Honeywell

# Windows Mobile 6.5

## 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 Windows Mobile 6.5 Operating System*



## *Chapter 10 - Network Ports Summary*



## *Chapter 11 - Customer Support*

# 1 Introduction

This guide defines the security processes, both implemented and recommended by Honeywell, for all mobile computers running the Windows Mobile 6.5 operating system.

## Intended Audience

The target audience for this guide is the Windows Mobile 6.5 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 Windows Mobile 6.5 devices and the organization responsible for managing information technology risks. Honeywell will not be held responsible for the use of Windows Mobile 6.5 devices that does not comply with the best practices described in this document.

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

- Microsoft Windows Mobile 6.5
- Networking systems and concepts.
- Wireless systems.
- Security issues and concepts. In particular, the following systems need to be understood and properly setup:
  - Radius Server
  - Application Server (such as a web server or terminal emulation server)
  - Exchange Server (if used to set security policies)

## How to Use this Guide

*Note: WM6.5 references in this guide refer to Windows Mobile 6.5 devices.*

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

Honeywell mobile devices are 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 Honeywell mobile device to perform ADC operations (e.g., scanning during picking or placing of items).

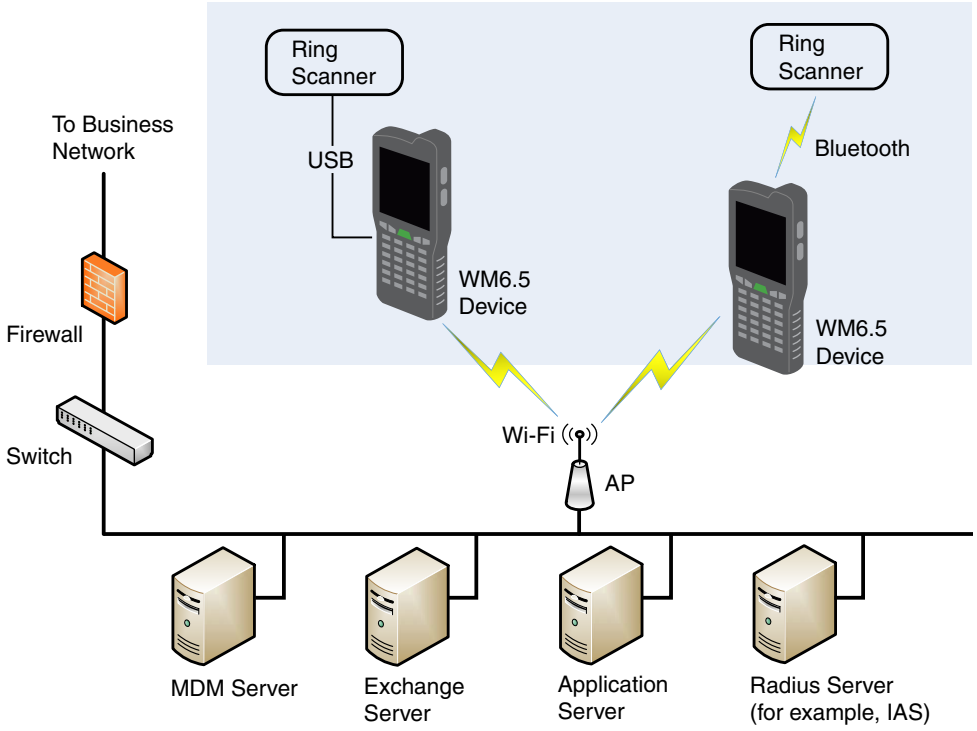
## System Architecture

The diagrams in this section illustrate sample architecture for in-premise and field system 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 mobile device system.

### Architecture of an In-Premise System

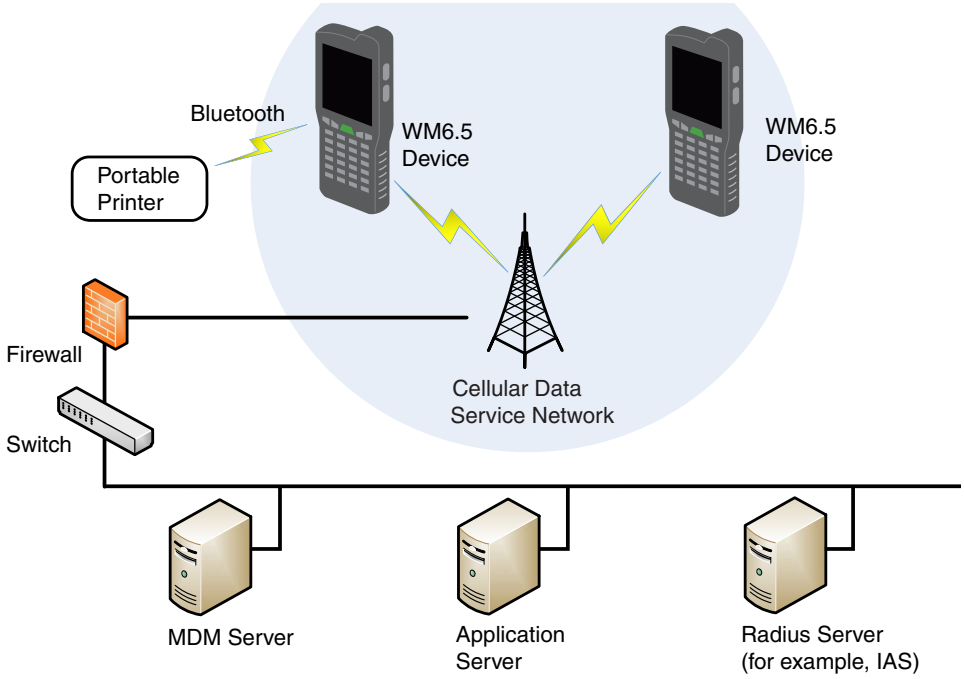
The diagram below provides an example of in-premise system architecture that includes multiple mobile devices, a wireless LAN (WLAN), a mobile device management (MDM) server, WM6.5 mobile devices, and an application support server (such as a web server or terminal emulation server). A Microsoft Exchange server may be present to allow security policies to be automatically supported in the WM6.5 devices.

A firewall prevents direct access from the system to the rest of the Business Systems Network (such as financial, HR, or other systems), and prevents the business systems from accessing the WM6.5 system.



### *Architecture of a Field Service System*

The diagram below provides an example of field application system architecture that includes cellular-based WM6.5 devices, a wireless wide area network (WWAN, or wireless phone service), and web applications, clients, and MDM servers.




## *Related Documents*

To download documentation for your Honeywell products:

1. Go to www.honeywellaidc.com.
2. Select **Resources** > **Download**.
3. Select your Honeywell product from the **Please make a selection** list and then click the red arrow.

# 2 Security Checklist

This chapter identifies common security threats that may affect networks containing Windows Mobile 6.5 (WM6.5) 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 that virus protection and the latest WM6.5 software are installed on the device. | http://www.kaspersky.com/downloads/trials/kms-trial-winmobile |
| Enable trusted mode on the WM6.5 device. Allow only digitally signed software from trusted sources to run. | |
| Allow only digitally signed software from trusted sources to run. | All software is required to be digitally signed. Drivers and Services cannot be installed by end user due to system construction. |
| Use a firewall at the interface between other networks and WM6.5 devices. | |

## Unauthorized External Access

This threat includes intrusion into the Honeywell WM6.5 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. | |
| Use Secure Hypertext Transfer Protocol (HTTPS, with TLS 1.0 or greater) or your virtual private network (VPN) when using Web servers across untrusted networks. | http://msdn.microsoft.com/en-us/library/windows/apps/xaml/hh849625.aspx#require_https_connections |
| Use a firewall at the interface between your business network and the WM6.5 network. | |
| 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. | Mobile Device Management (MDM) software |

| Mitigation Steps | |
|---|---|
| Honeywell recommends that you avoid the use of non-secure protocols such as File Transfer Protocol (FTP) or Telnet. | The construction of the operating system (OS) does not allow an application to disable ports that another application may require. To disable a port, you can remove the application that uses that port. If the application cannot be removed, set the security for that application to "one-tier prompt," and then disable prompting to effectively prevent users from running the application. For more information, see Securing Access to the Windows Mobile 6.5 Operating System on page 9-1.<br><br>Alternatively, you can use a locked-down menu program (such as Launcher for Windows or Enterprise Launcher) to prevent users from accessing specific applications. |
| Use the Windows Mobile VPN when the WM6.5 system requires data to traverse an untrusted network. | http://msdn.microsoft.com/en-us/library/cc440255.aspx |
| Use HTTPS (with TLS 1.0 or greater) when using web servers across untrusted networks. | |
| Use Transport Layer Security (TLS) 1.0 or greater for communication between native applications and specialty servers. | http://blogs.windows.com/buildingapps/2014/10/13/winsock-and-more-open-source-for-your-windows-store-apps/ |
| Use intrusion detection on wireless local area networks (WLANs). | See Intrusion Detection, page 8-1, or http://www.sans.org/security-resources/idfaq/ |

## *Unauthorized Internal Access*

This threat encompasses unauthorized access from people or systems with direct access to a WM6.5 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 | More Information |
|---|---|
| Do not allow the use of unauthorized removable media (for example, Secure Digital (SD) cards) on WM6.5 devices. | http://msdn.microsoft.com/en-us/magazine/cc982153.aspx |
| Monitor system access. | |
| Use and enforce a strong password policy on WM6.5 devices. | |
| Secure wireless devices. | |
| When using ActiveSync to connect to the WM6.5 device, Honeywell recommends that you disable Desktop Passthrough (DTPT) which can allow unexpected network bridging. | |

# 3 Developing a Security Program

## Forming a Security Team

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.

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 (for example, individuals responsible for running and maintaining Honeywell Windows Mobile 6.5 (WM6.5) devices and infrastructure).
  - Business applications (for example, individuals responsible for applications interfaced to the Honeywell WM6.5 system such as Human Resources, Physical Security, etc.).
  - IT systems administration.
  - IT network administration.
  - IT security.

## 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 such as routers, switches, firewalls, and ancillary items used to build the system).
  - Computer equipment, such as servers, cameras and streamers.
- Network configuration information, such as routing tables and access control lists.
- Information stored on computing equipment, such as databases and other intellectual property.
- Intangible assets, such as 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 (including malicious users inside or outside the company, and uninformed employees).
- Inanimate threats
  - natural disasters, such as fire or flood
  - malicious code, such as 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 local area network (LAN) and WM6.5 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 WM6.5 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

The original asset evaluation and associated risk assessment and mitigation plans should specify the security requirements for all networked components. To ensure that all modifications to networking capabilities continue to meet those security requirements, a formal change management procedure is vital.

A risk assessment should be performed on any change made to the WM6.5 software 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.
- ongoing risk assessments as new devices are placed on the network.
- the creation of an Incident Response Team.

## Additional Security Resources

| Type | URL |
|---|---|
| Microsoft | http://www.microsoft.com/technet/security |
| National Cyber Security Partnership | http://www.cyberpartnership.org |
| Cisco | http://www.cisco.com |
| The National Institute of Standards and Technology document *System Protection Profile - Industrial Control Systems Version 1.0* | http://www.nist.gov/manuscript-publication-search.cfm?pub_id=822602 |
| SANS Internet Storm Centre | https://isc.sans.edu |
| Cyber Emergency Response Team (CERT) | http://www.cert.org |
| AusCERT | http://www.auscert.org.au |
| Computer Security Institute | http://www.gocsi.com |

| 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 |

# 4 Disaster Recovery Planning

Disaster recovery refers to the process and measures performed when restoring standard operations on the Windows Mobile 6.5 device. Recovery is required in the case of data loss or deletion, or application corruption or inaccessibility.

Honeywell recommends two methods for disaster recovery:

- Device backup to external storage
- Remote device management solution

## Device Backup to External Storage

You should periodically create a backup of the WM6.5 device and data on external storage media, such as a Secure Digital (SD) card. This backup can be restored later if the WM6.5 device is compromised. For greater safety, SD cards should be copied to other storage such as a server. Note that if the SD card is encrypted, secondary backup is not possible.

## Remote Device Management Solution

You can create a backup of the WM6.5 device and upload the backup to a remote device management server. Configuration information, current and previous version of software, and supporting data files should be routinely backed up. For greatest safety, copies should be maintained in off-site storage.

# 5 Security Updates and Service Packs

## Windows Mobile 6.5 (WM6.5) Support and Updates

Microsoft will continue to support Windows Mobile 6.5 (WM6.5) until 2020. Honeywell will update the platform software as necessary to support changes in WM6.5, Honeywell software, or third-party software included with the WM6.5 device. These updates will be made available after Honeywell has verified that the software operates properly in the WM6.5 device. Use only these updates.

If other third-party software is installed on the WM6.5 device, Honeywell recommends testing the platform software update on a non-production system before making changes to production systems.

**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.**

Customers can obtain security updates and service packs through the Honeywell product website or by request from Honeywell product support.

# 6 Network Planning and Security

## Connecting to the Business Network

The Windows Mobile 6.5 (WM6.5) network and other networks (such as the Internet or business network) should be separated by a firewall. See System Architecture on page 1-2.

The nature of network traffic on a WM6.5 device 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 WM6.5 network and vice versa.

Ideally, there should be no direct communication between the WM6.5 network and the business network. However, practical considerations often mean a connection is required between these networks. The WM6.5 network may require data from the servers in the business network or business applications may need access to data from the WM6.5 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 (for example, 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 the WM6.5 customer. When a third-party application must be added to the device, 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 WM6.5 system are provided.

In addition, evaluate additional risks to the WM6.5 system with regard to the following:

- The service level agreement (SLA) 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.

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

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

# 7 Securing Wireless Devices

## Wireless Local Area Network (WLAN) and Access Point (AP) Security

Windows Mobile 6.5 (WM6.5) devices 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 WM6.5 device connects through a wireless access point (WAP) to an organization's server on a wired network, specific security precautions are required to mitigate the significant security risk the WLAN wireless access point (WAP) connection represents for the servers and devices on the wired network.

Non-WM6.5 wireless devices (such as laptops and printers) should either be on a separate WLAN with different security profiles, or the WAP 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 WM6.5 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. Honeywell supports and approves these security methods:
  - Wi-Fi Protected Access II  Extensible Authentication Protocol - Tunneled Transport Layer Security (WPA2 EAP-TTLS)
  - WPA2 EAP-Transport Layer Security (TLS)
  - WPA2 Protected Extensible Authentication Protocol - Microsoft Challenge-Handshake Authentication Protocol (PEAP-MSCHAP)
  - WPA2 PEAP-Generic Token Card (GTC)
  - WPA2 EAP-Flexible Authentication via Secure Tunneling (FAST)
  - WPA2 Pre-shared Key (PSK)
- Configure the Remote Authentication Dial-In User Service (RADIUS) server address.
- Configure for WPA2 Enterprise.Change the WAP RADIUS password. Do not use the default password.
- Configure 802.1x authentication.
- Enable media access control (MAC) filtering and enter the MAC addresses for all the wireless devices. This helps prevent unauthorized devices from connecting to the wireless network.

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

### Secure WM6.5 WLAN Configuration

Honeywell recommends the following when configuring WM6.5 devices for WLANs:

- Honeywell supports and approves these security methods:
  - WPA2 EAP-TTLS
  - WPA2 EAP-TLS
  - WPA2 PEAP-MSCHAP
  - WPA2 PEAP-GTC
  - WPA2 EAP-FAST
  - WPA2 PSK.
- Configure the proper SSID.
- Configure 802.1x authentication.
- Configure PEAP authentication.
- Configure the 802.1x supplicant (client) to prompt for the password needed by PEAP-MSCHAP.
- If EAP-TLS or EAP-PEAP-TLS are in use, a client certificate must be available on the WM6.5 device.
- Configure encryption to AES-CCMP.
- Honeywell recommends that you perform certificate validation. For more information, see the *Honeywell WLAN Secure Wireless Client User Guide*.

## *Bluetooth™ Wireless Technology Security*

All WM6.5 devices are equipped for short-range wireless communication using Bluetooth wireless technology. For secure Bluetooth communications, follow these security recommendations and precautions:

- Set the Bluetooth stack to “non-discoverable” on the WM6.5 device.
- Set the Bluetooth stack to “non-connectable” to stop arbitrary pairings on the WM6.5 device.
- Enable OBEX authentication on the device (disabled by default). To enable authentication, set HKLM\Software\Microsoft\Obex\Services{00000000-0000-0000-0000-000000000000}”TransportAuthenticate”=DWORD:0001.
- If possible, pair devices ONLY when in a physically secure area.

## *Wireless Wide Area Network (WWAN) Security*

Many devices provide WWAN capabilities. For secure WWAN communications, follow these security recommendations and precautions:

- Use Secure Hypertext Transfer Protocol (HTTPS, with TLS 1.0 or greater) with Web applications with a locked down browser that allows access to only specified uniform resource locators (URLs). Make sure that the client is configured to validate the server certificate and uses sufficiently secure cipher suites.

# 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 Windows Mobile 6.5 (WM6.5) device. 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 log should be available for retrieval via the package and a related console application on a server, or via a remote device management system. Periodic collection of additional logs (for example, virtual private network (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 (for example, 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 Windows Mobile 6.5 Operating System

Any security strategy for computers in the Windows Mobile 6.5 (WM6.5)device network should include securing access to the operating system, ensuring that:

- only authorized users have access to the system.
- user access to files, systems, and services is limited to that necessary for the performance of job duties.

The following links will provide information about the security features of the WM6.5 operating environment:

- http://technet.microsoft.com/en-us/library/cc182298.aspx
- http://go.microsoft.com/fwlink/?LinkId=118667

This section defines settings related to security policies on WM6.5.

## Registry Entry for Security Policies

The policies in the next table can be set by remote device management systems (or by Microsoft Exchange Server if used).

**Registry Key:** HKEY_LOCAL_MACHINE\Security\Policies\Policies\Policy ID

| Policy ID | Policy Setting | Recommended | Description |
|---|---|---|---|
| 2 | Auto Run Policy<br>SECPOLICY_CFAUTORUN | 1 (Not Allowed) | Indicates whether applications stored on a multimedia card (MMC) are allowed to auto-run when the card is inserted into the device. |
| 4097 | RAPI | 0 or 2 | Indicates whether desktop applications are allowed to perform actions on a remote device:<br>• 0 - RAPI communication with the desktop application is disabled.<br>• 2 - Communication with the desktop application is limited. Files, DLLs, and registry keys have reduced access. |
| 4101 | Unsigned CABS<br>SECPOLICY_UNSIGNEDCABS | 0 (Signed Only) | Indicates whether unsigned .cab files can be installed on the device. If a signed .cab file does not have a matching root certificate in the Software Publisher Certificate (SPC) store, the file is unsigned.<br>You should always use SECPOLICY_UNSIGNEDCABS together with SECPOLICY_UNSIGNEDAPPS. |
| 4102 | Unsigned Applications Policy<br>SECPOLICY_UNSIGNEDAPPS | 0 (Signed Only) | Indicates whether unsigned applications are allowed to run on Windows Mobile devices. If a signed application does not have a matching root certificate in the Privileged Execution Trust Authorities or the Unprivileged Execution Trust Authorities certificate store, the application is unsigned.<br>You should always use SECPOLICY_UNSIGNEDCABS together with SECPOLICY_UNSIGNEDAPPS. |
| 4122 | Unsigned Prompt Policy<br>SECPOLICY_UNSIGNEDPROMPT | 1 (No Prompt) | Indicates whether a user is prompted to accept or reject unsigned .cab, .dll and .exe files. |

| Policy ID | Policy Setting | Recommended | Description |
|---|---|---|---|
| 4127 | Software Certificates Policy<br>SECPOLICY_SOFTCERTS | 1 (Allowed) | Determines whether an outbound message that is sent over Secure/Multipurpose Internet Mail Extensions (SMIME) can be signed with a software certificate. |
| 4131 | Password Required Policy<br>SECPOLICY_LASS_PWD_REQUIRED | 0 (Require) | Indicates whether a password must be configured on the device. See HKEY_LOCAL_MACHINE\Comm\Security\LASSD\LAP\lap_pw. |
| 4134 | Encrypt Removable Storage Policy<br>SECPOLICY_MENCRYPT_REMOVABLE | 0 (Not Allowed) | Specifies if the user is allowed to change mobile encryption settings for removable storage media. |
| 4135 | Bluetooth Policy<br>SECPOLICY_BLUETOOTH | 0 (Blocked) | Specifies if a Bluetooth enabled device allows other devices to perform a search on the device. |
| 4146 | Desktop Quick Connect Authentication Policy<br>SECPOLICY_LASS_DESKTOP_QUICK_CONNECT | 0 (User must authenticate) | Specifies how device authentication is handled when connecting to the desktop. |

## *Recommended Registry Entries to Support Security Policies*

### *Enable Stronger Password*

**Registry Key:** HKEY_LOCAL_MACHINE\Comm\Security\LASSD\LAP\lap_pw\AllowSimplePIN

**Recommended Value:** 0

### *Length and Type of Password*

Enforces the length and type of password.

**Registry Key:** HKEY_LOCAL_MACHINE\Comm\Security\LASSD\LAP\lap_pw

**Recommended Values:** Set these values with the sub-keys described in the next table. These settings are enforced only if PasswordNotRequired is set to zero (0).

| Sub-Key Name | Recommended | Description |
|---|---|---|
| MinimumPasswordLength | 12 | Sets the minimum device password length the user can enter. The length is measured in characters and can be set to any number less than or equal to the maximum number of characters allowed. Entering zero (0) for MinimumPasswordLength results in the default setting of 1.<br>This value works in conjunction with security policy 4131, which when set to zero (0) indicates that password enforcement is required on the device. If password enforcement is not required, the value of MinimumPasswordLength is ignored. |
| PasswordComplexity | 0 | Sets the complexity of the Device Password:<br>• Zero (0): A strong password is required<br>• 1: A numeric personal identification number (PIN) is required<br>• Any other value: A numeric or alphanumeric password can be used.<br><br>Setting this parameter with the Exchange Security Manager results in a setting of zero (0) or 2. It is not possible to set this parameter to 1 using the Exchange Security Manager. |

### *Unique Password*

Prohibits the same password from being used for the previous *N* password changes.

**Registry Key:** HKEY_LOCAL_MACHINE\Comm\Security\LASSD\LAP\lap_pw\NumberOfPasswords

**Recommended Value:** 8

### *Password Expiration*

Specifies the time period (in seconds) for password expiration.

**Registry Key:** HKEY_LOCAL_MACHINE\Comm\Security\LASSD\LAP\lap_pw\ExpirationPeriod

**Recommended Values:** Listed in the next table. Select a value depending on the level of security required:

| Value | Days | Recommended Use |
|---|---|---|
| 2592000 | 30 | Critical use cases, or when WM6.5 device users might change frequently |
| 5184000 | 60 (Default) | Typical use cases |
| 7776000 | 90 | Less critical use cases |
| 10368000 | 120 | Very low security requirements |

### *Exponential Back Off*

Enable the exponential back off mechanism.

**Registry Key:** HKEY_LOCAL_MACHINE\Comm\Security\LASSD

**Recommended Value:** Listed in the next table. The time delay or lockout time is calculated by using this expression:

(InitialPenalty + (2^(Number of failures above Threshold)) * IncrementalPenalty)

| Sub-Key | Recommended | Description |
|---|---|---|
| InitialPenalty | 5 | Time, in seconds, for the initial penalty. Default is 0. |
| Threshold | 2 | Number of failures before the exponential back off mechanism is activated. Default value is 0 (exponential back off is disabled). |
| IncrementalPenalty | 3 | Time (in seconds) of the multiplier for the exponent. Default value is 0 (no delay beyond the value set for InitialPenalty). |

## *Securing Access for Interface Acquisition*

Honeywell recommends that applications that open handles (to ports, etc.) should open in “exclusive use” mode.

## *Miscellaneous Security Considerations for WM6.5 Devices*

This list includes WM6.5 security items to be considered that defy easy categorization.

- Use the SecureZeroMemory function to clear out memory when erasing or changing passwords.
- Honeywell recommends that only carefully vetted devices be allowed to connect to the computer, particularly USB devices connected directly or through docks.
- Honeywell recommends that users follow the proper procedures for replacing batteries in WM6.5 devices to prevent data corruption. To prepare for data corruption, see Disaster Recovery Planning on page 4-1.
- Load and execute only white-listed applications.

# 10 Network Ports Summary

## Network Port Table

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

A list of common network port numbers can be found at https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

# 11 Customer Support

## Where to Get Technical Support

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

For our latest contact information, see www.honeywellaidc.com/locations.

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

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

www.honeywellaidc.com

ALLSKU-M65-ENUS-ZY Rev A
9/15