



Physical Security of the Wireless Installation

Wireless Infrastructure, Article 11-15-2011

Investment in a wireless LAN reflects recognition that mobility is important for day to day business operation. In fact, mobile networking has become business and mission critical in many environments. Physical security of the wireless infrastructure components is more difficult than securing wired infrastructure components. By their very nature, the wireless access points, antennas, and connecting cables are "out in the open" so that they provide the best wireless coverage. Of course securing the access points and antennas is desirable, and in some business verticals, it is mandated.

- In Federal Government – Directive 8100.2 mandates FIPS 140-2 compliance wherein FIPS 140-2 paragraph 4.5 requires "*physical security mechanisms*" to be applied to wireless networks.
- In Retail – The Payment Card Industry Data Security Standard (PCI-DSS) requirement 9.1.3 states that the operator must "*Restrict physical access to wireless access points, gateways, and handheld devices*"
- In Healthcare – *the TIA -1179 Healthcare facility telecommunications cabling standard* specifies that, due to the life and mission critical nature of the network, additional precautions shall be taken to secure telecommunications components.

In addition to mandates to physically secure the wireless network, it simply makes sense from the standpoint of protecting the investment. Typically, the wireless LAN represents an investment in design, site survey, antennas, cabling, access points, and installation time. It is imperative to protect this investment, not only from theft or tampering, but also from accidental or unintentional moves and disconnects.

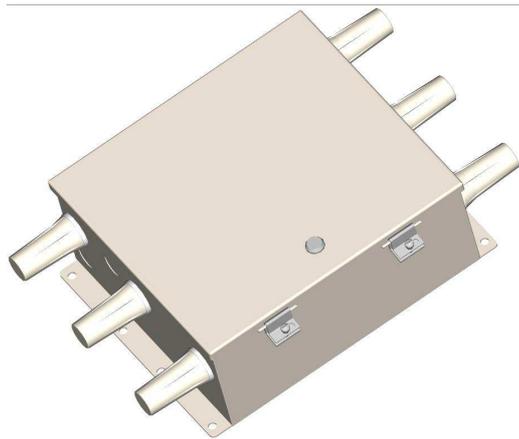
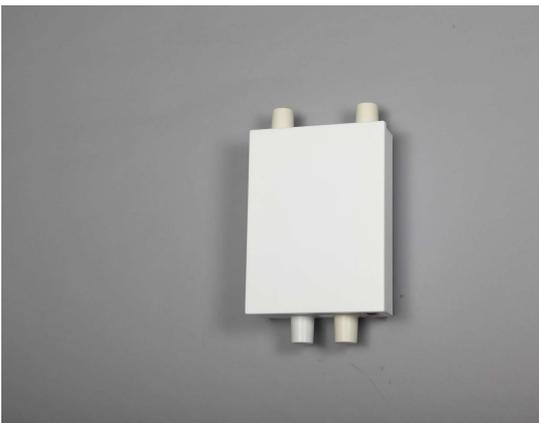
If physical security is mandated, simply concealing the wireless access point above a suspended ceiling or in a closet is not adequate. The access point, antennas, and associated cabling should be locked in place so as to prevent theft, tampering, vandalism, and accidental disruption and disconnects. Choose a locking solution which provides for securing access points and antennas in any environment in which they will be installed, including suspended ceilings, hard lid ceilings, wall mounts, warehouses, and outdoors. The physical security solution should also anticipate moves, adds and changes, and easily permit upgrades to new access points and antennas.



Secure, Convenient, Aesthetic suspended ceiling enclosures and mounts for wireless access points with non-detachable antennas or body integrated antennas



Suspended ceiling enclosures for wireless access points with detachable antennas. Interchangeable doors on enclosure permit easy upgrades to new APs and antennas.



Indoor/outdoor NEMA wall mounted security enclosures with antennas

Additional information on wireless network infrastructure is available at <http://www.oberonwireless.com/faq-resources.php>