Honeywell

THE POWER OF **CONNECTED**

Network and Security Guide

Honeywell Mobile Computers

with Android™ Operating Systems

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. The information in this publication does not represent a commitment on the part of HII.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for any damages, whether direct, special, incidental or consequential 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.

To the extent permitted by applicable law, Honeywell disclaims all warranties whether written or oral, including any implied warranties of merchantability and fitness for a particular purpose.

Web Address: www.honeywellaidc.com

Trademarks

Google, Google Play and Android are trademarks of Google Inc.

Microsoft is either a registered trademark or registered trademark of Microsoft Corporation in the United States and/or other countries.

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

microSD and microSDHC are trademarks or registered trademarks of SD-3C, LLC in the United States and/or other countries.

MITRE is a registered trademark of The MITRE Corporation.

Cisco and Catalyst are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.

UNIX is a registered trademark of The Open Group.

Wi-Fi and Miracast are registered trademarks of the Wi-Fi Alliance.

OpenSSL is a registered trademark of The OpenSSL Software Foundation, Inc.

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

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

TABLE OF CONTENTS

Customer Support

Technical Assistance

To search our knowledge base for a solution or to log in to the Technical Support portal and report a problem, go to www.hsmcontactsupport.com.

Product Service and Repair

Honeywell International Inc. provides service for all of its products through service centers throughout the world. To find your service center, go to www.honeywellaidc.com and select Support. Contact your service enter to obtain a Return Material Authorization number (RMA #) before you return the product.

To obtain warranty or non-warranty service, return your product to Honeywell (postage paid) with a copy of the dated purchase record.

Limited Warranty

For warranty information, go to www.honeywellaidc.com and click **Get Resources** > **Product Warranty**.

Send Feedback

Your feedback is crucial to the continual improvement of our documentation. To provide feedback about this manual, contact the Honeywell Technical Communications department at ACSHSMTechnicalCommunications@honeywell.com.

CHAPTER

1 INTRODUCTION

This guide defines the security processes, both implemented and recommended by Honeywell, for using Honeywell mobile computers with Android™ 4.0 or higher.

Intended Audience

The target audience for this guide is the customer organization that identifies and manages the risks associated with the use of information processing equipment. This includes, but is not limited to, Information Technology (IT). Third party organizations delivering and installing turnkey systems should also follow the guidelines in this guide. The intent of this guide is to drive the discussion between the organization using mobile computers with Android and the organization responsible for managing information technology risks.

A high degree of technical knowledge and familiarity in the following areas is assumed.

- Android 4.0 or higher operating systems.
- Networking systems and concepts.
- Wireless systems.
- Security issues and concepts. In particular, the following systems need to be understood and properly setup:
  - Radius Server
  - Mobile Device Management Software
  - Application Server (such as a Web server or Terminal Emulation server)

How to Use this Guide

Note: *Android references in this guide refer to devices with Android 4.0 or higher operating systems.*

If you have specific security concerns (e.g., the prevention of unauthorized access or virus protection), consult the Security Checklist (page 5) or select from the topics listed below.

Product Detail

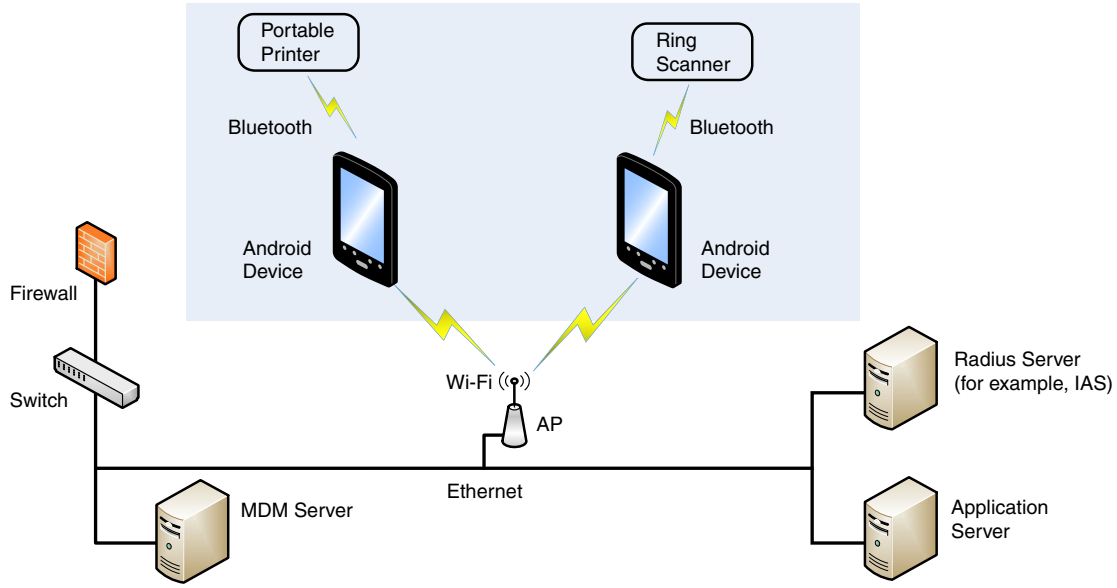
The Honeywell mobile computer with Android is a device intended for use in in-premise Automatic Data Collection (ADC) systems and for field ADC applications. In-premise systems typically exist in establishments such as distribution warehouses or retail stores. This type of system often uses terminal emulation servers or web servers to direct the Android to perform ADC operations (e.g., scanning during picking or placing of items). Field applications entail the use of the Android for field service applications and route distribution. Field service applications may use either Web applications or client applications that require different levels of connectivity to the customer servers.

System Architecture

The diagrams on page 3 illustrate sample architecture for in-premise and field system Android network deployments. In both examples, a firewall exists to prevent the systems from having direct access to external networks or the rest of the Business System Network (such as Finance or HR) and to prevent those systems from accessing the Android system.

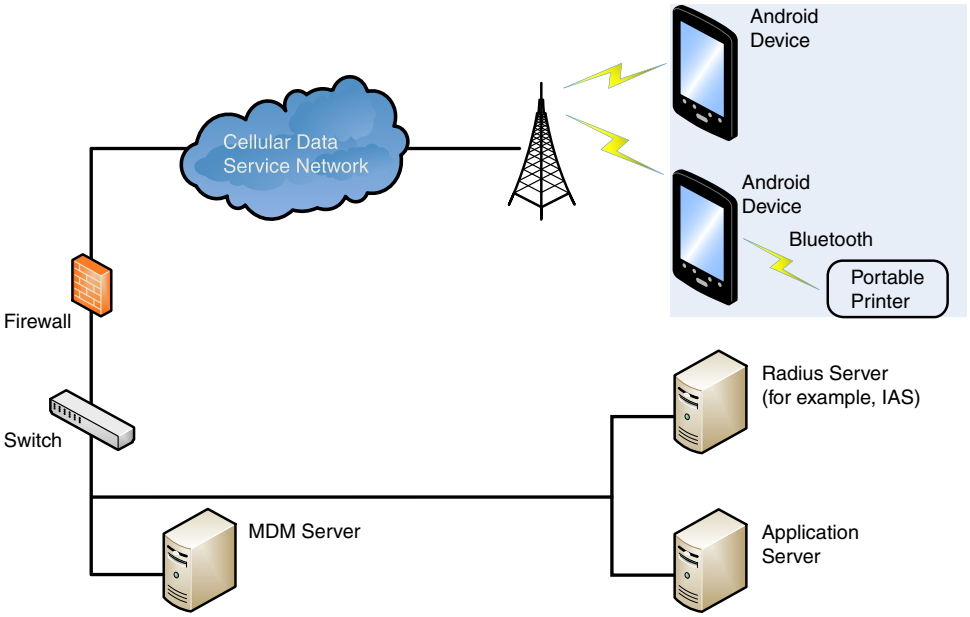
Architecture of an In-Premise Android System

The next diagram provides an example of in-premise system architecture that includes multiple Android with Android devices, a wireless LAN (WLAN), a mobile device management (MDM) server and an application support server (such as a web server or a terminal emulation server).



Architecture of a Field Service Android System

The next diagram provides an example of field application system architecture that includes Android devices, a wireless wide area network (WWAN, also known as wireless phone service), and web-applications, clients, and MDM servers.



Related Documents

User Guides	Additional Information
User Guides for Honeywell mobile computers powered by Android	Go to www.honeywellaidc.com to download the user guide specific to your computer model.
Dolphin Power Tools User Guide (for devices powered by Android)	

CHAPTER

2 SECURITY CHECKLIST

This chapter identifies common security threats that may affect networks containing Android devices. You can mitigate the potential security risk to your site by following the steps listed under each threat.

Infection by Viruses and Other Malicious Software Agents

This threat encompasses malicious software agents; for example, viruses, spyware (Trojans) and worms.

The intrusion of malicious software agents can result in:

- performance degradation,
- loss of system availability, and
- the capture, modification or deletion of data.

Mitigation Steps

Mitigation Steps
Ensure virus protection is installed, signature files are up-to-date, and subscriptions are active.
Allow only digitally signed software from trusted sources to run.
Use a firewall at the interface between other networks and Android devices.

Unauthorized External Access

This threat includes intrusion into the Honeywell Android system from the business network or other external networks including the Internet.

Unauthorized external access can result in:

- loss of system availability,
- the capture, modification, or deletion of data, and

- reputation damage if the external access security breach becomes public knowledge.

Mitigation Steps

Mitigation Steps	
Implement file system encryption.	https://source.android.com/devices/tech/security/encryption/
Use HTTPS when using Web servers across untrusted networks.	https://developer.android.com/training/best-security.html
Use a firewall at the interface between your other networks and Android devices.	
Secure wireless devices.	For information, see Secure Wireless Devices on page 19.
Set the minimum level of privilege for all external accounts, and enforce a strong password policy. This is especially true for Mobile Device Management (MDM) systems.	
Disable all unnecessary access ports, such as FTP.	
Use a VPN when the Android system requires data to traverse an untrusted network.	
Use SSL for communication between native applications and specialty servers.	https://developer.android.com/training/best-security.html
Use intrusion detection on WLAN networks.	

Unauthorized Internal Access

This threat encompasses unauthorized access from people or systems with direct access to a Android device. This threat is the most difficult to counter since attackers may have legitimate access to part of the system and are simply trying to exceed their permitted access.

Unauthorized internal access can result in:

- loss of system availability,
- the capture, modification, or deletion of data, and
- the theft or damage of system contents.

Mitigation Steps

Mitigation Steps	
Do not allow the use of unauthorized removable media, such as microSD™ or microSDHC™ cards, on Android devices.	https://developer.android.com/training/best-security.html
Implement password protection on Android devices.	Go to www.honeywellaidc.com to download the user guide specific to your computer model.
Monitor system access.	To learn more, see System Monitoring on page 23.

CHAPTER

3 DEVELOP A SECURITY PROGRAM

Form a Security Team

When forming a security team, you should:

- Define executive sponsors. It will be easier to ensure the success of security procedures if you have the backing of senior management.
- Establish a core cross-functional security team of representatives that include:
  - Building or facility management.
    Individuals responsible for running and maintaining Honeywell Android devices and infrastructure.
  - Business applications.
    Individuals responsible for applications interfaced to the Honeywell Android system.
  - IT systems administration.
  - IT network administration.
  - IT security.

Executive sponsorship and the creation of a formal team structure is a recommendation for the security program. The remaining tasks in the development of a security program are critical to the success of the program.

Identify Assets to be Secured

The term “assets” implies anything of value to the company. Assets may include equipment, intellectual property such as historical data and algorithms, and infrastructure capabilities such as network bandwidth and computing power.

When identifying assets at risk, you should consider:

- People, including your employees and the broader community to which they and your enterprise belong.
- Plant and Computer Equipment

    - Plant equipment including network equipment (e.g., routers, switches, firewalls, and ancillary items) used to build the system.
    - Computer equipment such as servers, cameras, and streamers.
- Network configuration information (e.g., routing tables and access control lists).
- Information stored on computing equipment (e.g., databases and other intellectual property).
- Intangible assets (e.g., bandwidth and speed).

Identify and Evaluate Threats

You need to consider the potential within your system for unauthorized access to resources or information through the use of a network, and the unauthorized manipulation and alteration of information on a network.

Potential threats to be considered include:

- People
    - Malicious users inside or outside the company.
    - Uninformed employees.
- Inanimate threats
    - Natural disasters such as fire or flood.
    - Malicious code such as a virus or denial of service.

Identify and Evaluate Vulnerabilities

Potential vulnerabilities that should be addressed in your security strategy include:

- The absence of security policies and procedures.
- Inadequate physical security.
- Gateways from the Internet to the corporation.
- Gateways between the business LAN and Android network.
- Improper management of modems.
- Out-of-date virus software.
- Out-of-date security patches or inadequate security configuration.
- Inadequate or infrequent backups.

Failure mode analysis can be used to assess the robustness of your network architecture.

Identify and Evaluate Privacy Issues

Consider the potential for unauthorized access to personal data stored within your system. Any information considered sensitive should be protected and all access methods should be reviewed to ensure correct authorization is required.

Create a Mitigation Plan

Create policies and procedures to protect your assets from threats. The policies and procedures should cover your networks, computer hardware and software, and Android equipment. You should also perform risk assessments to evaluate the potential impact of threats. A full inventory of your assets helps identify threats and vulnerabilities. These tasks assist you in deciding whether to ignore, mitigate, or transfer the risk.

Implement Change Management

A formal change management procedure is vital for ensuring any modifications made to the Android network continue to meet the same security requirements as the components included in the original asset evaluation and associated risk assessment and mitigation plans.

A risk assessment should be performed on any change made to the Android and its infrastructure that could affect security, including configuration changes, the addition of network components, and the installation of software. Changes to policies and procedures might also be required.

Plan Ongoing Maintenance

Constant vigilance of your security program should involve:

- Regular monitoring of your system.
- Regular audits of your network security configuration.
- Regular security team meetings where keeping up-to-date with the latest threats and technologies for dealing with security issues are discussed.

Additional Security Resources

Android	
Android Security Overview	https://source.android.com/security/
Android Open Source Project	https://source.android.com
Android Application Developers	https://developer.android.com

Android	
Android Security Team Contact Information	security@android.com
Android Security FAQ for Developers	https://developer.android.com/resources/faq/security.html
Android Security Best Practices for Developers	https://developer.android.com/guide/practices/security.html

Information Security Standards	
European Network and Information Security Exchange	http://www.enisa.europa.eu/
British Standards Institution - Information Security	http://www.bsi-global.com
International Organization for Standardization (ISO)	http://www.iso.org

Information Technology - Security Techniques	
ISO 15408 - Evaluation Criteria for IT Security, Parts 1 - 3	http://www.iso.org
ISO 27002 - Code of Practice for Information Security Management	http://www.iso.org
Open Web Application Security Project (OWASP) The OWASP tracks the top weaknesses of applications and provides valuable information about developing secure software.	http://www.owasp.org/

CHAPTER

4 DISASTER RECOVERY PLAN

This chapter describes the processes and tools recommended by Honeywell for the backup and restoration of the Android powered device to standard operation if disaster recovery is required due to data loss (e.g., deletion or corruption) and/or application inaccessibility or corruption.

The following actions are recommended as part of your disaster recovery plan.

- Perform routine backups of the Android powered device and any data located on external storage (i.e., microSD/SDHC card installed in the mobile computer).
- Save the backup files to a secondary location (e.g., off-site server) not on the Android powered device or the microSD card installed in the device.
- Perform routine disaster recovery testing.

Note: *If the microSD card is encrypted, a secondary backup is not possible.*

Honeywell Backup and Restore Power Tool Utility

The Backup Power Tool provides a utility for the backup and the restoration of settings and user data on the device. Once a backup is created using the utility, you can restore all the items or only those items you select. The type of item you can include in the backup varies depending on the OS version. The following list is a sample of common items you can include in the backup:

- Call Logs
- Contacts
- System Settings
- Music Play lists
- Browser Bookmarks

Access the Backup and Restore Power Tools

From the Home screen, select **All apps** > **Power Tools** > **Backup** to access the *Backup and Restore* utility screen.

Note: *Refer to the Dolphin Power Tools for devices powered by Android User's Guide for detailed information on the Backup and Restore Power Tools. Product guides are available for download at www.honeywellaidc.com.*

External Storage

The Backup Power Tool does not back up data saved on the microSD card installed in the mobile computer. You should perform a separate backup to ensure the safety of the data located on the memory card.

Any backup files located on the microSD card or the Android powered device device should be saved to a secondary external storage location for maximum safety in case the device is compromised. Backup files can then be used later to restore the Android powered device.

Note: *If the microSD card is encrypted, a secondary backup is not possible.*

Mobile Device Management Software

Create a backup of the Android powered device and upload the backup to the device management server.

Configuration information, current and previous versions of software, and supporting data files should be routinely backed up. Copies of the backups should be maintained in off-site storage for greatest safety. Device management software makes the processes of maintaining this data and restoring the data a controlled and feasible process.

Disaster Recover Testing

Disaster recovery plans should be tested at least once a year to confirm the current steps are valid and working as expected.

CHAPTER

5 SECURITY UPDATES AND SERVICE PACKS

One of the common weaknesses of system management as reported by, Open Web Application Security Project (OWASP) is "not keeping software up to date". It is critical to keep the latest patches and software versions on your Honeywell device powered by Android and supporting devices in the Android network. This is especially true for software that has reported Common Vulnerabilities and Exposures (CVE). The MITRE Corporation and the National Institute of Standards and Technology (NIST) track CVEs and mark their level of criticalness. For example, when a critical vulnerability was found in the popular OpenSSL® cryptographic software in April of 2014, the TLS heartbeat read overrun (CVE-2014-0160) was tracked and marked by both organizations. A CVE such as the CVE-2014-0160 must be addressed as soon as possible.

Honeywell provides system updates for both security and feature-related purpose. If the third-party software has been installed, Honeywell recommends testing the update on a non-production system to ensure Honeywell software continues to operate correctly.

Attention: Before installing any critical updates or making any system changes, ALWAYS back up the system. This will provide a safe and efficient recovery path if the update fails. See the Honeywell Backup and Restore Power Tool Utility, page 13.

Additional Resources

Security Resources	
The MITRE Corporation	http://www.mitre.org and http://cve.mitre.org
National Institute of Standards and Technology (NIST)	http://www.nist.gov
Open Web Application Security Project (OWASP)	http://www.owasp.org
U.S. National Vulnerability Database (NVD)	http://nvd.nist.gov

Honeywell SysInfo and Diagnostic Information

The SysInfo feature provides a read-out of important system information including firmware versions, application versions, system parameters, service pack versions, as well as network and radio information for your Android device.

To View System Information

1. From the Home screen, select **All apps** > **Power Tools**.
2. On computers with Android 4.0, select the **SysInfo** icon.
   On computers with Android 6.0 or higher, select **Diagnostic Information** > **SysInfo**. SysInfo queries the system, compiles the data and displays it on the SysInfo screen.

You cannot edit information in SysInfo. This information is gathered from the computer and changes only when the computer's configuration has changed.

Note: *To learn more, Refer to the Dolphin Power Tools user guide for devices powered by Android. Product guides are available for download at www.honeywellaidc.com.*

CHAPTER

6 NETWORK PLANNING AND SECURITY

Connect to the Business Network

The Honeywell mobile computer network and other networks (e.g., Internet or business network) should be separated by a firewall. See System Architecture on page 2. The nature of network traffic on a mobile computer network differs from other networks.

- The business network may have different access controls to other networks and services.
- The business network may have different change control procedures for network equipment, configuration, and software changes.
- Security and performance problems on the business network should not be allowed to affect the mobile computer network and vice versa.

Ideally, there should be no direct communication between the mobile computer network and the business network. However, practical considerations often mean a connection is required between these networks. The mobile computer network may require data from the servers in the business network or business applications may need access to data from the mobile computer network. A connection between the networks represents a significant security risk; therefore, careful consideration should be given to the system architecture design. Due to the security risk, it is strongly recommended that only a single connection is allowed and that the connection is through a firewall.

If multiple connections are required, a common practice is to create Data demilitarized zones (DMZ) where data servers that serve two different security domains are located. A DMZ is an area with some firewall protection, but is still visible to the outside world. Business network servers for Web sites, file transfers, and email are located in a DMZ. More sensitive, private services (e.g., internal company databases and intranets) are protected by additional firewalls and have all incoming access from the Internet blocked. You can also create an effective DMZ with just one firewall by setting up access control lists (ACLs) that let a subset of services be visible from the Internet.

Third Party Applications

Honeywell provides many applications to meet customer needs but there may be instances when a third party application must be added the computer.

If you want to add a third party application to the computer, always verify the following with the vendor before installation:

- Secure Development Lifecycle (SDL) practices were used by the vendor when writing the software.
- The proper means and security controls to mitigate any threats to the Android system are provided by the vendor.
- Secure network practices were used by the vendor for APIs to prevent accidental access to insecure networks. To learn more, see Secure Networking APIs on page 28.

In addition, make sure you evaluate additional risks to the Android system with regard to the following:

- The SLA agreement with the vendor.
- The change in the attack surface as a result of the software.
- Additional services used by the software that may consume needed resources for the computer with Android system.

If the above precautions cannot be done, then extra care must be taken in isolating and using the software. Additional settings might be needed in firewalls, point-to-point VPNs, or similar network features, depending on the additional risks in the third party software.

Note: *Third party software should be signed by a trusted authority before installation.*

CHAPTER

7 SECURE WIRELESS DEVICES

Wireless Local Area Networks and Access Point Security

All Android models are equipped with an 802.11x Wireless Local Area Network (WLAN) radio. The radio is interoperable with other 802.11x, Wi-Fi compliant products, including access points (APs), workstations via PC card adapters, and other wireless portable devices.

When the Android connects through a wireless access point (AP) 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-Android wireless devices (such as laptops and printers) should either be on a separate WLAN with different security profiles or the wireless AP should, at a minimum, support multiple service set identifiers (SSIDs). Devices on one WLAN should not be able to use the WLAN to connect to devices on another of the organization's WLANs. Isolation of different networks helps protect the Android system and the organization's other networks and devices from unauthorized access.

Secure Wireless AP Configuration

Honeywell recommends the following when configuring a wireless AP:

- Configure a unique SSID. Do not use the default SSID.
- Disable SSID broadcast.
- Configure authentication for EAP authentication to the network. PEAP and EAP-TLS are preferred.
- Configure the RADIUS server address.
- Configure for WPA2 Enterprise.
- Change the WAP RADIUS password. Do not use the default password.
- Configure 802.1x authentication.

- Enable MAC filtering and enter the MAC addresses for all the wireless devices. This prevents any unauthorized devices from connecting to the wireless network.

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

Secure Android WLAN Configuration

Honeywell recommends the following when configuring the Android for WLANs:

- Configure the proper SSID.
- Configure 802.1x authentication.
- Configure Protected EAP authentication.
- TLS, EAP-PEAP-TLS and EPA-PEAP-MSCHAP are supported.
- Configure the 802.1x supplicant (client) to prompt for the password needed by EAP-PEAP/MSCHAP, EAP-TTLS/MSCHAP.
- If EAP-TLS or EAP-PEAP-TLS are in use, a client certificate must be available on the Android.

Bluetooth™ Wireless Technology Security

All Android models are equipped for short-range wireless communication using Bluetooth wireless technology. Unless you plan to use Bluetooth devices, set Bluetooth to Off (**All Apps** >**Settings** > **Bluetooth**). Otherwise, follow the security recommendations and precautions listed below:

- Set the Android stack to non-discoverable.
- Set the Android stack to stop arbitrary pairings.
- Use a strong PIN or Password.
- If possible, pair devices ONLY when in a physically secure area.
- For devices with Android 4.4, set the visibility timeout to 2 minutes (**All Apps** > **Settings** > **Bluetooth** > **Menu** > **Visibility Timeout**).
- If simple secure pairing is used, Honeywell recommends that “just works” pairing is disabled.

Wireless Wide Area Network Security

Follow the security recommendations and precautions listed below for Wireless Wide Area (WWAN) Network security.

- Use HTTPS with Web applications with a locked down browser that allows access to only specified URLs. Make sure that the client is configured to validate the server certificate and uses sufficiently secure cipher suites.

- Use a secure Virtual Private Network (VPN) for remote access to the WWAN.
- Use TLS 1.2 between client applications and servers. Make sure the client is configured to validate the server certificate and uses secure crypto-suites.

Wireless Near Field Communication Security

Specific security precautions are recommended to mitigate the potential security risk associated with exchanging data using wireless Near Field Communication (NFC) between NFC enabled Honeywell devices and an NFC tags or other NFC enabled devices.

NFC security is based on the short range characteristic of the RF solution. In some applications, there is the potential for an attacker to utilize the Android Beam application and/or other applications to attack the Android powered device. For example, the Android Beam application can be used to exchange data between devices or from a tag to a device. The data exchange can include, but is not limited to, contacts, URLs, and applications. No confirmation is required on the receiving side of the connection and the Android device automatically runs the associated application. Attackers could potentially transfer a malicious URL and either trick the user into clicking it or exploit a browser bug to visit a malicious website and download malicious content.

Honeywell recommends the following security recommendations and precautions listed below:

- Disable NFC on the device unless it is critical to the application.
- If the application must allow NFC, it should only be enabled as needed and the user must have a means to confirm the transfer is expected. If the application transfers data between two Androids using NFC, then the application should enable encryption of the data.
- If the application must allow NFC but does not require the Android Beam feature to function, change the Android Beam protocol to Off (disabled) if NFC is enabled. You can change the device configuration using the Honeywell EZConfig software utility.

CHAPTER

8 SYSTEM MONITORING

The security recommendations outlined in this guide help reduce security risks but do not guarantee that an attacker may not be able to circumvent the safeguards put into place to protect network systems and devices including the Android. Early detection of an attack and/or system breach is essential to preventing further damage. The earlier a system intrusion is detected and the more evidence that is captured, the less damage is likely to occur and the greater the chances of identifying the intruder.

Providing a means to detect and document system exploits is vital. For example, the anti-virus package used should provide a method to collect logs created by the package. The logs should be available for retrieval via the package and a related console application on a server or via remote device management software. Periodical collection of additional logs (such as VPN connection information or login access failures) should also be implemented.

Intrusion Detection

Network Intrusion Detection Systems (NIDS) can take many forms. NIDS can be a dedicated server on the same network branch, freeware software available under GNU or similar licenses (often UNIX® based), or commercial products aimed specifically at Windows systems.

The purpose of NIDS is to scan incoming network packets and look for unusual traffic or for specific malformed packets known to be associated with attacks. If anomalies are found, NIDS take action such as raising alerts or even disconnecting the computer from the network. The latter is a dangerous option that causes denial of service while preventing damage from occurring to the system (e.g., by closing network ports).

Most firewalls, switches, and routers have reporting facilities whereby they can report various levels of events, varying from debugging to emergency failure. These reports can be viewed via secure shell (SSH), collected by a central logging server, or sent via email to an administrator. For example, the Cisco® PIX firewall

and Catalyst® 4500 switches can be configured to send selected levels of events to a central syslog server where further analysis can occur and significant events can be detected.

Remote Device Management

Honeywell recommends using a remote device management system to provision Android powered devices. The system should be used to monitor device software versions, applications and control any upgrade and/or downgrade processes.

To learn more about policy control for improved security, see Device Administration Policy (Recommended) on page 28.

CHAPTER

9 SECURE ACCESS TO THE ANDROID OPERATING SYSTEM

An essential component of any security strategy for computers in the network is to secure access to the operating system. Implementing access security measures ensures:

- Only authorized users have access to the system.
- User access to files, systems, and services is limited to those necessary for the performance of their duties.

Note: *To view security tips for Android systems, go to: https://developer.android.com/training/articles/security-tips.html.*

Basic Security Setup

The settings covered in this section are strongly recommended for your Android device.

Note: *To learn more about the device settings available on your computer, see the user guide for your specific model. User guides are available for download at www.honeywellaidc.com.*

SIM Card Lock

Enabling a SIM card PIN prevents unauthorized individuals from using the mobile computer as a phone or modifying data on the SIM card. Once enabled, you must enter a PIN to unlock your SIM card each time the phone is powered on.

Android 4.4

To access the SIM Card Lock settings from the Home screen, select **All Apps** > **Settings** > **Security** > **Set up SIM card lock**.

The recommended setting for the SIM Card Lock is enabled (checked) on WWAN Android models. The default setting is Off.

Screen Lock

Enabling a screen lock prevents unauthorized persons from accessing the mobile computer without a password, pin, or pattern to unlock the touch screen once it has been locked.

To access the Screen Lock settings from the Home screen, select **All Apps** > **Settings** > **Security** > **Screen Lock**.

The recommended setting for the Screen Lock is to enable a Password lock. Use a strong password value (e.g., include numbers, characters, special characters, and mix character case). Each device should have a unique password. There are five options: None, Slide, Pattern, PIN, or Password. The default setting is Slide.

Security Lock Timer

Once you have established a Screen Lock, additional settings appear on the screen depending on the type of security you implemented. When a Password screen lock is established, you can adjust the time increment for the screen to Automatically lock after entering Suspend (sleep) mode. This feature provides added security against unauthorized persons from accessing the device.

The recommended setting for Automatically lock is 10 minutes. The default setting is 1 minute.

Device Encryption

Full-Disk Encryption

Devices powered by Android 5.0 and higher support full-disk encryption.

When you select the Encrypt phone option from the security settings menu, all the data on the device is encrypted and protected by a single security key defined by the user (i.e., screen lock pin, password, or pattern).

Full-disk encryption makes it difficult for someone to pull readable data from a lost or stolen device since the key must be entered each time you power on the device. Before utilizing the Encrypt phone security option, you must set a Screen Lock (i.e., pin, password or pattern).

Note: *You cannot reverse full-disk encryption. The only way to revert back to an unencrypted state is to perform a factory reset, which erases all of your data.*

To access device encryption from the Home screen, select **All Apps** > **Settings** > **Security** > **Encrypt phone**.

Encrypting phone data is recommended to reduce risk of access to local confidential data on the device. Data is not encrypted by default on devices powered by Android 6.0 or lower.

File-Based Encryption

Devices powered by Android 7.0 and later support file-based encryption in addition to the optional full-disk encryption.

File-based encryption is implemented by default at the API level and cannot be turned off. A Screen Lock pin, password or pattern is not required for file-based encryption but Honeywell recommends you implement a password Screen Lock.

To learn more about Android device encryption, go to https://source.android.com/security/encryption/.

SD Card Encryption

If you plan on using an SD card in the device, and the SD card will be used to store sensitive data, Honeywell recommends that the SD card be encrypted.

On devices with Android 4.4:

From the Home screen, select **All Apps** >**Settings** > **Storage** > **Encrypt SDCard**.

On devices with Android 6:

1. From the Home screen, select **All Apps** >**Settings** > **Storage & USB.**
2. Select **SD Card** under “Portable Storage”.
3. Select the **more** icon (three vertical dots in the upper right corner) and choose **Format as internal**.

On devices with Android 7:

1. From the Home screen, select **All Apps** >**Settings** > **Storage.**
2. Select the **more** icon (three vertical dots in the upper right corner).
3. Select **Storage settings** > **Format as internal**.

Note: *The encrypted SD card will be unreadable on all other devices or PCs.*

USB Debugging

Developers use the USB debugging setting in conjunction with the Android Software Development Kit (SDK) to develop and debug apps. The recommended setting for USB debugging is disabled.

From the Home screen, select **All Apps** > **Settings** > **Developer options**. Verify the box next to “USB debugging” is not checked to disable the option.

Note: *Developer options including USB debugging are turned off by default.*

Bluetooth Wireless Technology

Bluetooth wireless technology on the device should be turned off (disabled) unless needed.

From the Home screen, select **All Apps** > **Settings** > **Bluetooth**. Verify "Bluetooth" is set to OFF.

If Bluetooth technology is enabled, the Android should only be made discoverable when absolutely necessary. The default and recommended setting is off (non-discoverable).

Note: *System bar icons at the top of the touchscreen indicate the status of the Bluetooth radio.*

NFC Wireless Technology

NFC wireless technology on the device should be disabled unless needed. From the Home screen, select **All Apps** > **Settings** > **More**. Verify the box next to "NFC" is not checked to disable the option. The default setting is on (enabled).

Note: *NFC functionality is hardware dependent and only available on select models. To learn if your device supports NFC, check the user guide for the model.*

Secure Networking APIs

When adding a third party application to the computer or developing new applications always make sure secure networking practices are implemented in API development. Third party application vendors should verify they used secure networking APIs and should define trust anchors, a debug-only override, prevention of clear-text transmission/reception and where possible, certificate pinning.

Device Administration Policy (Recommended)

The following table indicates the policies for Device Administration. Android allows remote administration capable of enforcing various policies provided by the Device Administration API. Honeywell recommends the use of Mobile Device Management (MDM) systems for policy control to provide the best available security. Policy recommendations and descriptions are provided in the next table.

Policy	Recommendation	Description
Password enabled	On	Requires that devices ask for PIN or passwords.
Minimum password length	12	Set the required number of characters for the password. For example, you can require PIN or passwords to have at least six characters.

<table>
<tr><th>Policy</th><th>Recommendation</th><th>Description</th></tr>
<tr><td>Alphanumeric password required</td><td>On</td><td>Requires that passwords have a combination of letters and numbers. They may include symbolic characters.</td></tr>
<tr><td>Complex password required</td><td>On</td><td>Requires that passwords must contain at least a letter, a numerical digit, and a special symbol.</td></tr>
<tr><td>Minimum letters required in password</td><td>1</td><td>The minimum number of letters required in the password for all admins or a particular admin.</td></tr>
<tr><td>Minimum lowercase letters required in password</td><td>1</td><td>The minimum number of lowercase letters required in the password for all admins or a particular admin.</td></tr>
<tr><td>Minimum non-letter characters required in password</td><td>1</td><td>The minimum number of non-letter characters required in the password for all admins or a particular admin.</td></tr>
<tr><td>Minimum numerical digits required in password</td><td>1</td><td>The minimum number of numerical digits required in the password for all admins or a particular admin.</td></tr>
<tr><td>Minimum symbols required in password</td><td>1</td><td>The minimum number of symbols required in the password for all admins or a particular admin.</td></tr>
<tr><td>Minimum uppercase letters required in password</td><td>1</td><td>The minimum number of uppercase letters required in the password for all admins or a particular admin.</td></tr>
<tr><td>Password expiration timeout</td><td>60 days (5,184,000)</td><td>When the password will expire, expressed as a delta in milliseconds from when a device admin sets the expiration time.
<table>
<tr><th>Days</th><th>Value</th><th>Recommended Usage</th></tr>
<tr><td>30</td><td>2,592,000</td><td>Critical usage case or when device users frequently change (multiple users)</td></tr>
<tr><td>60 (default)</td><td>5,184,000</td><td>Typical usage case</td></tr>
<tr><td>90</td><td>7,776,000</td><td>Less critical usage case</td></tr>
<tr><td>120</td><td>10,368,000</td><td>Very low security requirements</td></tr>
</table></td></tr>
<tr><td>Password history restriction</td><td>5</td><td>This policy prevents users from reusing the last n unique passwords. This policy is typically used in conjunction with setPasswordExpirationTimeout(), which forces users to update their passwords after a specified amount of time has elapsed.</td></tr>
<tr><td>Maximum failed password attempts</td><td>5</td><td>Specifies how many times a user can enter the wrong password before the device wipes its data. The Device Administration API also allows administrators to remotely reset the device to factory defaults. This secures data in case the device is lost or stolen.</td></tr>
</table>

Policy	Recommendation	Description
Maximum inactivity time lock	20	Sets the length of time since the user last touched the screen or pressed a button before the device locks the screen. When this happens, users need to enter their PIN or passwords again before they can use their devices and access data. The value can be between 1 and 60 minutes.
Require storage encryption	Off	Specifies that the storage area should be encrypted, if the device supports it.
Disable camera	Off	Specifies that the camera should be disabled. Note that this does not have to be a permanent disabling. The camera can be enabled/disabled dynamically based on context and time.
Make passwords visible	False	Specifies that the password will not be visible when typed. Verify that **Settings** > **Security** > **Make Passwords Visible** is not selected.
Disable the Browser Form Autofill option	True	Disables the browser auto-fill option. Verify that the **Browser app** > **Menu** > **Settings** > **General** > **Form auto-fill** feature is not selected.
Disable the use of plug-ins	True	Disables the use of browser plug-ins. Verify that the **Browser app** > **Menu** > **Advanced > Enable plug-ins** is not selected. Because the Chrome browser does not support plug-ins, this setting does not apply to Chrome.
Disable Google Play™	Disable	Disables automatic Google background services.
Full-Disk Encryption	On	To learn more, see "Full-Disk Encryption" on page 26. Devices powered by Android 5.0 or higher have full-device encryption turned off by default.
File-Based Encryption	On	On devices powered by Android 7 or higher, file-based encryption is turned on by default and cannot be turned off. To learn more Android device encryption, go to https://source.android.com/security/encryption/.
Storage Card Encryption	On	To learn more, see "SD Card Encryption" on page 27.
USB Mass Storage	Off	Specifies if a USB Mass Storage connection between the host and device is allowed. The default value is Off.
USB Host Storage	Off	Specifies if the device is allowed to connect and exchange data with an external storage device. The default value is On.
Google® Backup	Off	Specifies if data backup is permissible using Google backup. The default value is Off.
Android Beam	Off	Specifies the policy for Android Beam activation. Policy can be set to disable the Android Beam when NFC is enabled. To learn more about NFC and the Android Beam, see page 28. This policy is only supported on devices equipped with NFC technology. Setting can be adjusted using the Honeywell EZConfig software application.

Policy	Recommendation	Description
WiFi Direct	Off	Specify if a Wi-Fi connection is allowed without the use of an access point. Note: Policy not supported on CN75/CN75e or CK75 computers. Unless otherwise noted, this policy is supported on devices with Android 6.0 or higher. The default value is Off.
Google Account	Off	This policy is typically used in conjunction with setPasswordExpirationTimeout(), which enables or disables account management for specific account types. When account management is disabled, adding or removing an account for the specified type is not possible. Note: Policy not supported on CN75/CN75e or CK75 computers. Unless otherwise noted, this policy is supported on devices with Android 6.0 or higher running Google Mobile Services (GMS). The default is set to Off.
Miracast®	Off	Specifies if display mirroring to a secondary display (e.g., TV screen or laptop display) is permissible. Note: Policy is not supported on CN75/CN75e or CK75 computers. Unless otherwise noted, this policy is supported as Miracast source only on devices with Android 6.0 or higher. The default value is Off.

CHAPTER

10 NETWORK PORTS SUMMARY

Network Port Table

Port Used	Connection	Task	Comments
80	HTTP		Web Pages
443	HTTPS		Secure Web Pages

APPENDIX

A GLOSSARY

General Terms and Abbreviations

ACL	An Access Control List (ACL) is a list of user accounts and groups with each entry specifying a set of allowed, or disallowed actions. When applied to a firewall, an ACL is a list of device addresses and ports that may (or may not) pass through the device.
Authentication	When a user logs on to a system, the authentication process verifies the user is known to the system. See also "authorization".
Authorization	When a user logs on to a system, the authorization result dictates what a known user can do within the system. See also "authentication".
Business network	A collective term for the network and attached systems.
Digital signature	Using the private key of a digital certificate to encrypt the digital hash (digest) of an electronic document, code file, etc.
DMZ	Demilitarized zone (DMZ) is an area with some firewall protection, but which is visible to the outside world. This is where business network servers for Web sites, file transfers, and email are located.
Firewall	A firewall is a software or hardware barrier that sits between two networks, typically between a LAN and the Internet. A firewall can be a standalone network appliance, part of another network device such as a router or bridge, or special software running on a dedicated computer. Firewalls can be programmed to block all network traffic from coming through except that which has been configured to be allowed. By default, a firewall should block all 65,536 ports and open up only the ports you need. If you need to browse the Web, then it should allow "outgoing" traffic on port 80. If

	you would like DNS lookups to work for you, port 53 needs to be opened up for "outgoing" traffic. If you want to access your Internet mail server through POP3, open up port 110 for outgoing traffic. Firewalls are directional. They monitor where the traffic originates for both "incoming/inbound" and "outgoing/outbound" traffic. Quite frequently you will not want any unsolicited inbound traffic unless you have specific reasons (for example, you might have a Web server that you want people to access). However, in most cases, a Web server would probably be located outside your firewall and not on your internal network. This is the purpose of a demilitarized zone. The following Microsoft reference is a useful source of information about well known TCP/IP ports: http://support.microsoft.com/kb/832017.
IAS	Internet Authentication Service (IAS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy.
LAN	Local Area Network
Locking down	The procedure whereby a given user is given access to only one or a few specific programs is known as "locking down" a desktop or computer.
MAC	Media Access Control (MAC) is the lower level of the Data Link Layer (under the IEEE 802.11-1997 standard). In Wireless 802.11, MAC stands for "Medium Access Control". MAC can also be an abbreviation for "Message Authentication Codes", a cryptographic hash added to a message to enable the detection of tampering.
MDM	Mobile Device Management (MDM) technology provides the ability to deploy, secure, monitor, integrate, and manage mobile devices across multi-site enterprises. MDMs help manage the distribution of software updates, data, and configuration information across multiple devices or groups of devices. MDMs are also used to enforce security policies.
PEAP	Protected Extensible Authentication Protocol (PEAP) is a protocol proposed for securely transporting authentication data, including passwords, over 802.11 wireless networks.
Port	A port is a logical endpoint on a network computer or device used for communications. There are approximately 65,536 ports on which any one IP address can communicate. Some are dedicated to specific well-known services; some are used by application services; and some will be dynamically allocated to clients as they connect to remote services. A service

	listens on a known port for client connections, if the connection is accepted, the client will address messages to that port, and the server will send responses to the dynamically allocated client port.
RADIUS	Remote Authentication Dial In User Service (RADIUS) is a protocol that enables centralized authentication, authorization, and accounting for dial-up, virtual private network, and wireless access.
SDL	Security Development Lifecycle (SDL) is a software development process that helps developers to build more secure software and to address security requirements while reducing development cost.
SNMP	Simple Network Management Protocol (SNMP) is a protocol used to manage devices on IP networks.
SSID	Service set identifier (SSID) is a unique identifier for a wireless network.
Subnet	A group of hosts that form a subdivision of a network.
Subnet mask	A subnet mask identifies which bits of an IP address are reserved for the network address. For example, if the IP address of a particular computer or device is 192.168.2.3 with a subnet mask of 255.255.255.0, this subnet mask indicates the first 24 bits of the address represent the network address and the last 8 bits can be used for individual computer or device addresses on that network.
Switch	A switch is a multi-port device that moves Ethernet packets at full wire speed within a network. A switch may be connected to another switch in a network. Switches direct packets to a destination based on their MAC address. Each link to the switch has dedicated bandwidth (for example, 100 Mbps).
TCP/IP	Transmission Control Protocol/Internet Protocol.
TLS	Transport Layer Security
WAN	Wide Area Network
WAP	Wireless Access Point
WPA	Wi-Fi Protected Access (WPA) is a security standard adopted by the Wi-Fi Alliance consortium for wireless networks (www.wi-fi.org).
WPA2	Wi-Fi Protected Access 2 is the replacement for WPA.

Honeywell
9680 Old Bailes Road
Fort Mill, SC 29707

www.honeywellaidc.com