



Security

WDSi Group

1. Background

At the forefront of our customers mind when considering installing a WiFi network, is security. Nowhere is the need for robust security more important than in a WiFi network, particularly where that network is open.

- Differing registration methodology for each group
- Encrypted passwords for one group for access to special research work
- Firewalls between different groups
- Allowing standard internet access to one of the groups

2. The Challenge

A recent commission required a 4G network across a significant public sectors estate, the project came with a number of challenges from a security perspective:

- The estate was made of 5 discreet buildings each with multiple floors.
- Some of the building were extremely old and would not allow cabling to be run.
- The client needed to make the WiFi available to three different types of user
- The network required a very high degree of security as two of the user groups would be sharing extremely sensitive information/documentation
- In addition these two user groups may from time to time need access to sites that would normally be barred to users.



The challenges above drove us to consider the following requirements:

- Separation of three different user groups that have access to the same network
- Providing differing levels of access depending on which user group you were from
- Differing periods of access being made available to each group.

“WDSi were brilliant in identifying exactly what we needed in order for our networks to be secure and avoid sensitive information potentially being intercepted by guests visiting our premises. With cabling being a challenge and expensive, being able to provide secure WiFi networks via a 4G backhaul was a huge benefit and has been a great success.”

3. The Solution

4G as a solution

Each WiFi unit was programmed with a specific room number so that our engineers and support team could monitor usage for both security and control purposes

User Specific SSIDs and Passwords

Each user group was allocated its own SSID and password.

Content Filtering

Content filtering was programmed into all of the 4G units with group dependant levels of access. The user group which did from time to time need to circumvent the content restrictions was provided with a tailored process and specific password to enable access.

Firewalls

Given that two groups were sharing and accessing highly sensitive data firewalls were built into the network to prevent non authorised access.

4. Review

The entire estate now has a 4G network, with nearly 250 units individually programmed to serve three different user groups with very different profiles.

Branded landing pages have been designed that reflect the different registration processes that each user group has.

XX sessions have been recorded driven xx users since January 2017

No security breaches have ever been recorded over the life of the project.

5. Wider Outcomes

The success of this project has driven demand from other public sector offices. We have also recently been involved in a similar roll out for a public sector department with multiple offices across the UK.