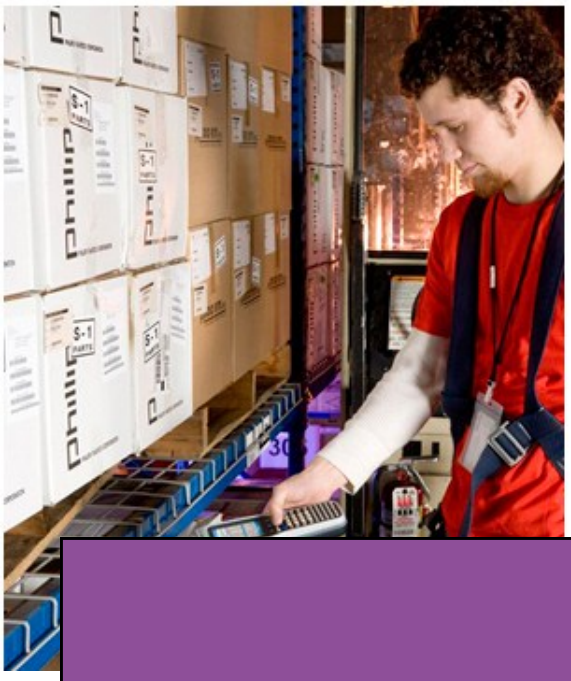
Cedar Bay

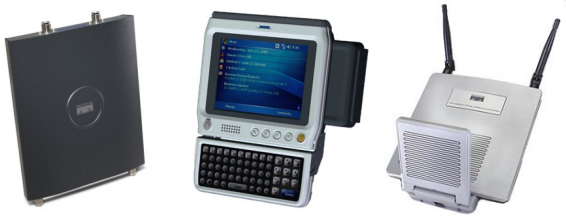


Wireless Services

IFS BUSINESS PARTNER

Wireless Services

Cedar Bay has a proven track record of helping companies in all areas of wireless deployment, providing a full set of services from site surveys, hardware selection, procurement, configuration and wireless security implementation.



Wireless Networks

As a leading provider of online, real-time automated data collection solutions, Cedar Bay is committed to investigating and implementing emerging technologies that provide our customers with a competitive edge.

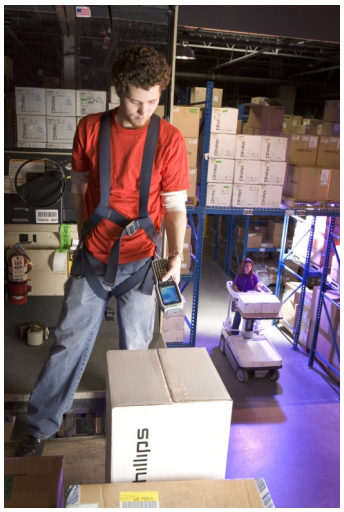
A substantial part of any automated data collection project will be the implementation of a wireless solution allowing the users to capture data at the point of use rather than having to return to a fixed terminal.
When designing a wired network, systems designers carefully plan the connections to each user location, taking into account the employee's applications, the bandwidth required to deliver a productive user experience, and the resources to be shared among network users. To be successful, the same network design discipline applies to wireless local area networks (WLANs). Once designed, configuration of the network to provide optimum data throughput, maintainability and security is vital.

Today business customers' single biggest objection to deploying wireless technology is the fact that it's not secure. This opinion is perhaps based on the inadequate security features available when WLANs started to become popular. Wireless networks are now commonplace in business enterprises, in part due to the necessary enhancements that have been made to wireless security.

Site Surveys

A site survey is a vital initial step in deploying a reliable WLAN. This is because wireless technology is very unpredictable without conducting tests using equipment within the environment the WLAN will be deployed. Even when using omni-directional antennas, the propagation of radio waves rarely travels the same distance in all directions. They are readily absorbed by anything with moisture content (e.g. walls, products, and people) and are reflected by metal often resulting in a highly irregular coverage pattern.

To further complicate matters the required bandwidth for potential wireless clients must be taken into consideration together with site specific conditions.
As an example WLANs may need to be deployed in external areas thus exposing equipment to local weather conditions or in hazardous areas where WLAN equipment must be certified to be 'Intrinsically-Safe'.



Cedar Bay issues a detailed pre-survey questionnaire to ensure that our experienced survey engineers are fully prepared prior to arriving on site. This defines the customer requirements such as required coverage areas, type and number of proposed wireless devices, required data link speed, and redundancy. Finally, specialist Wifi tools are now used by Cedar Bay to monitor both general Wifi activity and potential sources of interference to assist in a successful trouble-free deployment.

Automated data collection systems for IFS Applications

Cedar Bay produces a detailed report identifying the required components of the WLAN and detailing the steps required in order to prepare the site for a successful installation. This includes annotated facility plans detailing the required access point locations, photographs confirming mounting positions, Wifi readings at strategic locations and details of any existing Wifi activity. The report is sufficiently detailed to enable the customer to install the data cabling of Wifi equipment in readiness for the WLAN to be configured and commissioned. Cedar Bay configures the Wifi access points with IP addresses allocated by the customer to enable the access points to be installed as part of the cabling process.

"Cedar Bay has proven to be a strong business partner for Kimal's Data Capture Solution requirements for the long term, maintaining their convictions on the solution direction for day one."

Tony Guest, Project Leader Kimal Plc

Configuration & Commissioning

The process of deploying the WLAN is simplified having conducted an initial site survey enabling the WLAN to be carefully planned. A questionnaire is issued to the customer as a check list to ensure that the necessary installation steps have been completed in readiness for a successful 'Configuration & Commissioning' visit.

The WLAN is carefully configured based on the Wifi Activity study conducted as part of the site survey to keep the affects of radio interference to a minimum. Part of the configuration exercise includes securing the WLAN based on the customers' requirements. Coverage and connectivity tests are then conducted to verify that the WLAN is operational in all required areas of the site. Roaming tests are conducted to ensure each wireless client device can seamlessly roam between each Wifi access point whilst maintaining connectivity. Finally, a comprehensive report is compiled detailing each facet of the WLAN. This enables the customer to utilize this document for reference for first line support.

Wireless Security Background

Wireless security is a vital component to any WLAN deployment due to the nature of radio waves in the fact that they don't respect boundaries. An access point antenna will potentially transmit radio energy for relatively large distances. This opens up the prospect of potential connectivity to the WLAN beyond the boundary of a customers' site thus emphasizing the importance of adequate wireless security.

Early WLANs had limited security options and were often 'open' due to a lack of knowledge at the time of the potential threat of 'would be' attackers. It was also considered advisable to change the ESS-ID (network name) from the widely known 'factory default' value and to configure the access points (where possible) to 'hide' this ESS-ID. These two measures are no longer effective on the basis that wireless clients are more sophisticated and can easily derive the ESS-ID regardless of whether or not it is changed or indeed 'hidden'. The only real means of securing the data at the time was to use a data encryption technique called WEP (wired equivalent privacy). WEP encryption is now considered to be flawed in that it is possible to for Wifi hackers to decipher to WEP encryption key and hence gain access to any WEP encrypted network.

Current Wireless Security Techniques

Cedar Bay's security services provides the expertise and tools to assess, architect, implement and manage the security needs and demands of any business expanding into the wireless world. Various security options that we recommend are detailed below:

WPA & WPA2

The WPA and WPA2 standards were created by the Wifi Alliance industry group that promotes interoperability and security for the wireless LAN industry. The Wi-Fi Alliance WPA and WPA2 standards closely mirrors the official IEEE 802.11i wireless LAN security standards group but incorporates
additional EAP (Extensible Authentication Protocol) standards that the Wi-Fi Alliance considers secure. Cedar bay recommend using WPA or WPA 2 as a minimum security requirement. The simpler adoption of WPA is called PSK (Pre Shared Key) and enables a WPA Passphrase to be configured on the access points and wireless clients. WPA and WPA2 can also be used in conjunction with an 802.1x authentication server.

802.1X

802.1x is a security protocol that provides port-based authentication, involving communications between a supplicant, authenticator, and authentication server. The supplicant is often software on a client device, such as a laptop. The authenticator is a wired Ethernet switch or wireless access point, and an authentication server is generally a RADIUS database. The authenticator acts like a security guard to a protected network. The supplicant (client device) is not allowed access through the authenticator to the protected side of the network until the supplicants' identity is authorized. An analogy to this is providing a valid passport at an airport before being allowed to pass through security to the terminal.

This form of security is very confusing in that there are an increasing number of variations now in existence. Cedar Bay is able to offer guidance on which variation is most appropriate as it will only be possible to connect a wireless client device if it supports the method of EAP deployed.

ACL

Cedar Bay considers this form of security to be a 'belt and braces' approach. This can be used in addition to the other forms of security already supplied. It works by configuring each access point with the unique Radio MAC address identity of any wireless client devices you wish to allow access to the network. It has the added benefit of enabling the access point to log any attempts by 'none allowed' clients to an audit log file.

Cisco Wireless Control System

Cedar Bay recommends the WCS for customers who need to pro-actively manage their WLAN. The WCS is a powerful graphical tool that includes a key feature to monitor the WLAN for unwanted intruders such as 'rogue' access points and clients.

HOW CAN WE HELP YOU?:

Cedar Bay (Europe) Ltd
Eagle Tower,
Montpellier Drive,
Cheltenham,
Glos, UK. GL50 1TA
Tel: +44(0) 1242 304244
e-mail: info@cedar-bay.com
www.cedar-bay.com

IFS BUSINESS PARTNER