
Networking at Cardiff University

Wireless Access Point Policy and Guide

Table of Contents

1	INTRODUCTION	3
1.1	INTENDED AUDIENCE.....	3
1.2	OBJECTIVES.....	3
1.3	RISK.....	3
2	AUTHORITY SUPPORT AND RESPONSIBILITY.....	4
3	MANDATORY COMPLIANCE.....	5
3.1	NEW ACCESS POINTS.....	5
3.2	EXISTING ACCESS POINTS BOUGHT PRIOR TO THIS POLICY	5
3.2.1	Security.....	5
3.2.2	Channel Management.....	6
3.2.3	Location	6
4	WIRELESS CLIENTS	7

Please contact [insrvConnect](#) if you have any queries regarding the content of this document.

- Visit: 40-41 Park Place, Monday to Friday 9.00 to 17.00
- Telephone: 029 2087 4487, Monday to Friday 8.00 to 22.00
- Email: insrvConnect@cardiff.ac.uk

1 Introduction

Wireless networks provide users with an immense amount of freedom. Pushed by many high technology companies as the next "big thing," wireless is not only easy to use it is also being heavily promoted. Unfortunately, little is mentioned of the broad array of security deficiencies wireless technology is laden with.

To make matters worse, in an effort to make installation easy, almost all wireless hardware/software vendors ship their products configured with insecure settings by default. Therefore, wireless tends to be easy to install, but difficult to secure and manage.

We have had many incidents where the network is taken down by access points both rogue and sanctioned.

1.1 Intended Audience

This document is intended to be used as a policy guide to departments and departmental staff wishing to deploy wireless networking devices on the Cardiff University LAN.

1.2 Objectives

Cardiff University Information Services (INSRV) is responsible for the operation of Cardiff University's networks and therefore has the authority and responsibility to specify requirements for any devices connecting to Cardiff University's Network. This authority extends to device configuration management, as incorrect or conflicting information could adversely impact the operation of other network-connected devices

This policy specifies the requirements for Wireless Access Points (AP's) and related wireless LAN infrastructure operating in Cardiff University. It also provides related "best practice" recommendations.

As a User organisation of JANET Cardiff University must take all steps to ensure compliance with the conditions set out in the JANET Acceptable use Policy document, and to ensure that unacceptable use of JANET does not occur. The discharge of this responsibility must include informing those at the Organisation with access to JANET of their obligations in this respect.

The Janet Acceptable Use policy can be found at

<http://www.ja.net/documents/use.html>

All users of Cardiff University's network services must be familiar with, and adhere to, this and INSRV's acceptable use policy no matter how they connect to network services and infrastructure. As result, INSRV's key objective is to ensure the security and integrity of any wireless deployment within the Cardiff University campus.

1.3 Risk

Given that only a very small number of AP's can be in active operation within a given geographic area without creating performance degrading interference for each other. Even given limited deployment, it is important to have the AP's frequency settings configured in a non-interfering way. For this reason, coordination among those operating wireless LAN AP's is essential. This will be achieved centrally by use of trapeze equipment.

Authorised AP's may need to be shut down or reconfigured at a later date, if another academic or administrative unit in the area experiences interference in the relevant frequency ranges.

INSRV reserves the right to shut down or reconfigure previously authorised AP's if interference is caused to other wireless users within the same geographic area.

2 Authority Support and Responsibility

- All deployments and usage of wireless networks **must** comply with all INSRV Regulations.
- INSRV are actively policing the wireless network in an effort to discover unregistered AP's and will act on those discovered during the normal course of events in operating and/or troubleshooting the network.
- Non-compliant APs must be remedied immediately and will be removed from the network to reduce risk of networking failures for other network users.
- Charges may be applied for time spent by INSRV in troubleshooting problems attributable to a non-compliant or mis-configured AP's.
- Responsibility for problems lies with those responsible for the AP and not INSRV. However by prior agreement INSRV may, at its discretion, render help and service to departments and users running wireless networks.

3 Mandatory Compliance

3.1 New access points

- Users will need to purchase access points through INSRV
- The only access points permitted are Trapeze access points
- Access points will be deployed, configured, & maintained by INSRV

The purchasing procedure for new access points will be made available shortly.

3.2 Existing Access Points Bought Prior to This Policy

- Small office home office access points are not permitted on the Cardiff university network and must be removed.
- Only Access points that are bridging natively are permitted. Access points that are routing and NATing are not permitted.
- Anyone running a wireless AP must have registered the AP with INSRV via Permission To Connect procedure, details of which are available from INSRV reception.
- IP Address for the AP's must be obtained VIA DHCP allocated by INSRV via AP's Mac field in the Permission To Connect Form available from INSRV reception.
- SSID must be broadcasted from the unit to help with identification of the wireless network for users. With the exception of devices placed on the Heath campus where SSID must not be broadcast. SSID must begin with "CU-" to identify they are Cardiff university owned.
- In cases where access points have variable radio power levels, the minimal power level that provides the intended coverage must be chosen so as to limit interference with other devices operating in that frequency range.

3.2.1 Security

- Our obligations under the JANET acceptable use policy dictate that if INSRV through routine policing of the network discover a misconfigured or insecure AP, INSRV will act immediately to disconnect the device and remove the security risk from the LAN infrastructure without notification.
- No wireless Access Points are allowed on the trusted Admin network. Any AP's discovered on this network will be disconnected regardless of configuration and security measures.
- If an AP's is found to be moved or redeployed on the network after INSRV has taken steps to secure the network infrastructure, the case concerned will be immediately escalated to INSRV board level for a formal resolution.
- **Encryption must be used** on any access point that is used to connect to the Cardiff Network. However, INSRV is not responsible for prevention, implementation and policing of any security breaches that may occur. It is also recommended that the wireless network be treated as insecure even when encryption is enabled. Open systems are not permitted.
- WPA (or WPA2) Encryption must be used as a where possible as the encryption setting to ensure security between the wireless devices and the access points.
- WPA with RADIUS server authentication must be used where possible in preference to WPA-PSK. This must use record keeping of users and MAC addresses used with this information being made available to Cardiff Information Systems Security staff when requested.

- If WPA Pre-Shared Key is used, the key must not be given out to users and staff. This must be held by the IT person responsible for the Access Points in question.
- WEP encryption should be used only as a **last resort**. First choice should be 802.11i (WPA2) or WPA
- Media Access Control (MAC) filtering must be used, if possible, the access point as it provides an added layer of authentication for wireless clients. Ideally MAC addresses must be filtered and authorised with the use of a RADIUS server.
- AP devices **must not** provide DHCP services for wireless devices. All addresses for wireless devices, laptop network cards etc, must be obtained via Permission To Connect Form available from INSRV reception form quoting the wireless MAC address and the AP's acting as a bridge between the wireless device and the network. The SSID of the network if known must also be stated.
- Access point **must not** be open to guests, unauthorised and unauthenticated users, unless the client machine is registered with the P2C database as a guest.
- If an AP's has separate MAC addresses for the Radio and Wired network interface cards then both must be registered in P2C. An IP address will be assigned to each interface.
- INSRV currently runs a wireless network using WPA-Radius with 802.1x as an authentication supplicant. Users are logged in securely with their Netware user name and password. If you would like more information about this method of authorisation and authentication please contact Anthony Cope (INSRV) insrvConnect@cardiff.ac.uk

3.2.2 Channel Management

- Channels must be agreed with Information Services. You may be asked to change the channel at any time.

3.2.3 Location

- Careful planning of wireless LANs, including use of a formal site survey process can significantly reduce later frequency conflicts and network performance problems.
- Access points must be both logically and physically secure. Access points must be located in physically secured areas. These devices must also be setup to only allow administrators to make configuration changes. Most AP's, when reset, will revert to a default mode. If the AP is in an insecure or heavy traffic area, it is easy for someone to physically manipulate the access point and turn it off to deny service or reset it so that it reverts to the default configuration.
- The AP's must also be adequately secured so that unauthorised individuals cannot connect to and manipulate the secure configuration settings. Most AP's allow the creation of accounts and passwords for authorised users. These accounts must be created to limit unauthorised access to the AP.
- Do not deploy any wireless access points near lifts, electricity substations and areas where safety could be an issue.
- The AP must be security marked to show the IP address, AP's name and department responsible. This is to help prevent the deployment of rogue access points.

4 Wireless Clients

- Wireless clients **must be** equipped with a host-based personal firewall and anti-virus software. Wireless clients are more difficult to secure due to their mobility and subsequent dependence on the user to apply proper security measures during use. Hackers can use many attacks directed at wireless clients so it is essential to implement some host-based security on the user-controlled wireless devices.
- Wireless clients **must not** be configured to engage in ad-hoc communications. These ad hoc wireless networks allow two or more stations to communicate directly with each other without an access point routing their traffic. Hackers can conduct a number of attacks against systems using ad-hoc wireless networking.

The primary issue with ad-hoc networks is the lack of authentication. Ad-hoc networks can allow a hacker to execute man in the middle attacks, denial of service, and/or compromise systems. If a hacker can compromise one wireless client, the attacker can use the system to attack other systems on the network. If the wireless clients cannot communicate with each other initially through an ad-hoc configuration, it is more difficult for a hacker to attack or gather information from the network.