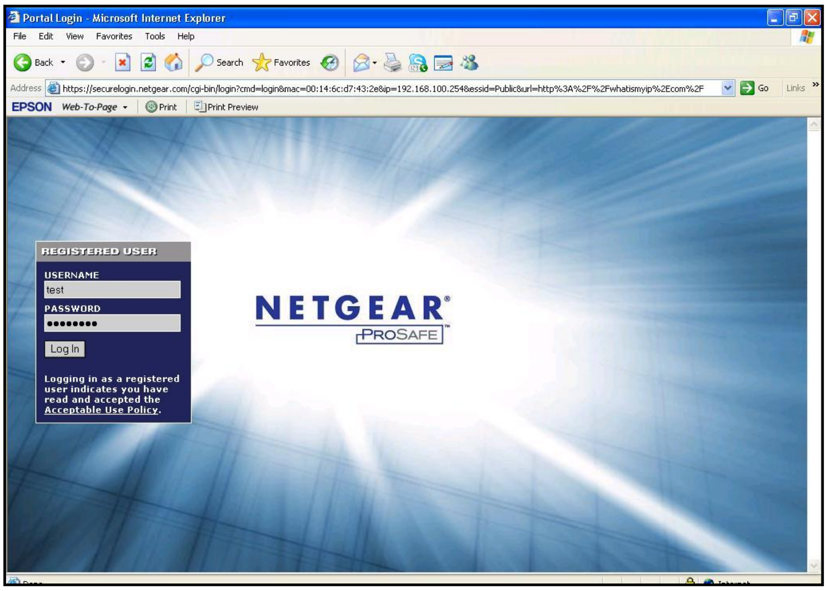
Enable Guest Logon	□
Enable User Logon	☑
Enable Logout Popup Window	☑
Protocol Type	○ http ● https
Redirect Pause Time(secs)	10
Welcome Page Location	/auth/welcome.html
Login Page Location	/auth/index.html
Logon Wait Interval	5 - 10 seconds
CPU Utilization Threshold	60 %
Match ESSID List	Public Add Delete
Proxy Host : Port	:
Wired-to-Wireless Roaming ESSID List	Add Delete

For our example, we will use all the default settings.

Notably, HTTPS as our protocol and no guest access.

Also, note that the SSID is already listed in the Match ESSID List.

Testing Performed



Portal Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go
Links
EPSON Web-To-Page Print Print Preview

https://securelogin.netgear.com/cgi-bin/login?cmd=login&mac=00:14:6c:d7:43:2e&ip=192.168.100.254&essid=Public&url=http%3A%2F%2Fwhatismyip%2Ecom%2F

REGISTERED USER

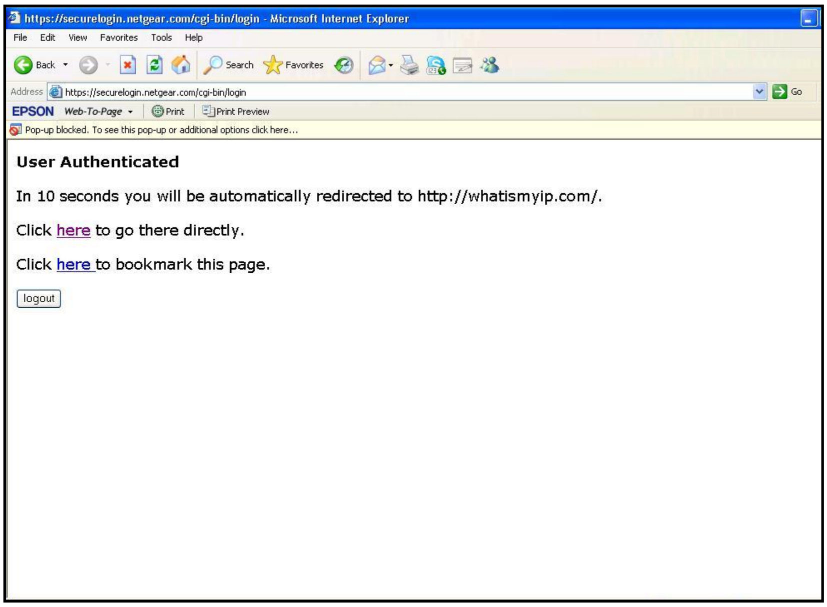
USERNAME test

PASSWORD ••••••••

Log In

Logging in as a registered user indicates you have read and accepted the Acceptable Use Policy.

Once you connect with a wireless client to the "Public" SSID and try to browse anywhere, you'll be redirected to the Captive Portal page.



https://securelogin.netgear.com/cgi-bin/login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go
EPSON Web-To-Page Print Print Preview

https://securelogin.netgear.com/cgi-bin/login

Pop-up blocked. To see this pop-up or additional options click here...

User Authenticated

In 10 seconds you will be automatically redirected to http://whatismyip.com/.

Click here to go there directly.

Click here to bookmark this page.

logout

After inputting your credentials, it will redirect you to the site you were trying to reach originally.

Useful procedures

Reset the switch to Factory Defaults:
Bring up the console and on the hyper-terminal type the following commands.

a. Reboot the box and hit enter when you see “Hit any key to stop autoboot” on the console.
b. On the cpboot prompt enter
   i. cpboot > setenv cfgfile foo
   ii. cpboot >saveenv
   iii. boot
c. The system will reset to factory default and when it boot up it will go to the initial setup screen.