Honeywell

Windows Embedded 8 Handheld

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.

This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of HII.

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 1 - Introduction

Chapter 2 - Security Checklist

Chapter 3 - Developing a Security Program

Chapter 4 - Disaster Recovery Planning

Chapter 5 - Security Updates and Service Packs

Chapter 6 - Network Planning and Security

Chapter 7 - Securing Wireless Devices

Chapter 8 - System Monitoring

Chapter 9 - Securing Access to the Windows Embedded 8 Handheld 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 all mobile computers running Windows Embedded 8.1 Handheld (WE8H) Operating Systems.

Intended Audience

The target audience for this guide is the Windows Embedded Handheld 8.1 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 Embedded 8.1 Handheld OS and the organization responsible for managing information technology risks.

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

- Windows Embedded 8.1 Handheld.
- 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)

How to Use this Guide

Note: WE8H references in this guide refer to Windows Embedded 8.1 Handheld OS 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.

Developing a Security Program, page 3-1

Disaster Recovery Planning, page 4-1

Security Updates and Service Packs, page 5-1

Network Planning and Security, page 6-1

Securing Wireless Devices, page 7-1

System Monitoring, page 8-1

Securing Access to the Windows Embedded 8 Handheld Operating System, page 9-1

Network Ports Summary, page 10-1

Product Detail

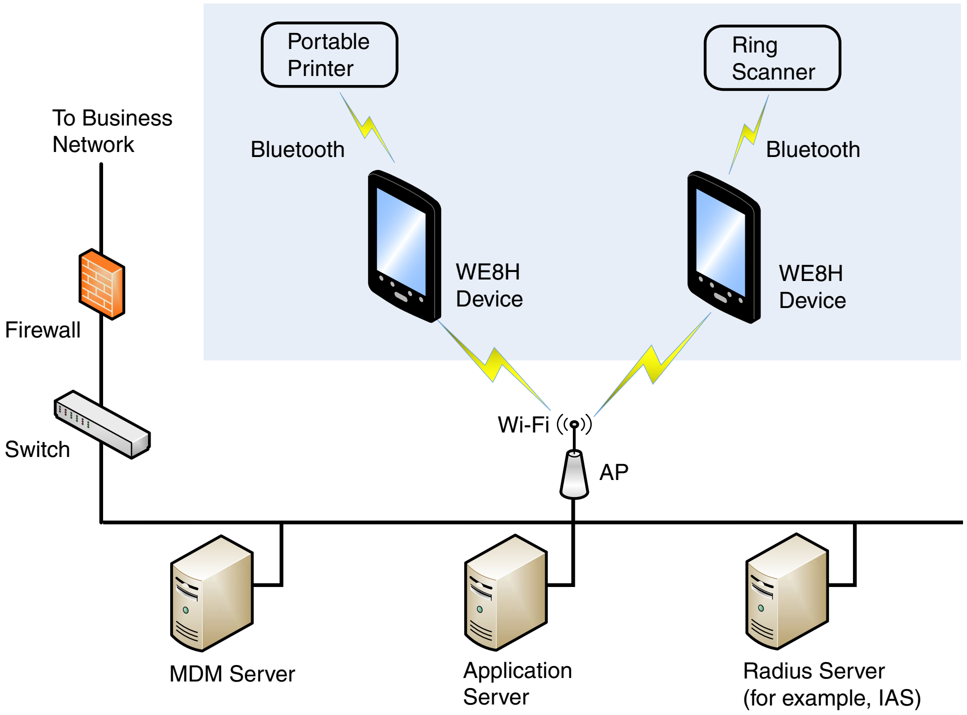
Honeywell mobile devices are intended for use in in-premise Automatic Data Collection (ADC) systems and for field ADC applications. In-premise systems typically exist in establishments such as distribution warehouses or retail stores. This type of system often uses terminal emulation servers or web servers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

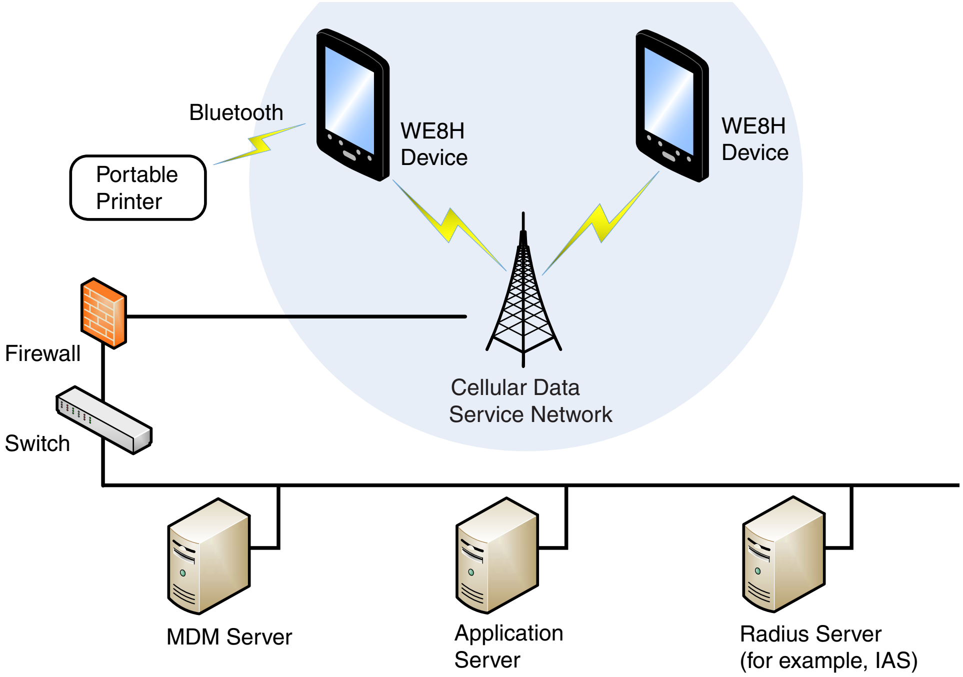
Architecture of an In-Premise System

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, WE8H mobile devices, and an application support server (e.g., web server or a terminal emulation server).



Architecture of a Field Service System

The diagram below provides an example of field application system architecture that includes cellular-based mobile 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 Embedded 8 Handheld (WE8H) 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	
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 WE8H devices.	

Unauthorized External Access

This threat includes intrusion into the Honeywell WE8H 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.	For information, see PolicyManager Configuration Service Provider on page 9-3.
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 other networks and mobile devices.	
Secure wireless devices.	

Mitigation Steps	
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
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 Embedded 8 Handheld Operating System on page 9-1. 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 a VPN when the system requires data to traverse an untrusted network.	Mobile Device Management (MDM) software
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 WE8H 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 (such as microSD™ or microSDHC™ cards) on WE8H devices.	http://msdn.microsoft.com/en-us/magazine/cc982153.aspx
Implement password protection on WE8H devices.	Mobile Device Management (MDM) software
Monitor system access.	
Add other mitigations for disabling radios, (such as 802.11, near field communication (NFC), location services, camera).	Mobile Device Management (MDM) software

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 Embedded 8 Handheld WE8H) devices and infrastructure).
  - Business applications (for example, individuals responsible for applications interfaced to the Honeywell WE8H 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 WE8H 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 WE8H 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 WE8H 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
Windows Phone Security	http://technet.microsoft.com/en-us/library/dn756284.aspx
Platform Security	http://technet.microsoft.com/en-us/library/dn756283.aspx
Access Control and Device Management	http://technet.microsoft.com/en-us/library/dn756285.aspx
Developing Secure Applications	http://msdn.microsoft.com/en-us/library/windows/apps/xaml/hh849625.aspx
Security for devices running Windows Embedded 8.1 Handheld	http://msdn.microsoft.com/en-us/library/dn499742.aspx
Administrator Guide for Windows Embedded 8.1 Handheld	http://msdn.microsoft.com/en-us/library/dn499757.aspx
Configuring Devices	http://msdn.microsoft.com/en-us/library/dn499730.aspx
Best Practices for configuring Devices	http://msdn.microsoft.com/en-us/library/dn499744.aspx
Provisioning the Device on Startup	http://msdn.microsoft.com/en-us/library/dn499751.aspx
Locking Down a Device	http://msdn.microsoft.com/en-us/library/dn798313.aspx
Prepare devices for application Deployment	http://msdn.microsoft.com/en-us/library/dn798310.aspx
Features in Windows Embedded 8.1 Handheld	http://msdn.microsoft.com/en-us/library/dn499748.aspx
Manage Devices	http://msdn.microsoft.com/en-us/library/dn499752.aspx

Type	URL
Windows Phone 8.1 mobile device management (MDM) protocol documentation	http://msdn.microsoft.com/en-us/library/dn499787.aspx
WE8H Develop Applications	http://msdn.microsoft.com/en-us/library/dn715923%28v=winembedded.81%29.aspx
WE8H application programming interface (API) Reference	http://msdn.microsoft.com/en-us/library/dn715928%28v=winembedded.81%29.aspx
Windows Phone API Reference	http://msdn.microsoft.com/en-us/library/windows/apps/ff626516%28v=vs.105%29.aspx
Security Development Lifecycle	http://www.microsoft.com/security/sdl/default.aspx
Wireless local area network (WLAN) profile Schema	http://msdn.microsoft.com/en-us/library/windows/desktop/ms707341%28v=vs.85%29.aspx

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) *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 Windows Embedded 8 Handheld (WE8H) devices to standard operation if disaster recovery is required due to data loss (such as 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 WE8H mobile devices and any data located on external storage (such as a micro Secure Digital (SD) card installed in the terminal).
- Save the backup files to a secondary location (e.g., off-site server) not on the WE8H mobile device or the microSD card installed in the device.

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

Note: Perform routine disaster recovery testing.*For backup and restore procedures for WE8H devices, see http://www.windowsphone.com/en-IE/how-to/wp8/settings-and-personalization/back-up-my-stuff.*

Disaster Recovery 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

It is critical to keep the latest patches and software versions on your Windows Embedded 8 Handheld (WE8H) devices. 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.

Microsoft 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 WE8H 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.

Additional Resources

Security Resources	
The MITRE Corporation	http://www.mitre.org, 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

Software updates and service packs tested and approved by Honeywell may be found at honeywellaidc.com.

Honeywell DiagnosticInfo Power Tool

The **DiagnosticInfo** Power Tool provides important system information including firmware versions, application versions, system parameters, and service pack versions, as well as network and radio information for your WE8H device.

To View System Information

From the Home screen, swipe left and touch **DiagnosticInfo**. You may need to scroll up or down to see the icon.

You cannot edit information in DiagnosticInfo. This information is gathered from the mobile device and changes only when the device configuration has changed.

See the device user manual for more information on viewing system information. See Related Documents on page 1-3.

6

Network Planning and Security

Connecting to the Business Network

The Windows Embedded 8 Handheld (WE8H) device 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 WE8H 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 WE8H device network and vice versa.

Ideally, there should be no direct communication between the WE8H device network and the business network. However, practical considerations often mean a connection is required between these networks. The WE8H device network may require data from the servers in the business network or business applications may need access to data from the WE8H device 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

The WE8H Ecosystem provides many applications. All Ecosystem applications for WE8H are required to be signed by the Microsoft Store and pass certification testing requirements. Unsigned applications are not allowed to be installed and executed on WE8H devices. 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 WE8H system are provided.

In addition, evaluate additional risks to the WE8H 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

All Windows Embedded 8 Handheld (WE8H) mobile 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 WE8H 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-WE8H 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 WE8H 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 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.

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

Secure WE8H WLAN Configuration

Microsoft provides a WiFi configuration service provider for initial 802.11 network provisioning. This configuration service provider uses the WLAN_profile Schema for configuration: http://msdn.microsoft.com/en-us/library/windows/desktop/ms707341%28v=vs.85%29.aspx

Honeywell recommends the following when configuring WE8H mobile devices for WLANs:

- Honeywell supports and approves these security methods:
  - WPA2 EAP-TTLS
  - WPA2 EAP-TLS
  - WPA2 PEAP-MSCHAP
  - 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 EAP-PEAP/MSCHAP, EAP-TTLS/MSCHAP.
- If EAP-TLS or EAP-PEAP-TLS are in use, a client certificate must be available on the WE8H device.

Bluetooth™ Wireless Technology Security

All WE8H mobile devices are equipped for short-range wireless communication using Bluetooth wireless technology. For secure Bluetooth communications, follow these security recommendations and precautions:

- When available, use Bluetooth 2.1 Secure Simple Pairing. Honeywell recommends that you do **not** use the “just works” mode.
- Use Device Management to disable Bluetooth if not required by application solutions.
- Use Device Managment to remove Bluetooth settings from the user roles.
- Use a strong personal identification number (PIN) or Password.
- 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.
- 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 WE8H devices and an NFC tags or other NFC enabled devices.

NFC security is based on the short range characteristic of the RF solution. Honeywell recommends the following security recommendations and precautions listed below:

- Using Device Management, disable NFC on the WE8H 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 WE8H devices using NFC, then the application should enable encryption of the data.
- Disallow the Wallet application using Device Management.

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 Embedded 8 Handheld (WE8H) mobile 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. The most relevant tool for this purpose at this time is the Field Medic Application at http://www.windowsphone.com/en-us/store/app/field-medic/73c58570-d5a7-46f8-b1b2-2a90024fc29c.

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 Embedded 8 Handheld Operating System

WE8H provides the following platform security features. The list is not exhaustive but meant to provide a high level overview of the system capabilities.

- UEFI enforcement of Secure Boot and Trustworthy Hardware
  - Secure Boot prevents root-kits and only signed code execution
  - Trusted Platform Module (TPM) standards based crypto-processor
- Data Execution Prevention (DEP) Standards
- Address Space Layout Randomization (ASLR)
- Device Encryption based on BitLocker Drive Encryption
- AppContainter Sandboxing blocks unauthorized access to system, apps and data
- Smart Screen Filter provides anti-phishing protection
- Remote Data Removal for Enterprise data
- Virtual Smart Cards for Two Factor Authorization (2FA)
- Information Rights Management protected email and documents based on Windows Rights Management Services (RMS) standards.
- Secure MDM Enrollment
- Security Policy management
- Removable Storage (SD Card) encryption
- Assigned Access to applications and system function based on user roles
- S/MIME support
- TLS 1.0 (or greater) support
- Wi-Fi support for EAP/TLS and EAP/TTLS certificate based authentication
- Integrated VPN support for IKEv2 and IPsec connections
- Vendor downloadable support for SSL VPN connections
- Auto-triggered VPN Connections
- Remote Lock
- Remote Wipe
- Remote PIN (user password) Reset
- Trusted System and Application Software – unsigned software is not allowed to execute.
- Application Allow Listing
- Application Deny listing
- Access Control Lists prevent unauthorized access to secured objects
- Feature enablement and disablement for Bluetooth, NFC, Wi-Fi, Camera, Location Based Services, Storage Card, voice recording, updates
- User Passwords

For more detailed information on each of these items, see:

- Microsoft WE8H OS specific information: http://msdn.microsoft.com/en-us/library/dn499742.aspx.
- Windows Phone 8.1 Security information: http://technet.microsoft.com/en-us/library/dn643717.aspx.

Many of the above features are capable of being managed by Mobile Device Management Software . System provisioning is used to enable and provide the level of enterprise security needed by your WE8H users.

The most complete documentation for the “Windows Phone 8.1 MDM Protocol” for the WE8H platform is at http://msdn.microsoft.com/en-us/library/dn499787.aspx. Enterprise customers are encouraged to review and understand all this documentation for proper implementation of security features.

Internal Firewall

By default the internal firewall of WE8H does not allow incoming network connections, including incoming connections that originate from code on the device used for loopback. Honeywell does not recommend the use of incoming connections for applications the enterprise does not control. For applications that desire to enable incoming connections, see: http://msdn.microsoft.com/en-us/library/windows/apps/xaml/dn640582.aspx#configuring_the_firewall.

Secure By Default Policy

Honeywell provides the following recommendations on security settings for a "secure by default" system in the following sections. Honeywell provides a provisioning XML to enable this scenario for our customers. Customers can then migrate from the Honeywell defined security settings to their enterprise needs through their own MDM policy choices and customization of the provisioning XML file.

Configuration Service Providers

Configuration Service Providers allow device settings to be established by the enterprise based upon their policies. Configuration Service Providers allow both enterprise and cellular carriers (for Cellular enabled devices) to manage settings on the WE8H device. Honeywell has no recommendations for changes to Carrier based Configuration Service Providers which are primarily used by carriers to configure cellular services. Enterprise Mobile Device management is not allowed access to these CSPs. Honeywell urges Enterprise to review these CSP settings with their carrier for the best security policy.

- Bootstrap Configuration Service Provider
- CellularSettings Configuration Service Provider
- BrowserFavorite Configuration Service Provider
- Application Configuration Service Provider
- W4 Application Configuration Service Provider
- W7 Application Configuration Service Provider
- CM_CellularEntries Configuration Service Provider
- CM_ProxyEntries Configuration Service Provider
- PXLogical Configuration Service Provider
- NAPDEF Configuration Service Provider
- DMAcc Configuration Service Provider
- DMS Configuration Service Provider
- NAP Configuration Service Provider
- Proxy Configuration Service Provider
- CMPolicy Configuration Service Provider
- SecurityPolicy configuration service provider
- User Plane Configuration Service Provider

DMClient Configuration Service Provider

This configuration service provider specifies Enterprise Specific mobile device management settings that identifies the device in the enterprise domain, allows for security migration for certificate renewal and server triggered un-enrollment. Honeywell provides no default configuration for this CSP.

HotSpot Configuration Service Provider

This configuration service provider configures and enables internet sharing on the device. Honeywell does not recommend Enterprise to enable internet sharing where security is a concern.   By default Internet Connection Sharing is disabled and there is no settings screen to allow configuration. If enabled a setting screen will be available but sharing will be turned off until the user enables it.

FileSystem Configuration Service Provider

This configuration service provider queries, adds, modifies and deletes files and directories. It also allows file attributes on the phone to be modified. Honeywell provides no default configuration for this CSP. Honeywell recommends Enterprise Customers use the EnterpriseEXTFileSystem instead of this provider.

EMAIL2 Configuration Service Provider

This CSP is used to configure SMTP email accounts. Honeywell does not provide a default recommendation for this service provider.   Enterprise customers use this CSP to configure any SMTP email accounts.

CertificateStore Configuration Service Provider

This configuration service provider is used to add certificates to the device. Honeywell does not provide a default recommendation for this service provider.   Enterprise customers use this CSP to add certificates to the system.

ActiveSync Configuration Service Provider

Honeywell does not provide a default recommendation for this service provider. Enterprise customers should use this CSP to establish and secure their Exchange ActiveSync connections.

DeviceLock Configuration Service Provider

This configuration service provider is used to configure device lock related policies. Honeywell provides the recommendation to set these values using the PolicyManager Configuration Service Provider.

EnterpriseAppManagment Configuration Service Provider

This configuration service provider is used to install, update and manage Enterprise Applications and Tokens. Honeywell does not provide a default recommendation for this service provider.

NodeCache Configuration Service Provider

This configuration service provider manages the cache for the system configuration nodes used by enterprise device management servers. Honeywell does not provide a default recommendation for this service provider.

Storage Configuration Service Provider

Honeywell recommends that storage cards are disabled for system solutions that do not require them.

PolicyManager Configuration Service Provider

Honeywell has the following recommendations for the Policy Manager CSP. The PolicyManager configuration service provider listed below are suggested in order to provide the highest level of security for the system. Unless otherwise noted each of these policies can be changed via MDM at any time based on enterprise needs.

PolicyManager CSP Recommendations

Node	System Default	Recommended Secure Setting
DeviceLock/AllowIdleReturnWithoutPassword	1 - Allow	0 - Prevent
DeviceLock/DevicePasswordEnabled	1 – not required	0 - Required
DeviceLock/AllowSimpleDevicePassword	1 – Allow	0 - Prevent
DeviceLock/MinDevicePasswordLength	4	8
DeviceLock/AlphanumericDevicePasswordRequired	2 – User Choice	0 - Required
DeviceLock/DevicePasswordExpiration	0 (days) – non expiring	90 (days)
DeviceLock/DevicePasswordHistory	0 – no history	10
DeviceLock/MaxDevicePasswordFailedAttempts	0 – never wipe	6
DeviceLock/MaxInactivityTimeDeviceLock	0 (minutes) – no timeout	3 minutes
DeviceLock/MinDevicePasswordComplexCharacters	1	2
WiFi/AllowWifi	1 - allow	1 – WLAN only Devices 0 – WWAN + WLAN devices (Disable)
WiFi/AllowInternetSharing	1 – allow	0 - prevent
WiFi/AllowAutoConnecttoWifiSenseHotspots	1 – allow	0 - prevent
WiFi/AllowWifiOfffLoading	1 – allow	0 - prevent
WiFi/AllowWifiHotSpotReporting	1 – allow	0 - prevent
WiFi/AllowManualWifiConfiguration	1 – allow	0 - prevent

PolicyManager CSP Recommendations (Continued)

Node	System Default	Recommended Secure Setting
Connectivity/AllowNFC	1 – allow	0 - prevent
Connectivity/AllowBluetooth	1 – allow	0 - prevent
Connectivity/AllowVPNRoamingOverCellular	1 – allow	1 - allow
Connectivity/AllowVPNOverCellular	1 – allow	1 – allow
Connectivity/AllowUSBConnection	1 – allow active sync	0 - prevent
Connectivity/AllowCellularDataRoaming	1 – allow	1 - allow
System/AllowStorageCard	1 – allow	0 - prevent
System/AllowTelemetry	2 – allow	0 - prevent
System/AllowLocation	1 – allow	0 - prevent
Accounts/AllowMicrosoftAccountConnection	1 – allow	0 – prevent *
Accounts/AllowAddingNonMicrosoftAccountsManually	1 – allow	0 - prevent
Security/AllowManualRootCertificateInstallation	1 – allow	0 - prevent
Security/RequireDeviceEncryption	1 – allow	1 – allow **
ApplicationManagement/AllowStore	1 – allow	0 – prevent*
ApplicationManagment/ApplicationRestrictions = VariableData depending on customer app needs	***	***
ApplicationManagement/AllowDeveloperUnlock	1 – allow	0 - prevent
Browser/AllowBrowser	1 – allow	0 – prevent*
Camera/AllowCamera	1 – allow	0 - prevent
Update/DeviceUpdateMode	4 - allow	0 - prevent
Search/AllowSearchToUseLocation	1 – allow	0 - prevent
Search/SafeSearchPermissions	1 – allow	0 - prevent
Search/AllowStoringImagesFromVisionSearch	1 – allow	0 - prevent
AboveLock/AllowActionCenterNotifications	1 – allow	0 - prevent
Experience/AllowCopyPaste	1 – allow	0 - prevent
Experience/AllowScreenCapture	1 – allow	0 - prevent
Experience/AllowManualMDMUnenrollment	undefined	0 - prevent
Experience/AllowVoiceRecording	1 – allow	0 - prevent
Experience/AllowSaveAsOfficeFiles	1 – allow	1 – allow
Experience/AllowCortana	1 – allow	1 – allow
Experience/AllowSyncMySettings – see warnings	*	*
System/AllowUserToResetPhone	1 – allow	1 – allow*

* EnterpriseAssignedAccess concerns with service or deep links

** Cannot be undone. Setting this bit is left to the customer. The default XML for secure lockdown does not set this bit.

*** List each application separately. This setting blocks the application from running if the user attempts to launch the application. The Enterprise could use this in conjunction with WEHLockdown Allow List to fully lock down the device. For instance, if you do not want users to browse the internet at all, you would not include IE in the WEHLockdown allow list. However, if users receive a URL, they are able to click on that URL to launch IE since we do not prevent that through WEHLockdown. This setting allows you to block the launching of IE in this case.

RemoteRing Configuration Service Provider

Honeywell provides no default configuration for this CSP. This configuration provider can be used to trigger an audible ring from a device to aid in finding a misplaced device.

VPN Configuration Service Provider

Honeywell provides no default configuration for this CSP but recommends customers use this CSP to establish VPN connections for devices connected to public networks.

WiFi Configuration Service Provider

This configuration service provider adds or deletes Wi-Fi networks on the device. Honeywell provides no default configuration for this CSP, but recommends Enterprise establish allowed WiFi connections using this CSP.

RemoteLock Configuration Service Provider

Use the RemoteLock CSP to lock a device that has a PIN or use it to reset a PIN on a device that does or does not have a PIN.   Honeywell does not provide a default configuration and Enterprise customers are urged to provide this capability.

RemoteWipe configuration Service Provider

Honeywell does not provide a default configuration for this CSP. Enterprise customers use the RemoteWipe CSP to remove enterprise data from a device that has been lost or stolen. Remote wipe may or may not remove enterprise provisioning data which depends on provisioning data in the value of the PersistData/PersistProvisionedData Policy in the EnterpriseAssignedAccess Configuration Service Provider.

EnterpriseAssignedAccess Configuration Service Provider

The EnterpriseAssignedAccess configuration service provider allows IT administrators to provision a WE8H device with a single locked down user experience (Kiosk behavior) or provide a user-role based lock down approach for device usage. Administrators can configure the system in the following ways on a per user account basis.

- Action Center Enable/Disable (Disable as Enable notifications can allow deep links into OS.)
- Allowed installed applications through allow listing
- Applications icon size pinned to the start menu and icon location in menu
- System Button Disablement
- Button Mapping for application launch
- Enable/Disable Application Menus on Tap and hold
- CSP Runner Enable/Disable (enable allows CSPs to be executed on the device when there is no MDM provider)
- Enable/disable System and Application Settings
- Enable/disable of Tile manipulation
- Start Screen Size (only configurable for default Role)

Assign Roles

Honeywell recommends either a Kiosk mode lockdown or a lockdown based on Administrator and Associate roles.

Assign Application Lockdown

Honeywell recommends the following application access based on roles for various users.

Application Access Recommendations

Application	GUID	Default	Admin	Associate
Alarms	5B04B775-356B-4AA0-AAF8-6491FFEA560A	X	X	
Battery Saver	C551F76F-3368-42BB-92DF-7BFBB9265636	X	X	
Bing Finance	1E0440F1-7ABF-4B9A-863D-177970EEFB5E	X		
Bing Food	CC512389-0456-430F-876B-704B17317DE2	X		
Bing Health	CBB8C3BD-99E8-4176-AD8C-95EC6A3641C2	X		
Bing News	9C3E8CAD-6702-4842-8F61-B8B33CC9CAF1	X		

Application Access Recommendations (Continued)

Application	GUID	Default	Admin	Associate
Bing Sports	0F4C8C7E-7114-4E1E-A84C-50664DB13B17	X		
Bing Travel	19CD0687-980B-4838-8880-5F68ABA1671E	X		
Bing Weather	63C2A117-8604-44E7-8CEF-DF10BE3A57C8	X		
Calculator	5B04B775-356B-4AA0-AAF8-6491FFEA5603	X	X	X
Calendar	36F9FA1C-FDAD-4CF0-99EC-C03771ED741A	X	X	X
Camera	5B04B775-356B-4AA0-AAF8-6491FFEA5631	X	X	X
Cortana	5B04B775-356B-4AA0-AAF8-6491FFEA568C	X	X	X
Data Sense	5B04B775-356B-4AA0-AAF8-6491FFEA5646	X	X	
Email	5B04B775-356B-4AA0-AAF8-6491FFEA5614	X	X	X
Facebook	0C340A67-3288-4C76-9375-0F2FEFBA0412	X		
Games	50A6AEF0-4F35-434B-9308-CB3251303AE4	X		
Internet Explorer	5B04B775-356B-4AA0-AAF8-6491FFEA5660	X	X	X
Maps	5B04B775-356B-4AA0-AAF8-6491FFEA5686	X	X	X
Messaging	5B04B775-356B-4AA0-AAF8-6491FFEA5610	X	X	X
Music	D2B6A184-DA39-4C9A-9E0A-8B589B03DEC0	X		
Office Hub	5B04B775-356B-4AA0-AAF8-6491FFEA561E	X		
OneDrive	AD543082-80EC-45BB-AA02-FFE7F4182BA8	X		
One Note Mobile	5B04B775-356B-4AA0-AAF8-6491FFEA561B	X		
People	5B04B775-356B-4AA0-AAF8-6491FFEA5615	X		
Phone	5B04B775-356B-4AA0-AAF8-6491FFEA5611	X	X	X
Photos	5B04B775-356B-4AA0-AAF8-6491FFEA5632	X	X	X
Podcast	C3215724-B279-4206-8C3E-61D1A9D63ED3	X		
Settings	5B04B775-356B-4AA0-AAF8-6491FFEA5601	X	X	
Storage Sense	5B04B775-356B-4AA0-AAF8-6491FFEA564D	X	X	
Store	5B04B775-356B-4AA0-AAF8-6491FFEA5633	X	X	
Video	6AFFE59E-0467-4701-851F-7AC026E21665	X	X	X
Wallet	5B04B775-356B-4AA0-AAF8-6491FFEA5683	X		

Assign Settings Lockdown

Honeywell recommends the following settings application lock down based on user role.

Application Lockdown Recommendations

Settings Application	Default	Administrator	Associate
Microsoft.About	Allow	Allow	Allow
Microsoft.Accessories	Allow	Allow	Disallow
Microsoft.AdvertisingId	Allow	Allow	Disallow
Microsoft.AirplaneMode	Allow	Allow	Allow
Microsoft.AppCorner	Allow	Allow	Disallow
Microsoft.CloudStorageCPL	Allow	Allow	Disallow
Microsoft.BatterySaver	Allow	Allow	Disallow
Microsoft.Bluetooth	Allow	Allow	Disallow
Microsoft.Brightness	Allow	Allow	Disallow
Microsoft.CellularConn	Allow	Allow	Disallow
Microsoft.DataSmart	Allow	Allow	Disallow
Microsoft.DateTime	Allow	Allow	Allow WLAN Only devices Disallow otherwise
Microsoft.DrivingMode	Allow	Allow	Disallow
Microsoft.Accessibility	Allow	Allow	Disallow
Microsoft.Accounts	Allow	Allow	Disallow
Microsoft.Feedback	Allow	Allow	Disallow
Microsoft.FindMyPhone	Allow	Allow	Disallow
Microsoft.Games	Allow	Disallow	Disallow
Microsoft.RoamingCpl	Allow	Allow	Disallow
Microsoft.TouchKeyboard	Allow	Allow	Disallow
Microsoft.KidZone	Allow	Disallow	Disallow
Microsoft.Language	Allow	Allow	Disallow
Microsoft.Location	Allow	Allow	Disallow
Micorosoft.PhoneLock	Allow	Allow	Allow
Microsoft.FlashAppSetting	Allow	Allow	Disallow
Microsoft.MusicVideo	Allow	Disallow	Disallow
Microsoft.Proximity	Allow	Allow	Disallow
Microsoft.NOcenterSettings	Allow	Allow	Disallow
Microsoft.Updates	Allow	Allow	Disallow
Microsoft.MirrorUS	Allow	Allow	Disallow
Microsoft.DoNotDisturb	Allow	Allow	Disallow
Microsoft.Regional	Allow	Allow	Disallow
Microsoft.Sounds	Allow	Allow	Disallow
Microsoft.RotationLock	Allow	Allow	Disallow
Microsoft.Speech	Allow	Allow	Disallow
Microsoft.Themes	Allow	Allow	Disallow
Microsoft.StorageSettings	Allow	Allow	Disallow
Microsoft.ProfileUpdate	Allow	Allow	Disallow
Microsoft.USB	Allow	Allow	Disallow

Application Lockdown Recommendations (Continued)

Settings Application	Default	Administrator	Associate
Microsoft.VPN	Allow	Allow	Disallow
Microsoft.Wifi	Allow	Allow	Disallow
Microsoft.CompanyAccount	Allow	Allow	Disallow
Microsoft.AssistUX	Allow	Allow	Disallow
Microsoft.IE	Allow	Allow	Disallow
Microsoft.Maps	Allow	Allow	Disallow
Microsoft.Messaging	Allow	Allow	Disallow
Microsoft.OfficeMobile	Allow	Allow	Disallow
Microsoft.Contacts	Allow	Allow	Disallow
Microsoft.Phone	Allow	Allow	Disallow
Microsoft.Photos	Allow	Allow	Disallow
Microsoft.Search	Allow	Allow	Disallow
Microsoft.Marketplace	Allow	Disallow	Disallow
Microsoft.Wallet	Allow	Disallow	Disallow

Button Lockdown

Honeywell recommends the search button be disabled for the associate role. Honeywell recommends the camera button be disabled for application solutions that do no require camera functionality. Honeywell does not recommend disabling Home or Back buttons unless your enterprise applications provide all navigational needs.

Button Remapping

Honeywell recommends that no buttons be remapped unless the application solutions require separate buttons for application launch.

Disable Action Center

Honeywell recommends disabling Action Center for associate roles in order to prevent associate access to system internals.

Disable Menu Items

Honeywell recommends disabling Menu Items for associate roles in order to prevent associate access to system internals.

Disable Tile Manipulation

Honeywell recommends that tile manipulation be disabled for both administrator and associate roles.

Disable PersistData/PersistProvisioned Data

Honeywell recommends that data is not persisted on the WE8H device when the device is wiped for the most secure setting. However the Persist Data settings can be used to restore a device that has been wiped.

EnterpriseEXT Configuration Service Provider

This service provider allows IT administrators to use an MDM service to setup a device and enroll it automatically with the MDM server, restart devices and manage device updates or other management tasks. Honeywell provides no default configuration for this CSP. Honeywell recommends that the enterprise customer provide the settings for this CSP based upon their MDM and Update server requirements before the system is deployed to end users.

Honeywell does not recommend that the enterprise disable EnterpriseValidation settings.

EnterpriseEXTFileSystem Configuration Service Provider

This configuration service provider allows Enterprise customers to add, delete, get or change files in the file system. Honeywell provides no default configuration for this CSP.

Application Security

Signing

All applications must be signed. Enterprise developed applications are required to be signed by an Enterprise Certificate available through Symantec. Unsigned applications cannot be executed on the device. During device enrollment this certificate will need to be placed on the WE8H device.

Capabilities

Applications are required to declare the capabilities that they use in order to access certain system feature. Note that not all applications can access all capabilities of the system. This is done to prevent applications from introducing security risks that come with system level capabilities. The following table shows which capabilities are unlocked by Store Signing Certificates, Enterprise Signing Certificates and Device Manufacturer Certificates (OEM).

Application Capabilities Unlockable by Certificates

Capability	3rd Party (Store)	Enterprise Certificate	2nd party (OEM)
ID_CAP_APPOINTMENTS	I	I	I
ID_CAP_BUILTIN_DEFAULT	I	I	I
ID_CAP_CHAMBER_PROFILE_CODE_NITEMP_RW	I	I	I
ID_CAP_CONTACTS	I	I	I
ID_CAP_EVERYONE	I	I	I
ID_CAP_GAMERSERVICES	I	I	I
ID_CAP_IDENTITY_DEVICE	I	I	I
ID_CAP_IDENTITY_USER	I	I	I
ID_CAP_ISV_CAMERA	I	I	I
ID_CAP_LOCATION	I	I	I
ID_CAP_MAP	I	I	I
ID_CAP_MEDIALIB	I	I	I
ID_CAP_MEDIALIB_AUDIO	I	I	I
ID_CAP_MEDIALIB_PHOTO	I	I	I
ID_CAP_MEDIALIB_PLAYBACK	I	I	I
ID_CAP_MICROPHONE	I	I	I
ID_CAP_NETWORKING	I	I	I
ID_CAP_NETWORKING_INTERNET_CLIENT	I	I	I
ID_CAP_NETWORKING_INTERNET_CLIENT_SERVER	I	I	I
ID_CAP_NETWORKING_PRIVATE_NETWORK_CLIENT_SERVER	I	I	I
ID_CAP_PHONEDIALER	I	I	I
ID_CAP_PUSH_NOTIFICATION	I	I	I
ID_CAP_PROXIMITY	I	I	I
ID_CAP_REMOVABLE_STORAGE	I	I	I
ID_CAP_RINGTONE_ADD	I	I	I
ID_CAP_SCREEN_RECORDER	I	I	I
ID_CAP_SENSORS	I	I	I

Application Capabilities Unlockable by Certificates (Continued)

Capability	3rd Party (Store)	Enterprise Certificate	2nd party (OEM)
ID_CAP_SPEECH_RECOGNITION	I	I	I
ID_CAP_VOIP	I	I	I
ID_CAP_WALLET	I	I	I
ID_CAP_WALLET_PAYMENTINSTRUMENTS	I	I	I
ID_CAP_WEBBROWSERCOMPONENT	I	I	I
ID_CAP_CALLMESSAGING_FILTER			I
ID_CAP_BLUETOOTH_ADMIN			I
ID_CAP_CAMERA			I
ID_CAP_CELL_API_COMMON			I
ID_CAP_CELL_API_LOCATION			I
ID_CAP_CELL_API_OEM_PASSTHROUGH			I
ID_CAP_CELL_API_UICC			I
ID_CAP_CELL_API_UICC_LOWLEVEL			I
ID_CAP_CELL_WNF			I
ID_CAP_CELL_OEM_UICC_DATASTORE			I
ID_CAP_CSP_FOUNDATION			I
ID_CAP_CSP_MAIL			I
ID_CAP_CSP_OEM			I
ID_CAP_CSP_W4_APPLICATION			I
ID_CAP_CSP_WIFI_HOTSPOT			I
ID_CAP_DATAPLANUSAGE_ADMIN			I
ID_CAP_DEVICE_MANAGEMENT			I
ID_CAP_DEVICE_MANAGEMENT_ADMIN			I
ID_CAP_DEVICE_MANAGEMENT_BOOTSTRAP			I
ID_CAP_DEVICE_MANAGEMENT_SECURITY_POLICIES			I
ID_CAP_DU_MIGRATOR_STATUS_OEM			I
ID_CAP_OEMPUBLICDIRECTORY			I
ID_CAP_PLATFORM_EXTENSIBILITY			I
ID_CAP_INTERNAL_DEPLOYMENT			I
ID_CAP_INTERNET_EXPLORER_FAVORITES			I
ID_CAP_INTERNET_EXPLORER_SEARCH_PROVIDER_KEYS_HKCU			I
ID_CAP_INTEROPSERVICES			I
ID_CAP_KIDZONE_CUSTOMIZATION			I
ID_CAP_MAP_WRITE			I
ID_CAP_MEDIALIB_PHOTO_FULL			I
ID_CAP_MO_CLOUDMESSAGING			I
ID_CAP_NATIVE_NETWORK_REPLACEMENT			I
ID_CAP_NETWORKING_ADMIN			I
ID_CAP_NETWORKING_VPN_PROVIDER			I
ID_CAP_NETWORKING_VPN_SERVICES			I
ID_CAP_NVREADWRITE			I

Application Capabilities Unlockable by Certificates (Continued)

Capability	3rd Party (Store)	Enterprise Certificate	2nd party (OEM)
ID_CAP_OEM_ADC			I
ID_CAP_OEM_CUSTOM			I
ID_CAP_OEM_DEPLOYMENT			I
ID_CAP_OEMPUBLICDIRECTORY			I
ID_CAP_PEOPLE_EXTENSION			I
ID_CAP_PEOPLE_EXTENSION_IM			I
ID_CAP_PEOPLE_EXTENSION_MOBILE			I
ID_CAP_PERSONAL_INFORMATION_IMPORT			I
ID_CAP_PHONE_ADMIN			I
ID_CAP_RUNTIME_CONFIG			I
ID_CAP_SHARED_USER_CERTIFICATES			I
ID_CAP_SHELL_DEVICE_LOCK_UI_API			I
ID_CAP_SHELL_OEM_ADMIN			I
ID_CAP_SCREEN_RECORDER_BKG			I
ID_CAP_SMS			I
ID_CAP_SMS_COMPANION			I
ID_CAP_SMS_INTERCEPT_AGENT			I
ID_CAP_SMS_INTERCEPT_RECIPIENT			I
ID_CAP_SYNC_EXTENSION			I
ID_CAP_VOICEMAIL			I
ID_CAP_WALLET_SECUREELEMENT			I
ID_CAP_WIFI_BASIC			I
ID_CAP_ENTERPRISE_SHARED_DATA		I	
ID_CAP_SHARED_USER_CERTIFICATES		I	

API Restrictions

Microsoft provides restrictions on which APIs applications can use as part of their certification process to ensure that APIs that could reduce system security are not used by applications. Another reason for the restriction is certain APIs may be planned for obsolescence and Microsoft does not want applications to require maintenance when APIs are removed. Honeywell recommends that enterprise customers follow Microsoft API recommendations.

Store applications are restricted to the APIs that they can use for application development. During the certification process if APIs are used that are restricted the application will not be allowed on the Store.

Honeywell applications may be restricted to the APIs that they can use for application development if they are planned to be built into the device image as part of the operating system or if they are to be commercially available through the store. In either of these cases if restricted APIs are used the application will not be certified and signed.

Enterprise applications can either be store signed or self-signed. When self-signed there is no processes by which APIs will restrict the ability of a developer to sign and deploy an application. This means that all Win32 APIs are available to the Enterprise Application. However use of Win32 APIs is still restricted by application capabilities. Any API that is a part of a capability to which Enterprise Applications are not entitled will create an access violation at runtime. Microsoft does not provide an API to Capability mapping thus making it difficult to tell which APIs are covered by capabilities and which are not. However high-security risk APIs are protected by capabilities. Enterprise decision to include APIs not documented as approved for store applications places the obsolescence, security and runtime error risk upon the Enterprise to manage. Honeywell does not recommend the behavior of using non-approved APIs for enterprise application development.

For the approved list of application APIs to use, see the following Microsoft documentation:

http://msdn.microsoft.com/en-us/library/windows/apps/ff626516%28v=vs.105%29.aspx

http://msdn.microsoft.com/en-us/library/dn715922(v=winembedded.81).aspx

For developing secure applications see the following Microsoft documentation:

http://msdn.microsoft.com/en-us/library/windows/apps/xaml/hh849625.aspx

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

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.

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.

12

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