

UConn Wireless Security Standards Worksheet

Purpose:

The intention of this document is to outline the minimum standards for a wireless installation. The document is broken up into 3 primary sections:

- **Common Requirements:** This is information that is required regardless of the deployment type.
- **Large Deployment:** It is assumed that a departmental deployment consists of multiple access points and utilizes enterprise grade equipment such as what is used by the UITS central wireless deployment.
- **Small/Individual Deployment:** It is assumed that an individual deployment consists of one or two access points and utilizes SOHO (small office home office) grade equipment such as a Linksys or Netgear access point.

Definitions:

Access Point (AP): A network device that serves as a common connection point for devices in a wireless network. Access points use RF instead of wired ports for access by multiple users of the wireless network. Access points are shared bandwidth devices connected to the UConn wired network.

Service Set Identifier (SSID): An alphanumeric string that identifies a wireless network. All devices on a specific wireless network must know the SSID of that network.

Wi-Fi Protected Access (WPA): A method of wireless network encryption. This provides an improvement over the WEP standard and is based on the TKIP protocol.

Simple Network Management Protocol (SNMP): The network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

Secure Sockets Layer (SSL): SSL is a application layer protocol created by Netscape for managing the security of message transmissions in a network. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

Media Access Control Address (MAC): A Unique number to every network device, including network cards.

Common Requirements

Please review the University Wireless Policy for policy related information.

Minimum Technical Requirements

- Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
- Place APs in secured areas to prevent unauthorized physical access and user manipulation.
- Change the default service set Identifier (SSID).

- Ensure that AP channel selection utilizes the maximum amount of non overlapping channels for the given spectrum.
- Use WPA or greater encryption.
- APs shall not be plugged into network hubs.
- Ensure that all APs have strong administrative passwords.
- Use SNMPv3 and/or SSL/TLS for Web-based management of APs.
- Access points cannot interfere with any part of the central University wireless network
- When disposing of access points that will no longer be used, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

Large Deployment

Minimum Technical Requirements

Secure Access

- User Authentication from a centralized server to obtain access
- User and event logging is automated, maintained and reviewed

Public Access

- It is acceptable to broadcast the SSID in this scenario
- Configure a firewall between the wireless and wired network to prevent access to sensitive UConn systems
- User Authentication
- User and event logging is automated, maintained and reviewed

Small/Individual Deployment

Minimum Technical Requirements

Secure Access

- Access points must have the broadcast SSID feature disabled so that the client SSID matches that of the Access Point (AP).
- MAC address access control lists

Public Access

Public access for this deployment is not allowed.