Simplified (minimal) Wireless Access Point Security Guidelines

Network Evaluation

Tutorials and Guides to help enhance the integrity and security of your systems

Network Evaluation has developed a number of guidelines for effective wireless security. These are available in a separate document. For users who need to set up wireless equipment and do not have an IT staff, or available contractor, this list of recommendations will improve security significantly over default (out-of-the-box) factory configurations.

- Make use of WEP mandatory. If there is an option to refuse non-WEP requests, set it. Details of these administrative steps vary by manufacturer and model.
- Use 128 bit WEP encryption - Use of a complex pass-phrase is recommended over setting the key manually
- Assign a "strong" admin password to the wireless access point - preferably a phrase with synonyms or deliberate misspellings: e.g. "EyeEightAnnApple", "MeatMe@TheeMoveEase", or "HuhWyeUnVayCayShun" (Hawaiian Vacation).
- Set the SSID (also called ESSID) to a long complex value up to 31 or 32 characters. This should NOT be a phrase, since it's usually sent in clear text. Instead, it should be a cryptic string such as: "A;'30Xyu5AE458%au-0)vc#$523fx7". If the access point only supports upper-case alpha-numeric, then use something like this: "4F8943789TLDF9084KLVD89045MDV89R". Some older types of equipment do not allow for the full 32 characters. In that case make the string as long as is allowed. Since this phrase only needs to be entered once per computer (or other wireless device), it should not matter if it's difficult to type. That's the purpose - to make it harder to figure out.
- Limit the DHCP range (how many IP addresses the access point will hand out) to only the expected number of users, up to a maximum of 10% over the number of users expected if this is an area where the user load is less predictable. This can be expanded if need be, but will minimize the "free ISP" and snooping risk.
- Disable SNMP (if the device has that capability).
- Disable the “Remote Management” capability, unless specifically needed.
- Log traffic for investigational review in case problems are encountered or suspected. This can often be done within the access point device itself.
- Disable the SSID Broadcast capability
- Reduce the Transmit power of the Wireless Access Point to the lowest level that will work for systems in use.