LANCOM Systems

Guidelines for wireless LAN security in hotels

Security plays a central role in wireless networking in hotels – for management as well as guests. We have developed guidelines intended to inform you of the security features you should consider when selecting hardware components for your hotel wireless LAN and when configuring your network.

1) Keep the network you provide for guests separate from your core hotel network.

If you wish to provide your guests with Internet access, set up a separate guest network (hotspot/Public Spot) with web-based user authentication. Authentication ensures that only guests with appropriate access details can actually access the guest network. This network should be separated from all other networks through its own SSID – a freely selectable "name" for a wireless network. The server used for hotel administration and the hotel's accounting cannot be accessed from the guest network.

Do not allow guests within the guest SSID network to communicate with each other.
There is no need for PCs to communicate with each other within a guest network that is only intended to provide Internet access. On the contrary, this represents a security risk if guests have inadvertently set up shared directories on their laptops.

Tip: The best choice here is a hotspot option that can be activated on access points (base stations), wireless LAN controllers (central control and management devices) or routers, such as LANCOM's Public Spot option. In this way you require no additional infrastructure.

2) Encrypt SSIDs with WPA2.

Assign a dedicated SSID to each sub-network within your hotel network, for example the guest network, the administration network, the restaurant network, etc. Each of these sub-networks can additionally have encryption. You should observe the current standard of encrypting SSIDs with WPA2. You can assign each SSID its own WPA2 password in order to increase security.

In practice, guest networks are not usually encrypted since they are only used for guest Internet access. Authentication is then effected via a web-based interface (Public Spot). In contrast, networks for employees must always be encrypted. The differing security requirements of guest and employee networks mean that these networks must be separated from one another.

Note: Modern professional equipment generally comes with WPA2 as standard. We would strongly recommend converting to WPA2-based equipment if you still use old access points with WEP.

LANCOM Systems

3) Separate individual networks from one another at layer 2 or layer 3.

At layer 2 (= network layer 2) each SSID represents a dedicated network and is mapped to a virtual LAN (virtually separated network). The virtual LANs (e.g. guest network, administration, restaurant, etc.) must be separated from one another on the network components as well. Devices such as access points and switches (central network distribution devices) can be configured correspondingly.

Important: Your access points must support both multiple SSIDs and virtual LANs. Any switches in your network must also support virtual LANs.

Network separation at layer 3 (= network layer 3) no longer requires complex configuration of virtual LANs. Your network requires a wireless LAN controller that allows your access points to be managed centrally. A layer-3 tunnel between the access points and the wireless LAN controller separates the wireless LAN from the underlying network.

Advantage: It is considerably easier to configure this type of network and you can also use inexpensive switches that do not support virtual LANs.

4) Use a RADIUS server for your internal network.

Use a RADIUS server to authenticate wireless LAN users to ensure the highest level of security. A client logs into an access point or RADIUS server with a dedicated user name and password. Unknown clients will be rejected and will not gain access to the hotel network.

Tip: Purchase access points or wireless LAN controllers with an integrated RADIUS server. In this way you require no additional infrastructure. Alternatively, you can use an external RADIUS server.

You and your wireless LAN will be secure if you follow these recommendations.