**Guest Wireless Services White Paper**

**05 October 2016**

# Introduction

Wireless guest services is a key customer service initiative that DoD organizations have implemented or are considering implementing, not only for guests but also for employees who wish to use wireless Local Area Network (LAN)[[1]](#footnote-1)-enabled mobile devices that are not authorized for direct access to the enterprise network. Wireless guest services more commonly refers to providing Internet access via wireless LAN, although cellular services may also be included in a comprehensive wireless guest service. A wireless guest service rarely provides direct access to a DoD site’s enterprise network. Most implementations provide only Internet access, but some may also provide access to a limited set of applications (for example, enterprise email).

A wireless guest service can increase the risk of attack on an enterprise network if it is not properly implemented. Therefore, a comprehensive evaluation of the risk of a proposed wireless guest service, based on the operational environment and services to be provided, should be completed prior to the deployment of any service. DoDI 8420.01, Commercial Wireless Local Area Network (WLAN) Devices, Systems, and Technologies[[2]](#footnote-2), provides overall DoD guidance for the system architecture of a wireless guest service. This paper will review key network configuration, security controls, and risk issues and provide best practice recommendations for the design of a wireless guest service in the DoD environment.

# discussion

The first key consideration when designing a wireless guest service is to ensure compliance with current DoD wireless policy, including draft DoDI 8420.01 and network component Security Technical Implementation Guides (STIGs). Key STIGs include the Network Wireless LAN Access Point (Internet Gateway Only Connection) STIG included as a component of the Network WLAN STIG and product-specific firewall, router, switch, and Intrusion Detection System (IDS) STIGs.

Second, determine what services will be provided. For the vast majority of cases, a wireless guest service only provides access to the Internet. Wireless guest services that provide access to a limited set of applications require a significantly more complex network design and access control mechanism. Paragraph 3.5 of draft DoDI 8420.01 states that guests may access DoD network resources via a Virtual Private Network (VPN), which implies that wireless guest services should not provide direct access to DoD applications or DoD network resources and, therefore, only provide Internet access. It is recommended that in the DoD environment, Internet-only access be provided, and guests requiring access to a DoD network be required to use a VPN.

Third, a decision needs to be made on the type of wireless service provided. Usually only wireless LAN service is provided, but increasingly, organizations are also providing cellular services, including signal amplifiers that boost existing cellular signals, in buildings where carrier signals from a nearby cell tower are not available. Note that draft DoD 8420.01 applies only to wireless LAN systems. For this paper, discussion will be limited to wireless LAN services only. Draft DoDI 8420.01 states that wireless LAN systems must be Wi-Fi Alliance certified and FIPS 140-2 validated.

Fourth, the operational environment should be analyzed to determine the amount of access the general public[[3]](#footnote-3) will have to the guest wireless LAN system. This analysis will impact the type of access control placed on the guest wireless service. For example, best practice is to use some form of user authentication for a wireless guest service. The design of the authentication mechanism should be based on the results of a threat assessment of the DoD facility and network infrastructure. The following access controls are recommended[[4]](#footnote-4):

* For low-threat environments where the wireless guest service is connected to a commercial ISP and wireless guest service traffic is not connected to a DoD network, implementing open access (no password required) to the wireless guest services may be considered. This use case would be similar to a guest Wi-Fi network in a restaurant. Note that draft DoD 8420-01 requires that the Authorizing Official (AO) determine if guests should be sponsored by host organizations prior to accessing wireless guest services. If the AO determines guests should be sponsored, implementation of open access to the wireless guest services may be precluded.
* For low-threat environments where the general public has limited access to the wireless LAN system, a system-wide password should be used that is changed on a periodic basis (for example, a new password every five days). The password can be provided to guests when they check in to the facility.
* For moderate-high threat environments or where the general public has significant access to the wireless LAN system, the access control mechanism for the wireless guest service should require for each user an individual user name/password that expires after a set time (for example, after 24 hours)[[5]](#footnote-5).

Fifth, regarding the network architecture for a wireless guest service, draft DoDI 8420.01 states that all guest traffic must be segmented by a physical boundary or logical boundary from other network traffic, and a wireless IDS must be used to provide “spectrum sweeps” to monitor for unauthorized wireless LAN activity. If a separate wireless LAN network is not set up to provide physical separation for wireless guest services traffic (most secure option), it is recommended that all guest wireless LAN components be placed in an isolated subnet, virtual LAN (VLAN), or a Demilitarized Zone (DMZ), and all traffic be routed to an Internet gateway. All access to the enterprise network should be disabled. Acquisition processes should ensure that network components providing logical separation between guest wireless traffic and enterprise traffic logical separation provided by the network components is adequate[[6]](#footnote-6). The wireless intrusion detection system (IDS) can be either a purpose-built wireless IDS or included in the wireless LAN product.

Another aspect of network design is determining if the wireless guest service will be connected to a commercial Internet Service Provider (ISP) or to the DoD ISP. The use of a commercial ISP or DoD ISP for the guest wireless network depends on the overall network architecture. If the guest wireless network access point (AP) is not connected to the DoD network, the guest wireless network router or firewall will be connected to a commercial ISP. If the guest wireless network AP is connected to the DoD network switch or firewall, the guest wireless network should be placed in an untrusted VLAN or zone and routed to the DoD ISP.

Sixth, STIG[[7]](#footnote-7)-compliant configuration of the wireless LAN system should be planned for. Key security controls include:

* Enable DoD warning banner (user must click acceptance of terms/conditions before wireless LAN access granted).
* Enable access control mechanism (may be integrated with the message/warning banner in some systems).
* Enable user inactivity timeout (30 minutes or less).
* Enable WPA2 security (use WPA2 Enterprise if access control [passwords] is enabled).
* Consider enabling forced timeout of user session if active for a set period of time (for example, eight hours). Implementation should be based on expected usage patterns of the wireless guest service.
* Configure network management interfaces of the wireless LAN system in accordance with the STIG.

# SUMMARY

The following is a summary of all recommendations discussed in this paper:

1. Review and become familiar with draft DoDI 8420-01, the WLAN Access Point (Internet Gateway Only Connection) STIG, and all applicable network component product STIGs.
2. Determine if the wireless guest service will provide any service other than Internet access.
3. Determine the type of wireless service that will be included in the wireless guest service (wireless LAN and/or cellular). Only Wi-Fi Alliance certified and FIPS 140-2 validated wireless LAN products should be procured.
4. Determine the appropriate access control mechanism for the wireless guest service based on the operational environment and risk assessment.
5. Decide if the guest wireless LAN system will be installed so that it is physically separated from the enterprise network or if the enterprise network will provide logical separation between enterprise and guest wireless traffic. For the latter case, ensure only Common Criteria certified network components (switches, routers, firewalls, and/or wireless access points/switches) are used to provide logical separation. As part of the network design for the wireless guest service, determine if the service will be connected to a commercial ISP or to the DoD ISP.
6. Configure the guest wireless access point and other components according to the WLAN Access Point (Internet Gateway Only Connection) STIG and other recommendations provided in this paper.

1. “Wireless LAN” refers to IEEE 802.11 systems compliant products throughout this paper. [↑](#footnote-ref-1)
2. An update of DoDI 8420.01 is in final DoD-wide coordination by the DoD CIO’s office and is expected to be released by October 2016. The coordination draft version of DoDI 8420.01 is currently being used by most DoD organizations since the published version was released in 2009 and is considered out of date. The coordination draft version of DoDI 8420.01 is used as reference for this white paper because it provides guidance on required security controls for wireless guest services. [↑](#footnote-ref-2)
3. General public is defined as non-guests who are outside the physical boundary of the DoD-controlled facility (e.g., someone walking or parked outside a DoD building). [↑](#footnote-ref-3)
4. Note: These recommendations are based on the assumption that all network configurations and wireless LAN configurations recommended in this paper have been followed. [↑](#footnote-ref-4)
5. Commercial access control systems are available where employees can register guests (or themselves) for temporary passwords to the wireless guest service. [↑](#footnote-ref-5)
6. One way to ensure compliance is to buy only Common Criteria certified network components. [↑](#footnote-ref-6)
7. The applicable STIG is the WLAN Access Point (Internet Gateway Only Connection) STIG. [↑](#footnote-ref-7)