# NETGEAR®
Connect with Innovation™

# WFS709TP
Quick Start Guide

## Table of Contents

Minimum requirements for a WFS709TP Deployment ......................................................... 2

Initial Setup using existing DHCP server.......................................................................... 4

Initial Setup Configuring the WFS709TP as a DHCP server ............................................. 6

Provisioning Access Points............................................................................................... 9

Final Notes ....................................................................................................................... 9

Appendix: Converting WG102 and WAG102 to WFS709TP compatible firmware ......... 10

# Minimum requirements for a WFS709TP Deployment

At the very least, in a hardware level, to deploy the WFS709TP controller you will need one or more compatible access points, WGL102 and WAGL102. (Note that WG102 and WAG102 APs can be upgraded with a Lightweight image to work with the WFS709TP, refer to the Appendix at the end of this document for more information). If you want to offer internet connection to your hosts, it is assumed another device will be connected to the controller to offer web connectivity.
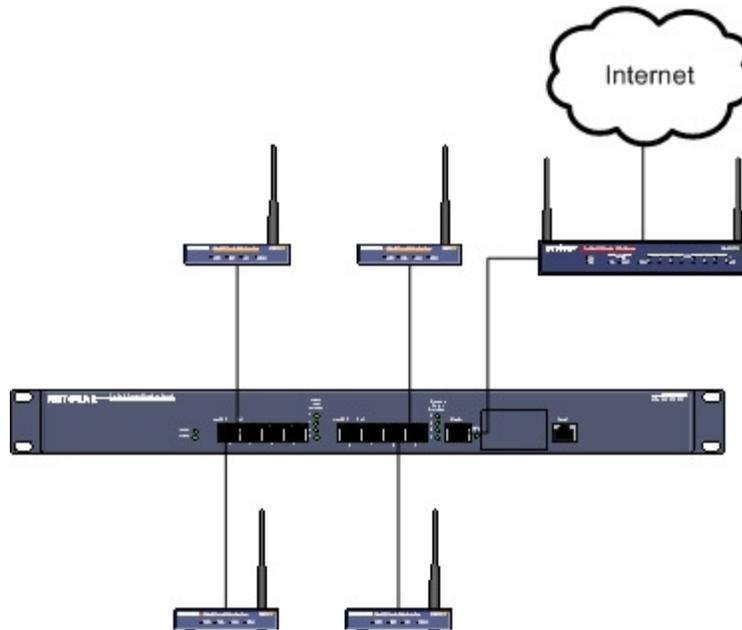


Figure A: Access Points connected directly to wireless controller.

The access points can be connected through other devices in a local network (Figure B). The access points need to be able to communicate to the Wireless Controller at an IP level so any VLAN or sub-net implementation requires careful consideration.

The scope of this document will be to explain the initial installation of the WFS709TP in a network that is not using any VLAN scheme.
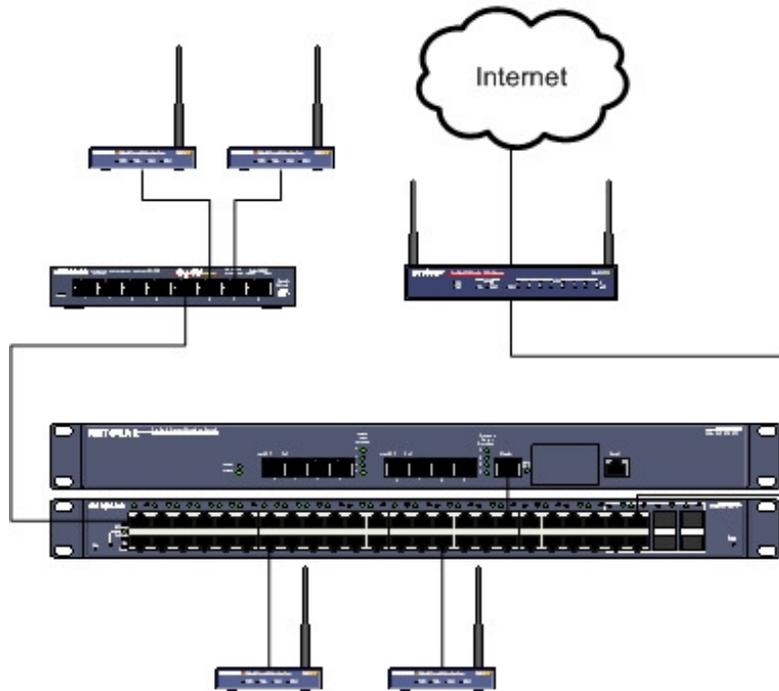
Figure B: Access Points connected to wireless
controllers through other switches.

All communication done between the Access Points and the Wireless Controller is done at Layer 3, and
for the Access Points to be accessible in the initial setup it is necessary to have a device capable of
offering IP addressing by using DHCP.

The WFS709TP controller is capable itself of serving as a DHCP server, therefore we will cover both
possible deployment scenarios in this document – using the WFS709TP as the DHCP server, or using an
already existing server in the network.

# Initial Setup using existing DHCP server

Most existing networks will have already a device offering IP addressing via DHCP, so for this deployment example, we will assume there is an existing DHCP server in the network and we will use it to allow communication between the WFS709TP controller and the Access Points.
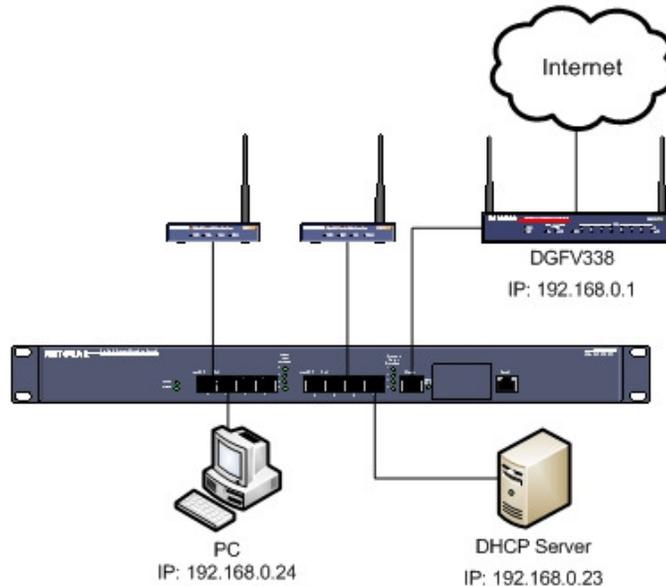


Figure D: Using an external DHCP server.

Log to the controller by accessing it through it's default IP address, 192.168.0.250, and configure the initial settings. Please note that if your PC is in a different network than 192.168.0.0/24 you will need to change your PC's IP address to match. If you choose to change the default IP address of the controller to one in a different network, you will need to ensure the IP address of your PC is in that same network.

After this configuration is done, the test lights on the Access Points should flicker off after a couple of minutes and they should show in the network summary page as unprovisioned:

# Initial Setup Configuring the WFS709TP as a DHCP server

**NOTE:** Most existing networks will have already a device offering IP addressing via DHCP, be sure to that no other device is offering this service before you configure your Wireless Controller as a DHCP server, as having two DHCP servers in the same network will cause network communication issues.
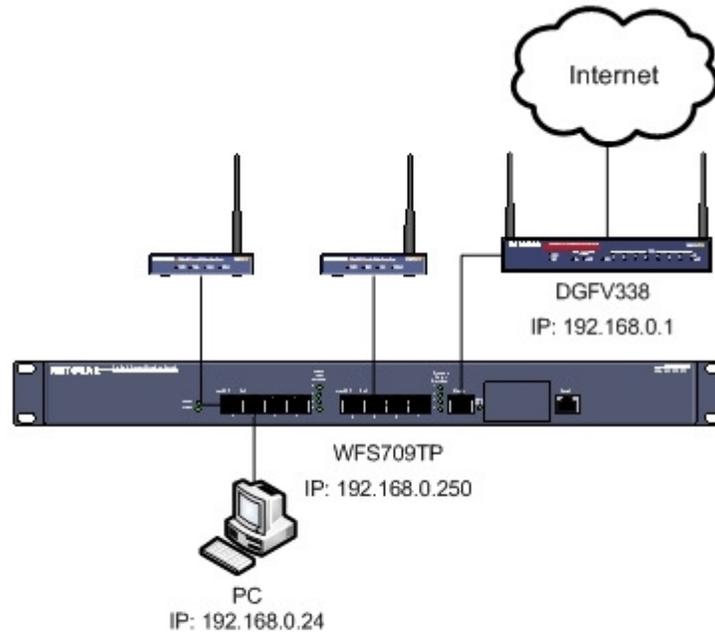


Figure C: Using the Wireless Controller as DHCP server.

With a computer directly connected to the WFS709TP, change the computer's IP address manually so it is in the same default IP subnet that the WFS709TP uses – which is 192.168.0.0/24. The default IP address of the WFS709TP is 192.168.0.250

Open a web browser, and access the initial configuration page via the IP address of the wireless controller – here you can set up the basic configuration parameters:



For this example we'll use these values, but you can change them to match your current IP scheme. Note that if you set your controller to a different subnet you will need to change your PC's IP address to match.

Even though there are access points connected to the controller, they will not be detected. Without the DHCP server in the current network, the access points are not able to communicate with the controller. Until the WFS709TP is configured to offer DHCP or there is another server in the network with that service, you won't be able to see the Access Points and their test light will remain on.

## Network Summary

**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>

### WLAN Network Status

| | Total Up | Total 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 |

Go to Configuration -> Advanced -> Controller -> General and then click on the DHCP tab. Fill the different settings to match your desired configuration.

## Controller > DHCP > Add DHCP Pool

**Basic | Advanced**
**Controller**
General
Management
**WLAN**
Network
Radio
Advanced
**RF Management**
Calibration
Optimization
Protection
Monitoring
Advanced
**Security**
Rogue AP
AAA Servers
Authentication Methods
Firewall Settings
**RF Policies**
Policies

« Back

| | |
|---|---|
| Pool Name | Default |
| Default Router | 192.168.0.1 |
| DNS Servers | 192.168.0.1 ☐ Import from DHCP (Multiple DNS Servers should be separated by spaces) |
| Domain Name | |
| WINS Servers | ☐ Import from DHCP (Multiple WINS Servers should be separated by spaces) |
| Lease | 0 Days 24 Hrs 0 Mins |
| Network | IP Address 192.168.0.0 Netmask 255.255.255.0 |

Done   Cancel

**NOTE:** The IP address pool has to be the same network used for the VLAN 1 IP of the controller which we set up previously. The default VLAN 1 IP address is 192.168.0.250. This limitation is only relevant because we're using a single VLAN setup.

Basic | Advanced    Controller > DHCP Server
Controller
  General
  Management
WLAN
  Network
  Radio
  Advanced
RF Management
  Calibration
  Optimization
  Protection
  Monitoring
  Advanced
Security
  Rogue AP
  AAA Servers
  Authentication Methods
  Firewall Settings
RF Policies
  Policies

General | Port | VLAN | IP Routing | VRRP | **DHCP Server**

**Enable DHCP Server**                                        ☑

**Pool Configuration**

| Name | Default Router | Network | Range | Action |
|------|----------------|---------|-------|--------|
| Default | 192.168.0.1 | 192.168.0.0 | 192.168.0.2-192.168.0.23 192.168.0.25-192.168.0.249 192.168.0.251-192.168.0.254 | Edit  Delete |

Add

**Excluded Address Range**

Excluded Address     | 192.168.0.24 192.168.0.250 |     Add

Delete

Apply

Configuration Updated Successfully
**Commands**                                         View Commands

**NOTE: Be sure** to tick the box "Enable DHCP Server" and click Apply after all settings are input. Changes will not take affect until the Apply button is clicked.

After this is set up, you will notice the test light in the connected Access Points will flicker off and they'll be listed in the Network Summary.

Configuration | Monitoring | Diagnostics | Maintenance | Plan | Even

**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**
  netgear-ap
**Debug**
  Local Clients
  Process Logs
**Custom Logs**
  <No Custom Logs Found>

**Network Summary**

**WLAN Network Status**

|  | Total Up | Total Down |
|--|----------|------------|
| WLAN Controllers | 1 | 0 |
| Access Points | 2 | 0 |
| Air Monitors | 0 | 0 |
| Wired Access Points | 0 | 0 |
| Unprovisioned Access Points | 2 | |
| 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 |

If you've concluded this part successfully, proceed to the section named: **Provisioning Access Points**

# Provisioning Access Points

To provision the access points, go to Configuration -> Basic -> Access Point Installation Wizard. Select Layer 2 as discovery method. Click next through the different wizard screens, confirming all your APs are detected, until you get the option to "Provision Now". Click on this button and wait for the provisioning process to occur. Note that the APs will be rebooted after the process is complete.

After this is done, you should be able to see your Network Summary should reflect that no Access Points are Unprovisioned:

**Network Summary**

**WLAN Network Status**

|  | Total Up | Total Down |
|---|---|---|
| WLAN Controllers | 1 | 0 |
| Access Points | 2 | 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 |

# Final Notes

For deployments that use multiple access points, it is advised to look at RF Planning and ARM settings. These settings will dynamically ensure that the wireless coverage is implemented in the most efficient way.

Although how to configure these settings is not covered in this guide, there will be a guide made specifically for ARM configuration and RF Planning.

## Appendix: Converting WG102 and WAG102 to WFS709TP compatible firmware

If you have existing WG102 or WAG102 access points, you can load a Lightweight Firmware image to make them compatible with the WFS709TP. Please note that this process is not reversible and will make the Access Points unusable without a WFS709TP controller.

The links to the images are the following:

(Please make sure you download the firmware relevant to the correct relevant geographic zone configured on the WFS709TP controller)

WG102 to WGL102: http://kbserver.netgear.com/release_notes/d103134.asp

WAG102 to WAGL102: http://kbserver.netgear.com/release_notes/d103135.asp