Honeywell

# Dolphin™ 70e Black

powered by Android

## Network and Security 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*

Android is a trademark 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 is a registered trademark of 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.

# Table of Contents

## *Chapter 7 - Securing Wireless Devices*



## *Chapter 8 - System Monitoring*



## *Chapter 9 - Securing Access to the Android 4.0 Operating System*



## *Chapter 10 - Network Ports Summary*



## *Chapter 11 - Glossary*



## *Chapter 12 - Customer Support*

# 1 Introduction

This guide defines the security processes, both implemented and recommended by Honeywell, for using the Dolphin™ 70e Black mobile computer with Android™4.0.

## Intended Audience

The target audience for this guide is the Dolphin 70e Black with Android 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 the Dolphin 70e Black 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 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 (e.g., Remote MasterMind™)
  - Application Server (e.g., Web server or Terminal Emulation server)

## How to Use this Guide

*Note: Dolphin 70e Black references in this guide refer to devices with Android 4.0 operating systems.*

If you have specific security concerns (e.g., virus protection or preventing unauthorized access), consult the Security Checklist (page 2-1) or select from the topics listed below.



## Product Detail

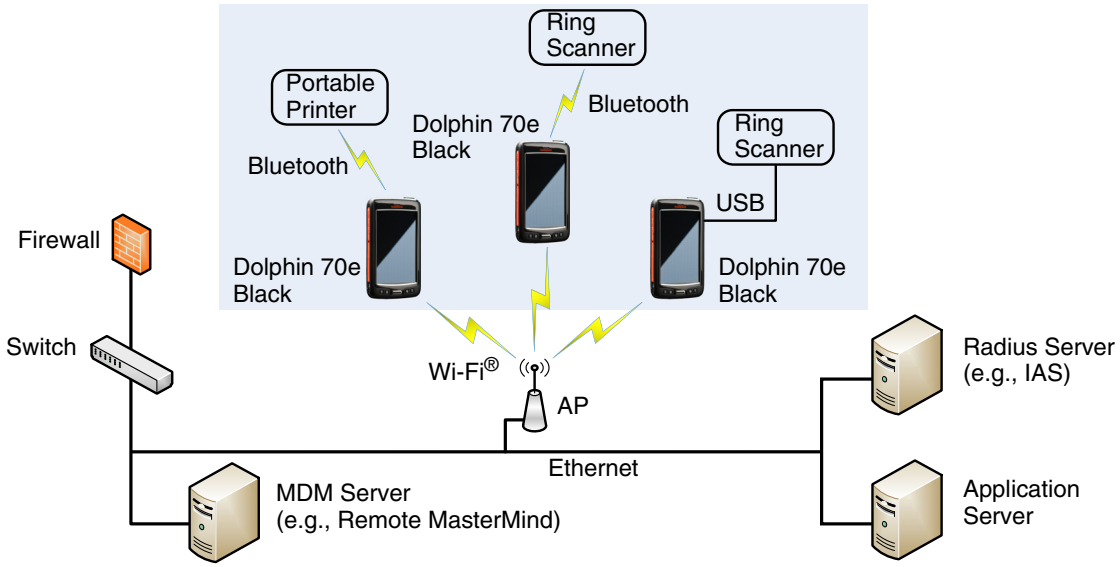
The Honeywell Dolphin 70e Black is a device intended for use in in-premise Automatic Data Collection (ADC) systems and for field ADC applications. In-premise systems typically exist in establishments such as distribution warehouses or retail stores. This type of system often uses terminal emulation servers or web servers to direct the Dolphin 70e Black to perform ADC operations (e.g., scanning during picking or placing of items). Field applications entail the use of the Dolphin 70e Black 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 1-2 illustrate sample architecture for in-premise and field system Dolphin 70e Black 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 (e.g., Finance or HR) and to prevent those systems from accessing the Dolphin 70e Black system.

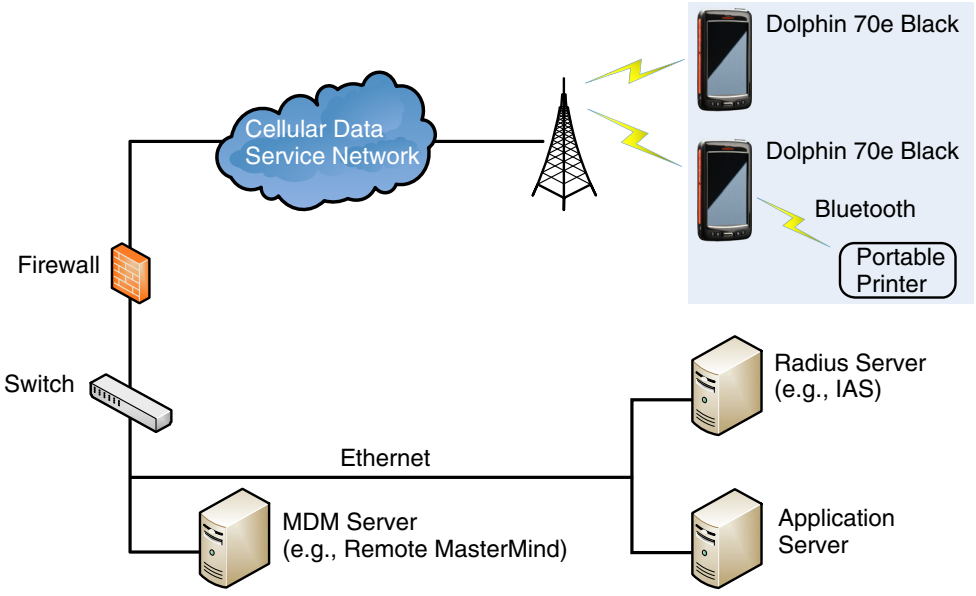
## *Architecture of an In-Premise Dolphin 70e Black System*

The diagram below provides an example of in-premise system architecture that includes multiple Dolphin 70e Black with Android devices, a wireless LAN (WLAN), a mobile device management (MDM) server (e.g., Honeywell's Remote MasterMind device management software) and an application support server (e.g., web server or a terminal emulation server).




## *Architecture of a Field Service Dolphin 70e Black System*

The diagram below provides an example of field application system architecture that includes Dolphin 70e Black with Android devices, a wireless wide area network (WWAN) (e.g., wireless phone service), and web-applications, clients, and MDM servers (e.g., Remote MasterMind device management software).



## *Related Documents*

| User's Guides | Additional Information |
|---|---|
| Dolphin 70e Black powered by Android User's Guide | Available for download from the Dolphin 70e Black product page at www.honeywellaidc.com. |
| Dolphin Power Tools for devices powered by Android User's Guide | |

# 2 Security Checklist

This chapter identifies common security threats that may affect networks containing Dolphin 70e Black 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 Dolphin 70e Black devices. | |

## Unauthorized External Access

This threat includes intrusion into the Honeywell Dolphin 70e Black 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/encryption/android_crypto_implementation.html |
| Use HTTPS when using Web servers across untrusted networks. | http://developer.android.com/training/articles/security-ssl.html |
| Use a firewall at the interface between your other networks and Dolphin 70e Black devices. | |
| Secure wireless devices. | |
| 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 (e.g., FTP). | |
| Use a VPN when the Dolphin 70e Black system requires data to traverse an untrusted network. | |
| Use SSL for communication between native applications and specialty servers. | http://developer.android.com/training/articles/security-ssl.html |
| Use intrusion detection on WLAN networks. | |

## Unauthorized Internal Access

This threat encompasses unauthorized access from people or systems with direct access to a Dolphin 70e Black 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 (e.g., microSD™ or microSDHC™ cards) on Dolphin 70e Black devices. | http://source.android.com/devices/tech/security/index.html |
| Implement password protection on Dolphin 70e Black devices. | Refer to the Dolphin 70e Black *powered by Android User's Guide* available for download at www.honeywellaidc.com.<br><br>http://source.android.com/devices/tech/security/index.html#password-protection. |
| Monitor system access. | |

# 3 Developing a Security Program

## Forming 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 consisting of representatives from:
  - Building or facility management (i.e., individuals responsible for running and maintaining Honeywell Dolphin 70e Black devices and infrastructure).
  - Business applications (i.e., individuals responsible for applications interfaced to the Honeywell Dolphin 70e Black 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.

## Identifying Assets to be Secured

The term “assets” implies anything of value to the company. Assets may include equipment, intellectual property (e.g., historical data and algorithms), and infrastructure (e.g., 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.
- Equipment
  - Plant equipment including network equipment (e.g., routers, switches, firewalls, and ancillary items used to build the system).
  - Computer equipment (e.g., 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).

## Identifying and Evaluating 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 (e.g., malicious users inside or outside the company and uninformed employees).
- Inanimate threats
  - natural disasters (e.g., fire or flood)
  - malicious code (e.g., a virus or denial of service).

## Identifying and Evaluating 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 Dolphin 70e Black 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.

## Identifying and Evaluating 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.

## Creating 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 Dolphin 70e Black 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.

## Implementing Change Management

A formal change management procedure is vital for ensuring any modifications made to the Dolphin 70e Black 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 Dolphin 70e Black 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.

## Planning 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 | http://source.android.com/devices/tech/security/index.html |
| Android Open Source Project | https://source.android.com |
| Android Application Developers | https://developer.android.com |
| 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 |
| Android Security Community Discussion Groups | https://groups.google.com/forum/?fromgroups#!forum/android-security-discuss |

| **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)<br>*Note: The OWASP tracks the top weaknesses of applications and provides valuable information about developing secure software.* | http://www.owasp.org/ |

# 4 Disaster Recovery Planning

This chapter describes the processes and tools recommended by Honeywell for the backup and restoration of the Dolphin 70e Black 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 Dolphin 70e Black and any data located on external storage (i.e., microSD/SDHC card installed in the terminal).
- Save the backup files to a secondary location (e.g., off-site server) not on the Dolphin 70e Black or the microSD card installed in the device.
  *Note: If the microSD card is encrypted, a secondary backup is not possible.*
- Perform routine disaster recovery testing.

## Honeywell Backup and Restore Power Tool Utility

The Dolphin **Backup** Power Tool provides a utility for the backup and restoration of settings and user data on the terminal. The items listed below can be included in the backup. Once a backup is created using the utility, you can restore all the items or only those items you select.

- Call Logs
- Contacts
- Messages
- System Settings
- Music Playlists
- Browser Bookmarks
- Wi-Fi® firmware configure file
- Wi-Fi daemon APP configure file

### Accessing 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 terminal. 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 Dolphin 70e Black 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 Dolphin 70e Black.

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

## Remote MasterMind Device Management Software

Create a backup of the Dolphin 70e Black and upload the backup to the Remote MasterMind 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. Remote Mastermind software makes the processes of maintaining this data and restoring this data a well-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.

# 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 Dolphin 70e with Android and supporting devices in the Dolphin 70e Black 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 4-1.**

### 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 Power Tool

The **SysInfo** Power Tool 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 Dolphin 70e Black device.

### To View System Information

From the Home screen, select **All apps** > **Power Tools**. Touch the **SysInfo** icon once. 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 Dolphin terminal and changes only when the terminal's configuration has changed.

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

# 6 Network Planning and Security

## Connecting to the Business Network

The Dolphin 70e Black network and other networks (e.g., Internet or business network) should be separated by a firewall. See System Architecture on page 1-2.

The nature of network traffic on a Dolphin 70e Black 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 Dolphin 70e Black network and vice versa.

Ideally, there should be no direct communication between the Dolphin 70e Black network and the business network. However, practical considerations often mean a connection is required between these networks. The Dolphin 70e Black network may require data from the servers in the business network or business applications may need access to data from the Dolphin 70e Black 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 most of the applications that meet the needs of Dolphin 70e Black customer. In instances where a third party application must be added the the Dolphin 70e Black, always verify the following with the vendor:

- Secure Development Lifecycle (SDL) practices were used when writing the software.
- The proper means and security controls to mitigate any threats to the Dolphin 70e Black system are provided.

In addition, evaluate additional risks to the Dolphin 70e Black 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 Dolphin 70e Black 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.*

# 7

# Securing Wireless Devices

## Wireless Local Area Networks (WLAN) and Access Points (APs) Security

All Dolphin 70e Black models 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 via PC card adapters, and other wireless portable devices.

When the Dolphin 70e Black device 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-Dolphin 70e Black wireless devices (e.g., 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 Dolphin 70e Black 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 is 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 Dolphin 70e Black WLAN Configuration

Honeywell recommends the following when configuring the Dolphin 70e Black for WLANs:

- Configure the proper SSID.
- Configure 802.1x authentication.
- Configure Protected EAP authentication.
  *Note: 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 Dolphin 70e Black device.

## Bluetooth™ Wireless Technology Security

All Dolphin 70e Black models are equipped for short-range wireless communication using Bluetooth wireless technology. Follow the security recommendations and precautions listed below:

- Set the Dolphin 70e Black stack to non-discoverable.
- Set the Dolphin 70e Black stack to stop arbitrary pairings.
- On the Dolphin 70e Black, disable unused Bluetooth profiles.
- Use a strong PIN or Password.
- If possible, pair devices ONLY when in a physically secure area.

## Wireless Wide Area Network (WWAN) Security

Follow the security recommendations and precautions listed below for WWAN 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 (NFC) 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 Dolphin 70e Black 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 Dolphin 70e Black 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 Dolphin 70e Black 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 Dolphin 70e Black 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 Dolphin 70e Black devices using NFC, then the application should enable encryption of the data.

# 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 Dolphin 70e Black. 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, (e.g., Remote Mastermind software). Periodical collection of additional logs (e.g., 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.

# 9 Securing Access to the Android 4.0 Operating System

An essential component of any security strategy for computers in the Dolphin 70e Black 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: The following link provide overview information about the security tips of the Android system: https://developer.android.com/training/articles/security-tips.html.*

## Basic Security Setup

The following settings are strongly recommended for your Dolphin 70e Black device.

*Note: Refer to the Dolphin 70e Black powered by Android User's Guide, for detailed information on device settings. Product guides are available for download at www.honeywellaidc.com.*

### SIM Card Lock

Enabling a SIM card PIN prevents unauthorized individuals from using the terminal 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.

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 Dolphin 70e Black models. The default setting is Off.

### Screen Lock

Enabling a screen lock prevents unauthorized persons from accessing the terminal 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 Dolphin 70e Black 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 under the "Screen Security" heading 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 Dolphin 70e Black device.

The recommended setting for **Automatically l**ock is 10 minutes. The default setting is one minute.

### Device Encryption

**Encrypt phone** is an advanced security option. By encrypting all the data on your phone, you make it difficult for someone to pull readable data from the Dolphin 70e Black if the device is lost or stolen. When the phone is encrypted, you must enter a password each time you power on the device. A **Screen Lock** password must be set before utilizing device encryption.

**Warning:** You cannot reverse 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 not recommend unless there is risk of access to local confidential data on the Dolphin 70e Black. Data is not encrypted by default on the Dolphin 70e Black.

### *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.

### *Bluetooth Wireless Technology*

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

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

If Bluetooth technology is enabled, the Dolphin 70e Black 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 Dolphin 70e Black models ending with the letter N (e.g., 70exxN).*

## *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 Remote MasterMind software or other MDM systems to manage the policies to provide the best available security. In the Recommendation column, an entry indicates recommended policy.

| 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. |
| Alphanumeric password required | On | Requires that passwords have a combination of letters and numbers. They may include symbolic characters. |
| Complex password required | On | Requires that passwords must contain at least a letter, a numerical digit, and a special symbol. |
| Minimum letters required in password | 1 | The minimum number of letters required in the password for all admins or a particular admin. |
| Minimum lowercase letters required in password | 1 | The minimum number of lowercase letters required in the password for all admins or a particular admin. |
| Minimum non-letter characters required in password | 1 | The minimum number of non-letter characters required in the password for all admins or a particular admin. |
| Minimum numerical digits required in password | 1 | The minimum number of numerical digits required in the password for all admins or a particular admin. |
| Minimum symbols required in password | 1 | The minimum number of symbols required in the password for all admins or a particular admin. |

| Policy | Recommendation | Description |
|---|---|---|
| Minimum uppercase letters required in password | 1 | The minimum number of uppercase letters required in the password for all admins or a particular admin. |
| Password expiration timeout | 60 days (5,184,000) | When the password will expire, expressed as a delta in milliseconds from when a device admin sets the expiration time.<br><br>**Days** **Value** **Recommended Usage**<br>30 2,592,000 Critical usage cases or when Dolphin 70e Black users might change frequently (multiple users)<br>60 (default) 5,184,000 Typical usage cases<br>90 7,776,000 Less critical usage cases<br>120 10,368,000 Very low security requirements |
| Password history restriction | 5 | 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. |
| Maximum failed password attempts | 5 | 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. |
| 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. |

# 10 Network Ports Summary

## Network Port Table

| Port Used | Connection | Task | Comments |
|---|---|---|---|
| 80 | HTTP | | Web Pages |
| 443 | HTTPS | | Secure Web Pages |
| 3790 | SSL | Remote MasterMind | |

# 11 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.<br><br>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.<br><br>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.<br><br>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. An example of MDM is the Remote MasterMind software. |
| 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. |
| Remote MasterMind | Device management software available from Honeywell to facilitate the management of mobile computers, smartphones, and bar code scanners across multi-site enterprises. |

| | |
|---|---|
| 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.<br><br>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. |

# 12 Customer Support

## Product Service and Repair

Honeywell International Inc. provides service for all of its products through service centers throughout the world. To obtain warranty or non-warranty service, please visit www.honeywellaidc.com and select **Support > Contact Service and Repair** to see your region's instructions on how to obtain a Return Material Authorization number (RMA #). You should do this prior to returning the product.

For ongoing and future product quality improvement initiatives, the Dolphin 70e Black comes equipped with an embedded device lifetime counter function. Honeywell may use the lifetime counter data for future statistical reliability analysis as well as ongoing quality, repair and service purposes.

## Technical Assistance

If you need assistance installing or troubleshooting your device, please contact us by using one of the methods below:

**Knowledge Base:** www.hsmknowledgebase.com

Our Knowledge Base provides thousands of immediate solutions. If the Knowledge Base cannot help, our Technical Support Portal (see below) provides an easy way to report your problem or ask your question.

**Technical Support Portal:** www.hsmsupportportal.com

The Technical Support Portal not only allows you to report your problem, but it also provides immediate solutions to your technical issues by searching our Knowledge Base. With the Portal, you can submit and track your questions online and send and receive attachments.

**Web form:** www.hsmcontactsupport.com

You can contact our technical support team directly by filling out our online support form. Enter your contact details and the description of the question/problem.

**Telephone:** www.honeywellaidc.com/locations

For our latest contact information, please check our website at the link above.

Honeywell Scanning & Mobility
9680 Old Bailes Road
Fort Mill, SC  29707

www.honeywellaidc.com