Honeywell

Network and Security

for Honeywell Printers

User Guide

Disclaimer

Honeywell International Inc. (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. HII makes no representation or warranties regarding the information provided in this publication.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material. HII disclaims all responsibility for the selection and use of software and/or hardware to achieve intended results.

Web Address: www.sps.honeywell.com

Trademarks

Google and Android are trademarks of Google LLC.

Bluetooth trademarks are owned by Bluetooth SIG, Inc., U.S.A. and licensed to Honeywell.

microSD is a registered trademark of SD-3C, LLC.

Qualcomm and Snapdragon are registered trademarks or trademarks of Qualcomm Incorporated in the United States and/or other countries.

Other product names or marks mentioned in this document may be trademarks or registered trademarks of other companies and are the property of their respective owners.

Patents

For patent information, refer to www.hsmpats.com.

Customer Support

Technical Assistance

Go to honeywell.com/PSStechnicalsupport to search our knowledge base for a solution or to log into the Technical Support portal.

Product Service and Repair

Honeywell International Inc. provides service for all of its products through service centers throughout the world. Go to sps.honeywell.com and select **Support** to find a service center near you or to get a Return Material Authorization number (RMA #) before returning a product.

Limited Warranty

For warranty information, go to sps.honeywell.com and click **Support** > **Warranties**.

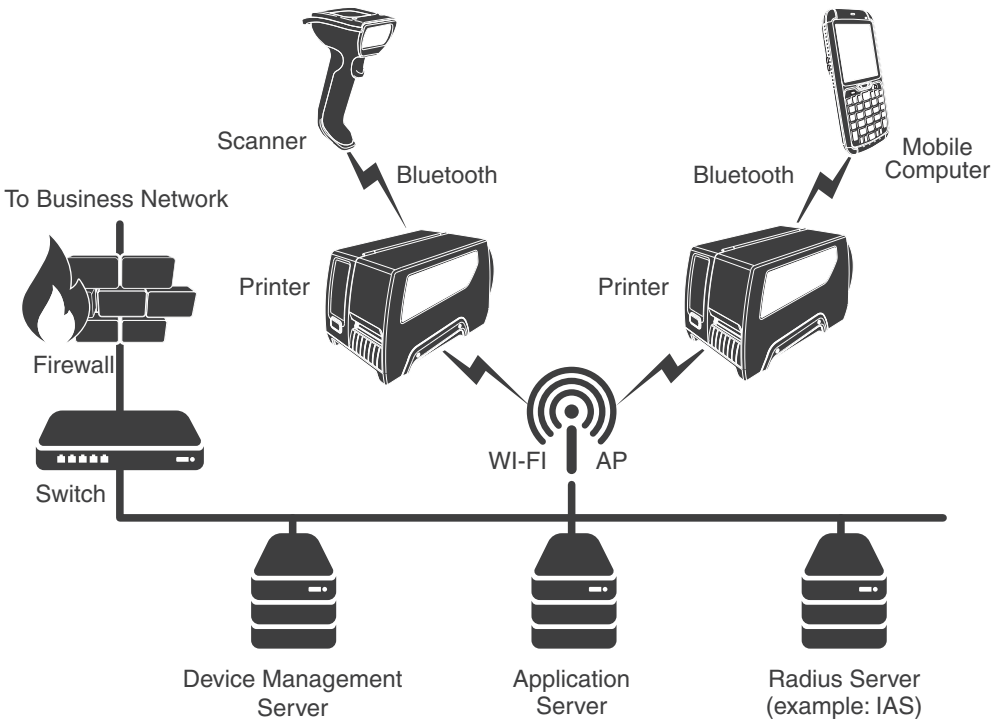
CHAPTER

1 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 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

The printer firmware and its extensions, such as simulators or other printer software must be kept up to date to reduce any security risks.

Note: *Honeywell recommends using up-to-date firmware with the latest features and security updates.*

Latest printer firmware release files are signed and authenticated for new printers (except PC43) to ensure authorized firmware updates.

Password Authentication Policy and Management

The following user accounts are available for initial configuration. Passwords must be changed on first log-in.

Note: *Honeywell recommends following the principle of least privilege.*

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

Honeywell recommends that the user change the default passwords and remove any unused 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.

When Fingerprint run command is used to change to admin / itadmin for system configuration, you need to change back to user account after the configuration is done.

Command:

```
run "su user"
```

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 443-recommended or Port 80-optional)
- SFTP (Port 22-disabled by default)

- FTP (Port 21-disabled by default)
- NET1 service (Port 9100)
- SNMP (Port 161)
- LPR (Port 515)
- SSH (Port 22-disabled by default)
- Telnet (Port 23-disabled by default)
- XML (Port 9200)
- NTP (Port 123-disabled by default)
- Device Management (Port 9300)
- Connectivity Agent (Port 10000-disabled by default)
- Verifier Integration Interface, VII (Port 9301-disabled by default)

To disable the services running on these ports:

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

Note: *Honeywell recommends using 802.1x over Ethernet for confidential data sending to the printer.*

Secure Communication

Below services can support TLS encrypted data communication. You can enable the feature under **Settings > Network Services**.

- Net1 service (Port 9100)
- XML Printing (Port 9200)
- Device Management (Port 9300)

Note: *Honeywell recommends to encrypt the communication over an open network.*

Bluetooth Security

Some Honeywell printers provide 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.

Note: *Honeywell recommends turning off Bluetooth communication if it is not required for your application.*

Wi-Fi Security

Some Honeywell printers are equipped with a Wireless Local Area Network (WLAN) radio. The radio is interoperable with other 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, it's important to use security precautions to mitigate any potential risk the WLAN AP connection may present to the servers and devices on the wired network.

Non-printing wireless devices should either be on a separate WLAN with different security profiles or the wireless AP should support multiple service set identifiers (SSIDs). 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 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 the WPA2 Enterprise, change the AP RADIUS password, and do not 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.

Printer Webpage (HTTP/HTTPS protocol)

The Honeywell printer web page supports both HTTP and HTTPS protocol. It is recommended for users to make use of https to access the printer web page for encrypted data transfer.

The certificate is self-signed, and modern web browsers may have a warning prompt indicating that the web page you are accessing may not be secured.

To avoid this warning prompt, IT administrators can install their custom certificates for HTTPS. This can be done by uploading the certificate into printer directory: /home/user/certificates/webserver

Note: *Honeywell recommends user to use a valid certificate from a Certificate Authority that would ensure robust security along with integrity and authenticity, instead of using self-signed certificate.*

The certificate must be in PEM (Privacy Enhanced Mail) format and must be named as: server.pem

Once uploaded into the directory, the printer must be rebooted for the certificate installation to take effect.

Only IT administrators, using the itadmin account, can upload or remove this certificate. Normal users and administrators will not be able to view or change the contents of this directory.

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

The printer does not implement automatic 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.

SNMP v1/v2 Support

Honeywell printers will eventually phase out SNMP v1/v2 support in future releases, and users are advised to migrate their network management infrastructure to use SNMP v3 that employs authentication and encryption security, and to stop using SNMP v1/v2 in their environment to ensure continued compatibility.

RFID

RFID (Radio frequency Identification) is a method to communicate information from one point to another point by the use of electromagnetic waves (radio waves). RFID has a unique characteristics that make it attractive for use in industrial systems.

Data and Tag Security

- Tag Passwords - You can set optional 32-bit passwords that allow you to access tag data, to lock tag data, or to permanently disable a tag.
- Data Locking Options- Tag memory can be safeguarded with flexible locking options. For example, you can lock a tag's memory to prevent it from being encoded accidentally and later unlock it for writing. A permanent locking feature prevents rewriting of tag data.

Honeywell
855 S. Mint Street
Charlotte, NC 28202

www.sps.honeywell.com

ALLSKU-PR-EN-SG-01 Rev E
08/22