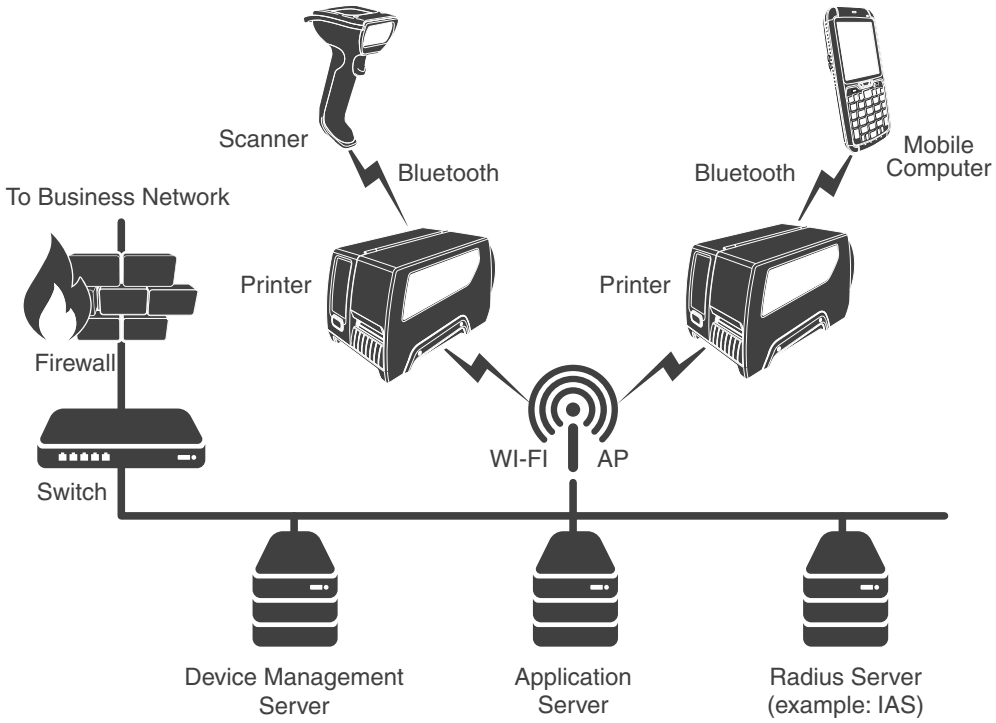
Printer Security Guide

Introduction

This Security Guide provides information and recommendations to the help the user understand how to configure the Honeywell printers for the highest levels of security on their network.

System Architecture

The illustration below provides an example of a system architecture that includes multiple printers and other devices such as scanners and mobile computers, a Wireless infrastructure (WLAN), a device management server, an application support server (for sending out the Print jobs to the printer), and a RADIUS server. The firewall exists to prevent the systems from having the direct access to the external networks or to the rest of business system network. It also exists to prevent those systems from accessing the Honeywell printers.



Firmware Binary Image

Honeywell recommends that the printer firmware and its extensions, such as simulators or other printer software, be kept up to date to reduce any security risks.

Password Authentication Policy and Management

The following user accounts and passwords are preconfigured on the printer by default. The printers do not have a root account.

User Account	Password
user	<No Password>
itadmin	pass
admin	pass

Honeywell recommends that the user change the default passwords and remove the unused user accounts to prevent a security breach. The password should be at least 12 characters in length, include special characters, and contain combinations of upper and lowercase characters. In addition, Honeywell recommends that you change passwords every 90 days.

Network Security

To ensure network security, Honeywell recommends that you configure proper network settings, including the firewall, router, and IDS settings. Honeywell also recommends that you turn off unused or unsecured network services, such as Telnet and FTP.

Here is a list of ports and services that can run on the Honeywell printers.

- Web server (Port 80)
- FTP (Port 21)
- Avalanche (Port 1777)
- NET1 service (Port 9100)
- SmartSystems (Port 62241)
- SNMP (Port 161)
- LPR (Port 515)
- IKEv2 (Port 500)
- SSH (Port 22)
- Telnet (Port 23)
- XML (Port 9001)
- NTP (Port 123)

Honeywell printers have all of the ports enabled by default except NTP and IKEv2. To disable the services running on these ports, use this procedure.

1. Open the printer user interface, printer web page, or Printset,
2. Go to **Settings** > **System Settings** > **Manage services** > and disable the identified service.

Bluetooth Security

Some Honeywell printers provide short-range wireless communications using Bluetooth wireless technology. Follow these security recommendations and precautions for Bluetooth security:

- Configure the printer to be non-discoverable. Enabling Bluetooth discovery advertises the Bluetooth address of the printer and allows anyone to pair and connect with the printer.
- Use a strong PIN or Password. If you are using legacy pairing (Bluetooth V2.0 and below), we recommend that you use a PIN of at least 8 digits.
- If possible, pair devices ONLY when in a physically secure area. Keep paired devices close together when possible to monitor both devices. Remove paired devices that are no longer in use.

Wi-Fi Security

Some Honeywell printers are equipped with an 802.11a/b/g/n Wireless Local Area Network (WLAN) radio. The radio is interoperable with other 802.11a/b/g/n, Wi-Fi compliant products, including access points (APs), workstations through PC card adapters, and other wireless portable devices.

When the printer connects through a wireless access point to an organization's server on a wired network, specific security precautions are required to mitigate the significant security risk the WLAN wireless AP connection represents for the servers and devices on the wired network.

Non-printing wireless devices (such as, laptops and printers) should either be on a separate WLAN with different security profiles or the wireless AP should support multiple service set identifiers (SSIDs). Devices on one WLAN should not be able to connect to devices on another of the organization's WLANs. By isolating the different networks from each other, the user helps to protect the printers and the other networks and devices from unauthorized access.

Secure Wireless AP Configuration

When configuring a wireless AP, Honeywell recommends that the user:

- Configure a unique SSID, and not to use the default SSID.
- Disable the SSID broadcast.
- Configure for the EAP authentication to the network. EAP-PEAP, EAP-TTLS, EAP-TLS and EAP-FAST are viable EAP methods. PEAP is preferred.
- Configure the RADIUS server address.

- Configure for the WPA2 Enterprise, change the AP RADIUS password, and do not to use the default password.
- Configure the 802.1x authentication.
- Enable MAC filtering and enter the MAC addresses for all the wireless devices. Performing these steps can help prevent unauthorized devices from connecting to the wireless network.

For detailed configuration information, refer to the setup instructions from the wireless AP supplier.

Secure Printer WLAN Configuration

For the WLAN configuration of the Printer, Honeywell recommends these settings:

- Configure the proper SSID.
- Configure the 802.1x authentication.
- Configure the Protected EAP authentication.
- Configure for EAP-LEAP, EAP-TLS, EAP-TTLS, EAP-FAST, and EAP-PEAP.
- If EAP-TLS or EAP-PEAP-TLS is in use, a client certificate must be available on the Printer.

Debug Log

Some Honeywell printers log the debug information/logs into a "/var/log/messages" file. It cannot be modified. The log information can be useful in analyzing the security attacks and also can perform limited intrusion detection. For example, you could see: Login userid/password failures.

Backup and Recovery

Honeywell recommends that users keep backups of the configuration settings, user applications, and user files. Keeping backup files makes it possible to return the printer to service quickly using the printer configuration capabilities if a failure occurs.

Recovery from Crashed System

The printer does not implement automatic recovery from a system hang or crash. The only recovery option is a system reboot.

Honeywell recommends that the user keep backups of the current and previous versions of the user applications and settings. In the event of a crash or other failure, user can quickly return the printer to service.